



Reliability, Resilience and Defense technology for the grid

D2.3 – Final version of the R²D² Requirements and Detailed Architecture Design

Date: 31/01/2024



**Funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Horizon Europe Grant agreement N° 101075714.



D2.3 – Requirements and Detailed Architecture Design

Deliverable details

Title	WP	Version
D2.3 – Requirements and Detailed Architecture Design	2	2.0

Contractual delivery date	Actual delivery date	Delivery type*
31/01/2024	31/01/2024	R

*Delivery type: R: Document, report; DEM: Demonstrator, pilot, prototype; DEC: Websites, patent fillings, videos, etc; OTHER; ETHICS: Ethics requirement; ORDP: Open Research Data Pilot.

Author(s)	Organisation
Srđan Subotić	EMSS
Ugo Stecchi, Lucas Pons	ETRA
Mathaios Panteli	UCY

Organisation	Contributors*
ETRA	Sergi Grau, Pablo Bort
S2	Alex Alhambra, Aida Carrillo
ELPROS	Tadeja Babnik, Bojan Mahkovec
GUARD	Margo Raja, Mihkel Väljaots, Priit Anton
CYBER	Papadatos Kostas, Rantos Konstantinos, Aslanidis George, Makrygeorgou Argyris, Valkaniotis Tilemachos, Zapalidi Aggeliki
ICCS	Ektor Stasinou, Athanasios Botsis, Dimitris Lagos, Marios Zoutis, Savvas Karras
SCC	Kristina Janošević, Dušica Marković, Andrijana Prešić, Bojan Stamenković, Predrag Simić, Dušan Prešić, Ismar Sinanović
EMSS	Julijana Vićovac, Jasmina Đorđević, Simona Radonjić, Ivana Stamenić, Marija Miljuš, Jelena Đorđević, Milica Nektarijević, Petar Petrović, Srđan Mladenović, Vladimir Bečejac, Nemanja Vukojičić, Mirko Mladenović, Jovica Vidaković, Neven Nikolić, Stefan Tirnanić, Petar Petrov, Nikola Savić, Nemanja Bralušić, Borko Čupić, Miroslav Vilček, Miloš Bojanić, Miroslav Novaković, Miroslav Žerajić, Filip Đorđević, Aleksandar Vojinović
HEDNO	Theofanis Kontopoulos, , Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis
ELEK	Anja Korošec, Jurij Curk, Boris Turha, Janez Pirnovar
ELOVE	Suzana Wallner, Božana Govednik, Anton Žagar, Simon Peternel
EDP	Motaz Ayid, João Mateus
IMP	Marija Popović, Goran Jakupović, Igor Bundalo, Milan Josifović
UCY	Mathaios Panteli, Georgios Paphitis, Marios Siimillas
RTE-i	César Clause, Anouar Guesrami
ICL	Dawei Qiu

*Contributors presented in this table were engaged on the definition of UCs, requirements, system architecture and KPIs during whole period of WP2 activities, including the preparation of deliverable [11]

D2.3 – Requirements and Detailed Architecture Design

Version	Date	Person	Action	Status*	Dissemination**
0.1	13.12.2023	Srđan Subotić	Initial draft	Draft	CO
0.2	10.1.2024	Mathaios Panteli Ugo Stechi, Lucas Pons,	Initial draft completion (without Annexes)	Draft	CO
0.3	23.1.2024	Dušan Prešić, Tadeja Babnik, Elena Montojo Vanrell	Commenting and corrections	Draft	CO
0.4	24.1.2026	Srđan Subotić, Lucas Pons, Mathaios Panteli	Drafting of Annexes I, III, IV and VI	Draft	CO
0.5	29.1.2024	Ektor Statinos Srđan Subotić	Drafting of Annexes I and IV, corrections	Draft	CO
1.0	30.1.2024	Srđan Subotić	Final draft	Final	Pu
2.0	25.6.2024	Srđan Subotić	Final draft corrections after request for revision	Final	Pu

*Status: Draft, Final, Approved, Submitted (to European Commission).

Dissemination Level: **PU: Public; **CO**: Confidential, only for members of the consortium (including the Commission Services)

Executive Summary

This deliverable refers to several activities related to Work Package 2, which are:

- The definition of use-cases, the definition of the requirements (T2.1),
- The design of the smart grid architecture for R²D² solutions (T2.2) and
- The definition of the project KPIs (T2.3) for quantifying the effects of the products through defined use-cases on certain pilot sites.

The development of the three tasks constitutes the foundation stone of R²D² project, on top of which it will be possible to develop the four R²D² products in the next Work Packages (C3PO in WP3, IRIS in WP4, PRECOG in WP5 and EMMA in WP6).

Given the critical role these tasks are covering in the project, an overall methodology for the definition of the project foundation is described in the next chapters. The centrality of this document, therefore, requires a solid and structured approach to the definition of the methodology on which the foundations of the project are based, even more because the interaction of several tasks requires precise coordination and a clear division of roles between the partners (see Section 3 for more details). This methodology is not only expressed in the definition of the project foundations but also goes so far as to detail the individual activities of which it is composed, to guarantee coherent planning and execution with the subsequent project activities. In particular, the following chapters describe for each of the individual activities within Tasks 2.1, 2.2 and 2.3 a clear and systematic procedure for the definition of Use Cases, requirements, KPIs and the architecture underlying the R²D² solutions.



D2.3 - Requirements and Detailed Architecture Design

The project foundations are organised in a double iteration procedure as explained in Section 3. The output of the first iteration was described in Deliverable 2.1 and it includes the preliminary version of the Use Cases and the requirements. After that, it was possible to start defining architectural diagrams for the R²D² solutions and, in parallel, to assign project KPIs to Use Cases and Products. This coincides with the achievement of the project Milestones number 2 “Technical Settlement”, since the results presented in Deliverable 2.1 constitute the technical basis to start the active development of the tools and products in WP 3, 4, 5 and 6, allowing technical partners to complete the final design of their developments.

Once the full design of the four main Products was ready, the second iteration of the project foundation started in July 2023. Results of concluded definition of the Use Cases and requirements as well final architecture for R2D2 products are described in this deliverable D2.3, which is the second version of deliverable [11].

Thus, the D2.3 report additionally contains the following in relation to [11]:

- 2 new use cases (UC39 and UC40)
- 203 new requirements (mainly related to UC of EMMA and IRIS product)
- Information and function SGAM layers for UC1-38, and all SGAM layers for UC39-40

Also, there are several updated use cases, which also affected requirements, SGAM diagrams and KPIs.

Throughout the activities carried out in T2.1, T2.2 and T2.3 the following final results were achieved:

- 7 Business Cases in line with the project objectives
- 40 Use Cases supported by a definition template (following IEC 62559) and a revision form
- 355 requirements defined, validated and revised according to VOLERE methodology;
- 40 project and complementary KPIs assigned to each Use Case and to each R²D² Product and tool
- 352 system's architecture diagrams including business, components and communication layer diagrams

Detailed information about UCs definition, UCs revision, the requirements, the architecture and the KPIs of the UCs are in this document presented separately in Annexes I to VII.

Please note: at the time of writing this deliverable, the partner EDP Spain informed the project coordinator of its wish to leave the consortium. This event will have consequences on the Spanish demonstrator site, which will be replaced by a new pilot site, and at which site the use cases described here will have to be tested. At the moment, a new demonstrator site has not yet been confirmed. Therefore, for the continuation of the project and to be able to deliver the document by the due date, where the Spanish demo is indicated in the use cases described below, reference will be made to the new demonstrator site to be involved in the project.



Keywords

Business Cases, Use Cases, Requirements, Project Products, System Architecture, SGAM, KPIs

Copyright statement

The work described in this document has been conducted within the R²D² project. This document reflects only the R²D² Consortium view and the European Union is not responsible for any use that may be made of the information it contains.

This document and its content are the property of the R²D² Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the R²D² Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the R²D² Partners.

Each R²D² Partner may use this document in conformity with the R²D² Consortium Grant Agreement provisions.

1. TABLE OF CONTENTS

1.	TABLE OF CONTENTS	6
1.1	List of tables.....	9
1.2	List of figures.....	10
2.	INTRODUCTION	25
2.1	Purpose of the Document	25
2.2	Scope of the Document.....	25
2.3	Structure of the Document	26
3.	R ² D ² FOUNDATIONS	27
3.1	Overall Methodology.....	27
3.2	Objectives and Business Cases	29
4.	USE CASES	32
4.1	Introduction	32
4.2	Use Case Methodology.....	32
4.2.1	Introduction	32
4.2.2	Use Case Identification	34
4.2.3	Use Case Definition	34
4.2.4	Use Case Revision	38
4.2.5	Use Case Finalization	39
4.3	Use Cases analysis	40
4.3.1	WP3 (C3PO) Use Cases	42
4.3.2	WP4 (IRIS) Use Cases	46
4.3.3	WP5 (PRECOG) Use Cases	49
4.3.4	WP6 (EMMA) Use Cases	52
4.3.5	Additional information about Use Cases	56
4.3.5.1	Use Cases and Business Cases	57
4.3.5.2	Use Cases and Project Tasks	58
5.	REQUIREMENTS	60
5.1	Introduction and Methodology.....	60
5.1.1	Requirement Definition	61
5.1.2	Validation and Revision	62
5.2	R ² D ² requirements.....	63
6.	SYSTEM ARCHITECTURE DEFINITION	82



D2.3 - Requirements and Detailed Architecture Design

6.1	Methodology and SGAM architecture.....	82
6.1.1	Inputs for the architecture	84
6.2	SGAM and Use Cases - communication layer diagrams	85
6.2.1	Business Layer	85
6.2.2	Component Layer	91
6.2.3	Communication Layer	91
6.2.4	Function Layer	92
6.2.5	Information Layer	95
7.	KPI IDENTIFICATION AND MONITORING PREPARATION	98
7.1	Introduction and Methodology.....	98
7.2	Methodology for defining, quantifying and monitoring KPIs.....	98
7.3	List and analysis of KPIs.....	100
8.	CONCLUSIONS	104
9.	References	106
9.1	References	106
9.2	Acronyms	106
10.	ANNEX I: USE CASE DEFINITION FORMS	108
10.1	USE CASE 1 FORM	109
10.2	USE CASE 2 FORM.....	123
10.3	USE CASE 3 FORM.....	131
10.4	USE CASE 4 FORM	139
10.5	USE CASE 5 FORM.....	146
10.6	USE CASE 6 FORM.....	155
10.7	USE CASE 7 FORM.....	164
10.8	USE CASE 8 FORM	174
10.9	USE CASE 9 FORM.....	186
10.10	USE CASE 10 FORM	197
10.11	USE CASE 11 FORM	209
10.12	USE CASE 12 FORM	220
10.13	USE CASE 13 FORM	231
10.14	USE CASE 14 FORM	242
10.15	USE CASE 15 FORM	250
10.16	USE CASE 16 FORM	261
10.17	USE CASE 17 FORM	269
10.18	USE CASE 18 FORM	279
10.19	USE CASE 19 FORM	286



D2.3 - Requirements and Detailed Architecture Design

10.20	USE CASE 20 FORM	306
10.21	USE CASE 21 FORM	322
10.22	USE CASE 22 FORM	336
10.23	USE CASE 23 FORM	356
10.24	USE CASE 24 FORM	367
10.25	USE CASE 25 FORM	378
10.26	USE CASE 26 FORM	390
10.27	USE CASE 27 FORM	403
10.28	USE CASE 28 FORM	415
10.29	USE CASE 29 FORM	425
10.30	USE CASE 30 FORM	436
10.31	USE CASE 31 FORM	449
10.32	USE CASE 32 FORM	459
10.33	USE CASE 33 FORM	470
10.34	USE CASE 34 FORM	485
10.35	USE CASE 35 FORM	496
10.36	USE CASE 36 FORM	515
10.37	USE CASE 37 FORM	532
10.38	USE CASE 38 FORM	543
10.39	USE CASE 39 FORM	552
10.40	USE CASE 40 FORM	571
11.	ANNEX II: USE CASE REVISION FORM	582
12.	ANNEX III: FULL INFORMATION REQUIREMENTS TABLE	585
13.	ANNEX IV: SYSTEM ARCHITECTURE	683
13.1	SGAM Function Layer, sequence and activity diagrams	683
13.1.1	WP3-C3PO	683
13.1.2	WP4-IRIS	712
13.1.3	WP5-PRECOG	744
13.1.4	WP6-EMMA	775
13.2	SGAM Information Layer	835
13.2.1	Business Context View	835
13.2.1.1	WP3-C3PO	835
13.2.1.2	WP4-IRIS	844
13.2.1.3	WP5-PRECOG	854
13.2.1.4	WP6-EMMA	862
13.2.2	Canonical Data Model	875



D2.3 - Requirements and Detailed Architecture Design

13.2.2.1	WP3-C3PO	875
13.2.2.2	WP4-IRIS	884
13.2.2.3	WP5-PRECOG	894
13.2.2.4	WP6-EMMA	902
13.2.3	Standard and Information Object Mapping	915
13.2.3.1	WP3-C3PO	915
13.2.3.2	WP4-IRIS	924
13.2.3.3	WP5-PRECOG	934
13.2.3.4	WP6-EMMA	942
13.3	SGAM Communication Layer	955
13.3.1	WP3-C3PO	955
13.3.2	WP4-IRIS	964
13.3.3	WP5-PRECOG	974
13.3.4	WP6-EMMA	982
13.4	SGAM Component Layer	995
13.4.1	WP3-C3PO	995
13.4.2	WP4-IRIS	1004
13.4.3	WP5-PRECOG	1014
13.4.4	WP6-EMMA	1022
14.	ANNEX V: KPI TEMPLATES	1035
15.	ANNEX VI: QUANTIFICATION INFORMATION OF KPIs	1038
16.	ANNEX VII: CONTINUOUS SW QUALITY AND SECURITY DEPENDENCY	1071

1.1 LIST OF TABLES

Table 1 – Terminology definitions	29
Table 2 – UCs from C3PO (WP3)	43
Table 3 – UCs from IRIS (WP4)	47
Table 4 – UCs from PRECOG (WP5)	49
Table 5 – UCs from EMMA (WP6)	53
Table 6 – Use Cases and business cases correlation	57

Table 7 – Correspondence between UCs and WPs	59
Table 8 – List of requirements	63
Table 9 – Number of requirements per Product/WP and per Type	81
Table 10 – Number of requirements per priority level	81
Table 11 – Use Cases vs KPIs mapping	101
Table 12 – Products vs KPIs mapping	103
Table 13 – Acronyms	106

1.2 LIST OF FIGURES

Figure 1 – Overall methodology for the R ² D ² foundations from tasks 2.1, 2.2 and 2.3	27
Figure 2 – IEC 62559 standard series [4]	33
Figure 3 – Use case creation process	34
Figure 4 – Process of requirement definition, validation and revision	61
Figure 5 – Screenshot of new requirement definition in “Volere” tool	62
Figure 6 – SGAM interoperability layers: Source: [8]	82
Figure 7 – SGAM Framework	84
Figure 8 – Sample of input diagram adopted in R ² D ²	85
Figure 9 – Representation of R ² D ² Business Goals, Actors and Business Cases	86
Figure 10 – BA1-centric business layer diagram	87
Figure 11 – BA2-centric business layer diagram	88
Figure 12 – BA3-centric business layer diagram	89
Figure 13 – BA4-centric business layer diagram	90
Figure 14 – Example of Component layer diagram	91
Figure 15 – Example of communication layer diagram	92
Figure 16 – Example of Function layer diagram	94
Figure 17 – Example of Sequence Diagram under the Function layer	94
Figure 18 – Example of the Activity Diagram under the Function Layer	95

Figure 19 - Example of Information layer diagrams: Business Context view within the Information Layer	96
Figure 20 - Example of the Standard and Information Object Mapping diagram within the Information Layer	97
Figure 21: Example of a canonical data model representation within the Information Layer	97
Figure 22 - Methodology for defining, quantifying, monitoring and reporting KPIs	99
Figure 23 - UC22 Functional Layer	683
Figure 24 - UC22 Activity Graph	684
Figure 25 - UC22 Basic Path	685
Figure 26 - UC23 Functional layer	686
Figure 27 - UC23 Activity Graph	687
Figure 28 - UC23 Basic Path	688
Figure 29 - UC24 Functional Layer	689
Figure 30 - UC24 Activity Graph	690
Figure 31 - UC24 Basic Path	691
Figure 32 - UC25 Functional Layer	692
Figure 33 - UC25 Activity Graph	693
Figure 34 - UC25 Basic Path	694
Figure 35 - UC26 Functional Layer	695
Figure 36 - UC26 Activity Graph	696
Figure 37 - UC26 Basic Path	697
Figure 38 - UC29 Functional Layer	698
Figure 39 - UC29 Activity Graph	699
Figure 40 - UC29 Basic Path	700
Figure 41 - UC30 Functional Layer	701
Figure 42 - UC30 Activity Graph	702
Figure 43 - UC30 Basic Path	703
Figure 44 - UC32 Functional Layer	704



D2.3 - Requirements and Detailed Architecture Design

Figure 45 - UC32 Activity Graph	705
Figure 46 - UC32 Basic Path	706
Figure 47 - UC32 Alternative Path	707
Figure 48 - UC39 Functional layer	708
Figure 49 - UC39 Activity Graph	709
Figure 50 - UC39 Basic Path	710
Figure 51 - UC39 Alternative Path	711
Figure 52 - UC07 Actors Involved	712
Figure 53 - UC07 Functional Layer	713
Figure 54 - UC07 Activity Graph	714
Figure 55 - UC07 Scenario 1	715
Figure 56 - UC07 Basic Path	716
Figure 57 - UC10 Functional Layer	717
Figure 58 - UC10 Basic Path	718
Figure 59 - UC10 Sequence Diagram	719
Figure 60 - UC11 Functional Layer	720
Figure 61 - UC11 Activity Graph	721
Figure 62 - UC11 Sequence Diagram	722
Figure 63 - UC12 Functional Layer	723
Figure 64 - UC12 Activity Graph	724
Figure 65 - UC12 Basic Path	725
Figure 66 - UC15 Functional Layer	726
Figure 67 - UC15 Activity Graph	727
Figure 68 - UC15 Basic Path	728
Figure 69 - UC16 Functional Layer	729
Figure 70 - UC16 Activity Graph	730
Figure 71 - UC16 Basic Path	731



D2.3 - Requirements and Detailed Architecture Design

Figure 72 - UC18 Functional Layer	732
Figure 73 - UC18 Activity Graph	733
Figure 74 - UC18 Basic Path	734
Figure 75 - UC19 Functional Layer	735
Figure 76 - UC19 Activity Graph	736
Figure 77 - UC19 Basic Path	737
Figure 78 - UC21 Functional Layer	738
Figure 79 - Activity Graph	739
Figure 80 - UC21 Basic Path	740
Figure 81 - UC35 Functional Layer	741
Figure 82- UC35 Activity Graph	742
Figure 83 - UC35 Basic Path	743
Figure 84 - UC27 Functional Layer	744
Figure 85 - UC27 Activity Graph	745
Figure 86 - UC27 Basic Path	746
Figure 87 - UC28 Functional Layer	747
Figure 88 - UC28 Activity Graph	748
Figure 89 - UC28 Basic Path	749
Figure 90 - UC28 Alternative Scenario Basic Path	750
Figure 91 - UC33 Actors involved	751
Figure 92 - UC33 Functional Layer	752
Figure 93 - UC33 Activity Graph	753
Figure 94 - UC33 Basic Path	754
Figure 95 - UC34 Actors Involved	755
Figure 96 - UC34 Functional Layer	756
Figure 97 - UC34 Activity Graph	757
Figure 98 - UC34 Basic Path	758



D2.3 - Requirements and Detailed Architecture Design

Figure 99 - UC36 Actors Involved	759
Figure 100 - UC36 Functional Layer	760
Figure 101 - UC36 Activity Graph	761
Figure 102 - UC36 Basic Path	762
Figure 103 - UC37 Actors Involved	763
Figure 104 - UC37 Functional Layer	764
Figure 105 - UC37 Activity Graph	765
Figure 106 - UC37 Basic Path	766
Figure 107 - UC38 Actors Involved	767
Figure 108 - UC38 Functional Layer	768
Figure 109 - UC38 Activity Graph	769
Figure 110 - UC38 Basic Path	770
Figure 111 - UC40 Actors Involved	771
Figure 112 - UC40 Functional Layer	772
Figure 113 - UC40 Activity Graph	773
Figure 114 - UC40 Basic Path	774
Figure 115 - UC01 Actors Involved	775
Figure 116 - UC01 Functional Layer	776
Figure 117 - UC01 Activity Graph	777
Figure 118 - UC01 Basic Path (1)	778
Figure 119 - UC01 Basic Path (2)	779
Figure 120 - UC01 Basic Path (3)	780
Figure 121 - UC02 Actor Involved	781
Figure 122 - UC02 Functional Layer	782
Figure 123 - UC02 Activity Graph	783
Figure 124 - UC02 Basic Path (1)	784
Figure 125 - UC02 Basic Path (2)	785



D2.3 - Requirements and Detailed Architecture Design

Figure 126- UC03 Actors Involved	786
Figure 127 - UC03 Functional Layer	787
Figure 128 - UC03 Activity Graph	788
Figure 129 - UC03 Basic Path	789
Figure 130 - UC04 Actors Involved	790
Figure 131 - UC04 Functional Layer	791
Figure 132 - UC04 Activity Graph	792
Figure 133 - UC04 Basic Path (1)	793
Figure 134 - UC04 Basic Path (2)	794
Figure 135 - UC05 Actors Involved	795
Figure 136 - UC05 Functional Layer	796
Figure 137 - UC05 Activity Graph	797
Figure 138 - UC05 Basic Path	798
Figure 139 - UC06 Actors Involved	799
Figure 140 - UC06 Functional Layer	800
Figure 141 - UC06 Functional Graph	801
Figure 142 - UC06 Basic Path	802
Figure 143 - UC08 Actors Involved	803
Figure 144 - UC08 Functional Layer	804
Figure 145 - UC08 Activity Graph	805
Figure 146 - UC08 Basic Path	806
Figure 147 - UC09 Actors Involved	807
Figure 148 - UC09 Functional Layer	808
Figure 149 - UC09 Activity Graph	809
Figure 150 - UC09 Basic Path (1)	810
Figure 151 - UC09 Basic Path (2)	811
Figure 152 - UC09 Basic Path (3)	812



D2.3 - Requirements and Detailed Architecture Design

Figure 153 - UC13 Actors Involved	813
Figure 154- UC13 Functional Layer	814
Figure 155 - UC13 Activity Graph	815
Figure 156 - UC13 Basic Path (1)	816
Figure 157 - UC13 Basic Path (2)	817
Figure 158 - UC14 Actors Involved	818
Figure 159 - UC14 Functional Layer	819
Figure 160 - UC14 Activity Graph	820
Figure 161 - UC14 Basic Path	821
Figure 162 - UC17 Actors Involved	822
Figure 163 - UC17 Functional Layer	823
Figure 164 - UC17 Activity Graph	824
Figure 165 - UC17 Basic Path	825
Figure 166 - UC20 Actors Involved	826
Figure 167 - UC20 Functional Layer	827
Figure 168 - UC20 Activity Graph	828
Figure 169 - UC20 Basic Path	829
Figure 170 - UC31 Actors Involved	830
Figure 171 - UC31 Functional Layer	831
Figure 172 - UC31 Activity Graph	832
Figure 173 - UC31 Basic Path (1)	833
Figure 174 - UC31 Basic Path (2)	834
Figure 175 - UC22 Business Layer	835
Figure 176 - UC23 Business Layer	836
Figure 177 - UC24 Business Layer	837
Figure 178 - UC25 Business Layer	838
Figure 179 - UC26 Business Layer	839



D2.3 - Requirements and Detailed Architecture Design

Figure 180 - UC29 Business Layer	840
Figure 181 - UC30 Business Layer	841
Figure 182 - UC32 Business Layer	842
Figure 183 - UC39 Business Layer	843
Figure 184 - UC07 Business Layer	844
Figure 185 - UC10 Business Layer	845
Figure 186 - UC11 Business Layer	846
Figure 187 - UC12 Business Layer	847
Figure 188 - UC15 Business Layer	848
Figure 189 - UC16 Business Layer	849
Figure 190 - UC18 Business Layer	850
Figure 191 - UC19 Business Layer	851
Figure 192 - UC21 Business Layer	852
Figure 193 - UC35 Business Layer	853
Figure 194 - UC27 Business Layer	854
Figure 195 - UC28 Business Layer	855
Figure 196 - UC33 Business Layer	856
Figure 197 - UC34 Business Layer	857
Figure 198 - UC36 Business Layer	858
Figure 199 - UC37 Business Layer	859
Figure 200 - UC38 Business Layer	860
Figure 201 - UC40 Business Layer	861
Figure 202 - UC01 Business Layer	862
Figure 203 - UC02 Business Layer	863
Figure 204 - UC03 Business Layer	864
Figure 205 - UC04 Business Layer	865
Figure 206 - UC05 Business Layer	866

Figure 207 - UC06 Business Layer	867
Figure 208 - UC08 Business Layer	868
Figure 209 - UC09 Business Layer	869
Figure 210 - UC13 Business Layer	870
Figure 211 - UC14 Business Layer	871
Figure 212 - UC17 Business Layer	872
Figure 213 - UC20 Business Layer	873
Figure 214 - UC31 Business Layer	874
Figure 215 - UC22 Canonical Data Model	875
Figure 216 - UC23 Canonical Data Model	876
Figure 217 - UC24 Canonical Data Model	877
Figure 218 - UC25 Canonical Data Model	878
Figure 219 - UC26 Canonical Data Model	879
Figure 220 - UC29 Canonical Data Model	880
Figure 221 - UC30 Canonical Data Model	881
Figure 222 - UC32 Canonical Data Model	882
Figure 223 - UC39 Canonical Data Model	883
Figure 224 - UC07 Canonical Data Model	884
Figure 225 - UC10 Canonical Data Model	885
Figure 226 - UC11 Canonical Data Model	886
Figure 227 - UC12 Canonical Data Model	887
Figure 228 - UC15 Canonical Data Model	888
Figure 229 - UC16 Canonical Data Model	889
Figure 230 - UC18 Canonical Data Model	890
Figure 231 - UC19 Canonical Data Model	891
Figure 232 - UC21 Canonical Data Model	892
Figure 233 - UC35 Canonical Data Model	893



D2.3 – Requirements and Detailed Architecture Design

Figure 234 – UC27 Canonical Data Model	894
Figure 235 – UC28 Canonical Data Model	895
Figure 236 – UC33 Canonical Data Model	896
Figure 237 – UC34 Canonical Data Model	897
Figure 238 – UC36 Canonical Data Model	898
Figure 239 – UC37 Canonical Data Model	899
Figure 240 – UC38 Canonical Data Model	900
Figure 241 – UC40 Canonical Data Model	901
Figure 242 – UC01 Canonical Data Model	902
Figure 243 – UC02 Canonical Data Model	903
Figure 244 – UC03 Canonical Data Model	904
Figure 245 – UC04 Canonical Data Model	905
Figure 246 – UC05 Canonical Data Model	906
Figure 247 – UC06 Canonical Data Model	907
Figure 248 – UC08 Canonical Data Model	908
Figure 249 – UC09 Canonical Data Model	909
Figure 250 – UC13 Canonical Data Model	910
Figure 251 – UC14 Canonical Data Model	911
Figure 252 – UC17 Canonical Data Model	912
Figure 253 – UC20 Canonical Data Model	913
Figure 254 – UC31 Canonical Data Model	914
Figure 255 – UC22 Information Object Mapping	915
Figure 256 – UC23 Information Object Mapping	916
Figure 257 – UC24 Information Object Mapping	917
Figure 258 – UC25 Information Object Mapping	918
Figure 259 – UC26 Information Object Mapping	919
Figure 260 – UC29 Information Object Mapping	920



D2.3 – Requirements and Detailed Architecture Design

Figure 261 – UC30 Information Object Mapping	921
Figure 262 – UC32 Information Object Mapping	922
Figure 263 – UC39 Information Object Mapping	923
Figure 264 – UC07 Information Object Mapping	924
Figure 265 – UC10 Information Object Mapping	925
Figure 266 – UC11 Information Object Mapping	926
Figure 267 – UC12 Information Object Mapping	927
Figure 268 – UC15 Information Object Mapping	928
Figure 269 – UC16 Information Object Mapping	929
Figure 270 – UC18 Information Object Mapping	930
Figure 271 – UC19 Information Object Mapping	931
Figure 272 – UC21 Information Object Mapping	932
Figure 273 – UC35 Information Object Mapping	933
Figure 274 – UC27 Information Object Mapping	934
Figure 275 – UC28 Information Object Mapping	935
Figure 276 – UC33 Information Object Mapping	936
Figure 277 – UC34 Information Object Mapping	937
Figure 278 – UC36 Information Object Mapping	938
Figure 279 – UC37 Information Object Mapping	939
Figure 280 – UC38 Information Object Mapping	940
Figure 281 – UC40 Information Object Mapping	941
Figure 282 – UC01 Information Object Mapping	942
Figure 283 – UC02 Information Object Mapping	943
Figure 284 – UC03 Information Object Mapping	944
Figure 285 – UC04 Information Object Mapping	945
Figure 286 – UC05 Information Object Mapping	946
Figure 287 – UC06 Information Object Mapping	947



D2.3 - Requirements and Detailed Architecture Design

Figure 288 - UC08 Information Object Mapping	948
Figure 289 - UC09 Information Object Mapping	949
Figure 290 - UC13 Information Object Mapping	950
Figure 291 - UC14 Information Object Mapping	951
Figure 292 - UC17 Information Object Mapping	952
Figure 293 - UC20 Information Object Mapping	953
Figure 294 - UC31 Information Object Mapping	954
Figure 295 - UC22 Communication Layer	955
Figure 296 - UC23 Communication Layer	956
Figure 297 - UC24 Communication Layer	957
Figure 298 - UC25 Communication Layer	958
Figure 299 - UC26 Communication Layer	959
Figure 300 - UC29 Communication Layer	960
Figure 301 - UC30 Communication Layer	961
Figure 302 - UC32 Communication Layer	962
Figure 303 - UC39 Communication Layer	963
Figure 304 - UC07 Communication Layer	964
Figure 305 - UC10 Communication Layer	965
Figure 306 - UC11 Communication Layer	966
Figure 307 - UC12 Communication Layer	967
Figure 308 - UC15 Communication Layer	968
Figure 309 - UC16 Communication Layer	969
Figure 310 - UC18 Communication Layer	970
Figure 311 - UC19 Communication Layer	971
Figure 312 - UC21 Communication Layer	972
Figure 313 - UC35 Communication Layer	973
Figure 314 - UC27 Communication Layer	974



D2.3 - Requirements and Detailed Architecture Design

Figure 315 - UC28 Communication Layer	975
Figure 316 - UC33 Communication Layer	976
Figure 317 - UC35 Communication Layer	977
Figure 318 - UC36 Communication Layer	978
Figure 319 - UC37 Communication Layer	979
Figure 320 - UC38 Communication Layer	980
Figure 321 - UC40 Communication Layer	981
Figure 322 - UC01 Communication Layer	982
Figure 323 - UC02 Communication Layer	983
Figure 324 - UC03 Communication Layer	984
Figure 325 - UC04 Communication Layer	985
Figure 326 - UC05 Communication Layer	986
Figure 327 - UC06 Communication Layer	987
Figure 328 - UC08 Communication Layer	988
Figure 329 - UC09 Communication Layer	989
Figure 330 - UC13 Communication Layer	990
Figure 331 - UC 14 Communication Layer	991
Figure 332 - UC17 Communication Layer	992
Figure 333 - UC20 Communication Layer	993
Figure 334 - UC31 Communication Layer	994
Figure 335 - UC22 Component Layer	995
Figure 336 - UC23 Component Layer	996
Figure 337 - UC24 Component Layer	997
Figure 338 - UC25 Component Layer	998
Figure 339 - UC26 Component Layer	999
Figure 340 - UC29 Component Layer	1000
Figure 341 - UC30 Component Layer	1001

Figure 342 - UC32 Component Layer	1002
Figure 343 - UC39 Component Layer	1003
Figure 344 - UC07 Component Layer	1004
Figure 345 - UC10 Component Layer	1005
Figure 346 - UC11 Component Layer	1006
Figure 347 - UC12 Component Layer	1007
Figure 348 - UC15 Component Layer	1008
Figure 349 - UC16 Component Layer	1009
Figure 350 - UC18 Component Layer	1010
Figure 351 - UC19 Component Layer	1011
Figure 352 - UC21 Component Layer	1012
Figure 353 - UC35 Component Layer	1013
Figure 354 - UC27 Component Layer	1014
Figure 355 - UC36 Component Layer	1015
Figure 356 - UC33 Component Layer	1016
Figure 357 - UC34 Component Layer	1017
Figure 358 - UC36 Component Layer	1018
Figure 359 - UC37 Component Layer	1019
Figure 360 - UC38 Component Layer	1020
Figure 361 - UC40 Component Layer	1021
Figure 362 - UC01 Component Layer	1022
Figure 363 - UC02 Component Layer	1023
Figure 364 - UC03 Component Layer	1024
Figure 365 - UC04 Component Layer	1025
Figure 366 - UC05 Component Layer	1026
Figure 367 - UC06 Component Layer	1027
Figure 368 - UC08 Component Layer	1028



D2.3 - Requirements and Detailed Architecture Design

Figure 369 - UC09 Component Layer	1029
Figure 370 - UC13 Component Layer	1030
Figure 371 - UC14 Component Layer	1031
Figure 372 - UC17 Component Layer	1032
Figure 373 - UC20 Component Layer	1033
Figure 374 - UC31 Component Layer	1034

2. INTRODUCTION

2.1 PURPOSE OF THE DOCUMENT

D2.3 – Document “Requirements and Detailed Architecture Design” (hereinafter: D2.3 Report) is a report on the end-user and business requirements, accompanied by the corresponding technical design and specifications of the individual components and integrated R²D² solution as defined in the R²D² Project documentation [1].

D2.3 Report is the final report and it contains all activities carried out by the project's M16 regarding Use Cases (UCs), Requirements and Detailed Architecture Design, as well as all previous activities related to these topics.

2.2 SCOPE OF THE DOCUMENT

This document describes the work carried out in tasks T2.1, T2.2 and T2.3, i.e.:

- Definition of business scenarios, UCs and requirements
- System architecture definition and
- KPIs identification

Defined UCs consider the needs of Transmission system Operators (TSOs), Distribution system operators (DSOs) energy producers and other end users in the scenario of threats (cyber, natural, weather, physical) and vulnerabilities that may affect the critical infrastructure of the Electrical Power Energy System (EPES), UCs serve as a basis for the integration of technologies and solutions which will be demonstrated in R²D² pilot sites.

The KPIs are identified and formulated to evaluate the success of the demonstrations of the UCs. The KPIs will be used to quantify and evaluate the integration and demonstration activities under SP6 and to elaborate on the replication and scaling-up of the project results within SP7.

- T2.1 Definition of business scenarios, UCs and requirements
 - This task defined the requirements needed for reaching the R²D² project objectives. Requirements are classified and prioritized according to the needs of the project and of the demonstrators. The requirements definition is an iterative process while identifying the needs of the different end-users (RSC, TSO, DSO, energy producers, etc.) and takes place in parallel with the UCs definition. The task specifies and describes in detail the R²D² use-cases associated with the integration of technologies and solutions to be demonstrated in R²D² pilots. UCs consider end-users' needs in the presence of cyber threats throughout EPES.
- T2.2 System architecture definition
 - This task defined the IT architecture of R²D² ecosystem, based on the requirements, scenarios, UCs and KPIs defined in the related tasks. This task formally analyses and further details the already identified scenarios to be demonstrated at each Demonstration Pilot Site, considering the operational constraints of each end-user.

- T2.3 KPI identification and monitoring preparation
 - During the project, specific KPIs are defined that could evaluate the success of the demonstrations throughout the EPES. The KPIs provided in this task are used to calculate the project impact and to elaborate on the replication and scaling-up of the project results.

2.3 STRUCTURE OF THE DOCUMENT

The structure of this document stems from the scope of the document, as presented in the previous section. Therefore, the document has the following structure:

Section 1 provides a table of contents.

In Section 2, a brief description of the purpose, scope and structure of the document is given.

Section 3 refers to the foundations of the R²D² project, with special reference to the basic methodologies, project goals and business cases.

Section 4 explains the methodology for creating use-cases, including the connection with Unified Modelling Language (UML) and relevant international standards, as well as the content of the form for defining use-cases. Also, this section explains use-cases development based on identification, definition, revision and finalization. This is followed by the presentation of use cases by products (work packages 3-6) with basic information, such as ID, name, link to business cases, short description, pilot site and list of actors. At the end of this part, a shorter analysis is given regarding the correlation of use-cases with tasks per work package and business cases.

Section 5 includes requirements, with a description of the methodology and the tools adopted for the requirements management.

Section 6 deals with the architecture of the R²D² solutions, following the Smart Grids Architectural Model.

Section 7 introduces the methodology for the definition of key performance indicators (KPIs), and their relevance to the R²D² products and tools. An analysis of the defined KPIs is also provided, highlighting their relevance to the aims and objectives of R²D².

Section 8 provides the conclusions.

The main part of the document ends with Section 9 References while annexes cover the completed forms for defining and revising all UCs, complete list and tables of requirements, SGAM diagrams and complete information about used KPIs.

3. R²D² FOUNDATIONS

3.1 OVERALL METHODOLOGY

This section describes the overall methodological approach adopted for the derivation of the business scenarios, UCs and end-user requirements of the R²D² project. The methodology also covers the interface of the specific task with other tasks that evolve in parallel and are significantly affected by its proceedings and outcomes.

The high-level task implementation methodology (Figure 1) comprises distinct, iterative, and interdependent steps. The individual but also combined outcome of these steps constitute the foundations of the R²D² solutions.

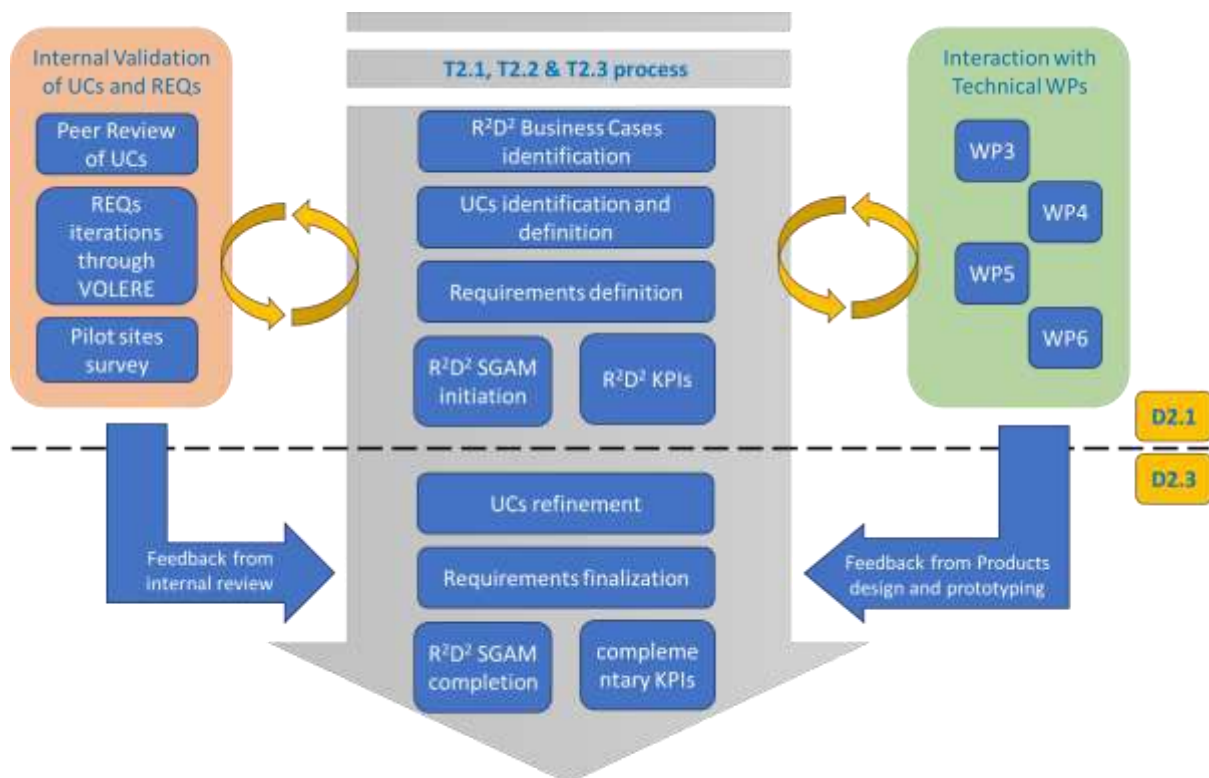


Figure 1 – Overall methodology for the R²D² foundations from tasks 2.1, 2.2 and 2.3

The process for the R²D² project foundation, is covered by tasks T2.1, T2.2 and T2.3, and the overall execution of the three tasks enable the correct and proper development of the R²D² products. As a matter of fact, whether they are three different tasks, they have been conceived as a unique activity with a common output, for a matter of integrity and coherence of the project's foundation.

The overall methodology is composed of two main iterative processes.

First iteration

The first iteration was carried out by the project month 10 and included the identification of the Business Cases, the definition of the UCs and the Requirements. All results of the first iteration were presented in [11].

The definition of R²D²'s Business Cases and UCs was the steppingstone to eliciting the business value behind the novel R²D² solutions. A thorough analysis of the project's high-level objectives, as in the Description of Action (DoA) was undertaken, along with a detailed study of R²D²'s defined objectives, in order to derive the outline of the business-oriented targets associated with all types of stakeholders across the electricity data value chain. At a lower level, for the definition of UCs and Requirements it was crucial the feedback from technical activities follow other iterative validation processes described in the next sections of this document. The requirements were defined and described following the VOLERE methodology (see Section 5).

After the UCs definition, it was possible to outline the R²D² architecture based on Smart Grid Architecture (SGAM) model [2]. In this iteration, three layers have been completed (namely business, components, and communication layers) through the inputs from scenarios and steps definition in UCs (See Section 6). These first three layers correspond to the logical and progressive sequence of the formal definition of the SGAM architecture, starting from an overall business perspective (business layers), mapping the available components (component layers) and establishing the communication flows across the components (communication layers). Once the products' designs were available, it was possible to include in this D2.3 report the information and functional layers as well.

In parallel with architecture-related activities, the final step of the process included the KPIs definition. For the first iteration, it was relevant to understand how the identified UCs are contributing to achieving the main R²D²'s KPIs from DoA (Section 7).

The output of the first iteration was included in deliverable [11].

Second iteration

In the second iteration of the project's foundation, the output of the first iteration [11] have been updated and completed.

Other activities from WP2 about pilot sites definition, and preliminary output from technical WPs (Deliverables D3.1, D4.1, D5.1 and D6.1) provided the necessary additional input to redefine, complete and refine the contents provided in this document. In particular, 20 UCs are revised after technical deliverables (design of the R²D² products) and the completion of the pilot sites definition (Deliverable 2.2) and additional one UC is created. The update of UCs bring to the revision of the previously established requirements, including definition of new requirements, and the completion of the missing layers of the SGAM architecture. Again, the requirements are finalised following the same VOLERE methodology as for the first iteration. Through the submission of the first version of the technical deliverables D3.1, D4.1, D5.1 and D6.1, it is also possible to redefine complementary KPIs aimed at verifying the performance of each tool and product. The integrated output of the first and the second iteration is included in this deliverable D2.3.

Terminology definition

Finally, to establish a common ground on the main outputs of this deliverable, Table 1 presents the terminology definition of business scenarios, UCs and requirements and the way they relate to the business context of R²D².

D2.3 – Requirements and Detailed Architecture Design

Table 1 – Terminology definitions

Item	Definition	Reference	Link to R ² D ² project
Business Case	“A business case provides justification for undertaking a project, programme or portfolio. It evaluates the benefit, cost and risk of alternative options and provides a rationale for the preferred solution.”	https://www.apm.org.uk/resources/what-is-project-management/what-is-a-business-case/#:~:text=Definition,rationale%20for%20the%20preferred%20solution.	Provide the landscaping of current business challenges but also of novel business opportunities that fall within the scope and positioning of R ² D ² .
Use Case	A use case describes how a user uses a system to accomplish a particular goal. It is a technique for capturing, modelling and specifying the requirements of a system.	Bittner, Kurt (2003). <i>Use case modelling</i> . Spence, Ian. Addison Wesley. ISBN 0-201-70913-9. OCLC 50041546.	Provide a break-down of R ² D ² 's business case; translate their objectives into distinct interactions and user journeys; and constitute the vehicle that transfers the business context into more technical terms to convey the R ² D ² vision.
Requirement	A requirement is a statement which translates or expresses a need and its associated constraints and conditions with the purpose to transform through their analysis the stakeholder, requirement-driven view of desired services into a technical view of a required product that could deliver those services	ISO/IEC/IEEE 29148:2011	Instantiate the R ² D ² 's UCs (and business innovation indirectly) into concrete needs for the development of the different components of R ² D ² 's tools and products.
Key Performance Indicators (KPIs)	“KPIs are the critical quantifiable indicators of progress toward an intended result. KPIs provide a focus for strategic and operational improvement, create an analytical basis for decision making and help focus attention on what matters most”	https://www.kpi.org/kpi-basics/	Apart from the typical definition of KPI concept in the business domain, in R ² D ² ' project KPIs will be also adopted to measure technical performance of the products and tools.

3.2 OBJECTIVES AND BUSINESS CASES

At the beginning of the project, the consortium defined seven Business Cases (BCs), in line with the project's objectives described in the DoA, as a matter of fact, they actually

coincide with them. The BCs can be considered as scenarios, with the aim of defining a framework within which to structure the needs of the project and model the most appropriate Use Cases. A description of each BC is below:

BC1: Contribute to the improvement of the overall security and resiliency in the power system

The main objective of R²D² is to improve the overall security and resilience of the electric power system through the multiple products developed within its framework. Thanks to a holistic and multidisciplinary approach R²D² will face the different categories of risks and vulnerabilities (whether natural or man-made) that may affect the normal operation and management of the EPES as a whole, including IT, OT and field equipment. As a result, a more secure operation of the system is expected to be achieved.

BC2: Model the impact of High Impact and Low Frequency (HILF) events on the power system in order to assess its resilience and determine the optimal operational planning measures and investments to enhance power system resilience.

R²D² will develop a novel toolkit of multi-temporal and multi-spatial static and dynamic cascading simulators for assessing and quantifying the effects of cascading events, including fast transient events. This will feed into machine learning-driven applications to assist the decision-making on operational planning measures, including the aggregated control of distributed energy resources contributing to the TSO-DSO resilience suite, and to optimization-driven approaches for resilience investment pathways and maintenance strategies.

BC3: Increase the cyber-security and cyber-resilience in OT and IT of the EPES

Increasing the cyber-security and cyber-resilience in OT and IT of the EPES through the adoption of novel digital tools and methodologies cooperating in a coordinated way, in order to monitor, mislead and detect attacks. R²D² will also develop a risk management tool to identify the security posture of the corresponding EPES components, to make sure that the appropriate security measures have been deployed. R²D² will improve the mitigation of cybersecurity risks by providing dynamic risk management services that will consider applicable existing and emerging threats and vulnerabilities and the peculiarities of the environment.

BC4: Enhance coordination, interaction, and information exchanges at the regional level between TSO-TSO and TSO-DSO during critical and emergency conditions

To enhance coordination, interaction and information exchanges at the regional level between Transmission System Operators (TSO) with the support of their Regional Security Centre (RCC), and between TSO and DSO, during critical and emergency situations in order to test and validate novel strategies and procedures for minimizing risks and exploiting the flexibility from RES to enhance the system resiliency (with environmental cascading effects).

BC5: Deliver a toolkit to improve the reliability of electrical assets and to contribute to the enhancement of the resilience of the network's components through advanced data-driven solutions and automated and robotic technologies

One of the aims of R²D² is to prioritize the adoption of advanced digital and automation technologies to improve the reliability of electrical equipment and assets and facilitate maintenance operations. The toolkit will be composed of different sub-tools based on machine learning and pattern recognition techniques being able to provide accurate estimation of the equipment conditions and time before failure. Through the adoption of



automated and robotic technologies, it will be possible to inspect assets and devices in an easier and faster way. This tool will help system operators and producer to check the actual condition of their physical infrastructure and equipment in order to prepare preventive countermeasures when a critical weather or natural event is forecasted or adopting/planning repairing actions once the event has happened.

BC6. Demonstrate project impact and replicability potential during the project and beyond the project activities

The project solutions will be demonstrated in four pilot sites in four different countries, involving all type of energy networks and complementary stakeholders, from big public DSOs and TSOs to LV customers, going through medium utilities and local energy communities, demonstrating higher impact and replicability potential and cooperation between system operators.

BC7 Contribute to the development of a shared knowledge

R2D2 will participate in the creation of shared knowledge through European system operators and stakeholders about the threats and vulnerabilities investigated in the project, the methodologies adopted, the solutions implemented, the benefits achievable for final users and, more in general, the best practices identified so far. To achieve such a vast objective, multiple actions will be implemented all across the project, including the setup of a repository to collect all information (events, procedures, results, analysis, etc.) from technical WPs to be shared with external stakeholders.

The consortium has defined the UCs based on the scenario depicted by each BC, therefore linking each UC to a specific BC. Nevertheless, given the complexity and, in some cases, the broad scope of certain UCs, a UC is more likely related to more than one BCs. Although UCs are introduced in the next section, a complete mapping of the BCs with the UCs is reported in

Table 6 (section 4.3.5), where it is possible to see how each BC (from 1 to 5) represents the reference for the UCs. The only BCs that do not correspond to any UCs activities are BC 6 and 7, which basically are addressed to cover other non-development aspects of the project about validation and dissemination.

4. USE CASES

4.1 INTRODUCTION

A use case represents formulated textual and visual modelling technique. These days use case modelling is associated with UML.

Unified Modelling Language (UML) is one of the most important modern development technologies [3]. UML has had a big impact on the software development industry.

UML is primarily a graphical language. Most of the elements of the language strictly refer to different diagrammatic techniques, while the text only describes them in more detail. Only certain parts of the language are relied upon for textual rather than graphic descriptions (this refers to use cases).

All UML diagrams can be divided into:

- Structural diagrams
- Behaviour diagrams

Structural diagrams describe the static structure of the software system and its parts. Structural diagrams include class diagram, object diagram, package diagram, composite structure diagram, component diagram, deployment diagram and profile diagram.

Behaviour diagrams deal with the dynamic nature of a software system. They describe the behaviour of individual objects or broader subsystems. Behaviour diagrams include use case diagram, activity diagram, state machine diagram, interaction diagrams (sequence diagram, communication diagram, timing diagram and interaction overview diagram).

So, we can see that use cases are just one type of UML diagram. Unlike other diagrams that are purely graphical (with the introduction of names for graphical elements), use cases contain extensive textual explanations that are crucial for understanding the technical solution described by UML diagrams.

Therefore, it was estimated that this project should be primarily based on the use of use cases as a tool for communication between future users and developers of the technical solution in question.

4.2 USE CASE METHODOLOGY

4.2.1 Introduction

Generally speaking, a use case is a method used in system analysis to identify, clarify and organize system requirements. The use case is made up of a set of possible sequences of interactions between systems and users in a particular environment and related to a particular goal.

In other words, the use case describes system functionalities in a technology-neutral way and identifies participating actors. Therefore, a method creates a document that describes all the steps taken by a user to complete an activity.

Depending on the level of decomposition of the system, the use cases can be at a higher or lower level of abstraction. When presenting the conceptual level of software, the aim is to describe the entire system with as few use cases as possible. For that matter, use cases are very abstract, and actually describe the use of the system by one type of user (so-called business use cases).

At lower levels of abstraction, one use case tends to correspond to one system user activity. As a lower limit of decomposition, it is usually required that a use case has a recognizable result.

Before starting a project, it should be decided upon the templates that are going to be used. In practice, it suffices to use two templates:

- Simple one with only a few properties for use cases that do not need to be worked out in detail (Casual version)
- More extensive one that has all properties that are relevant, for the other use cases (Fully Dressed version)

In this project, the Casual version was used in the preliminary phase of the project, while the Fully Dressed version is used for later stages and deliverables.

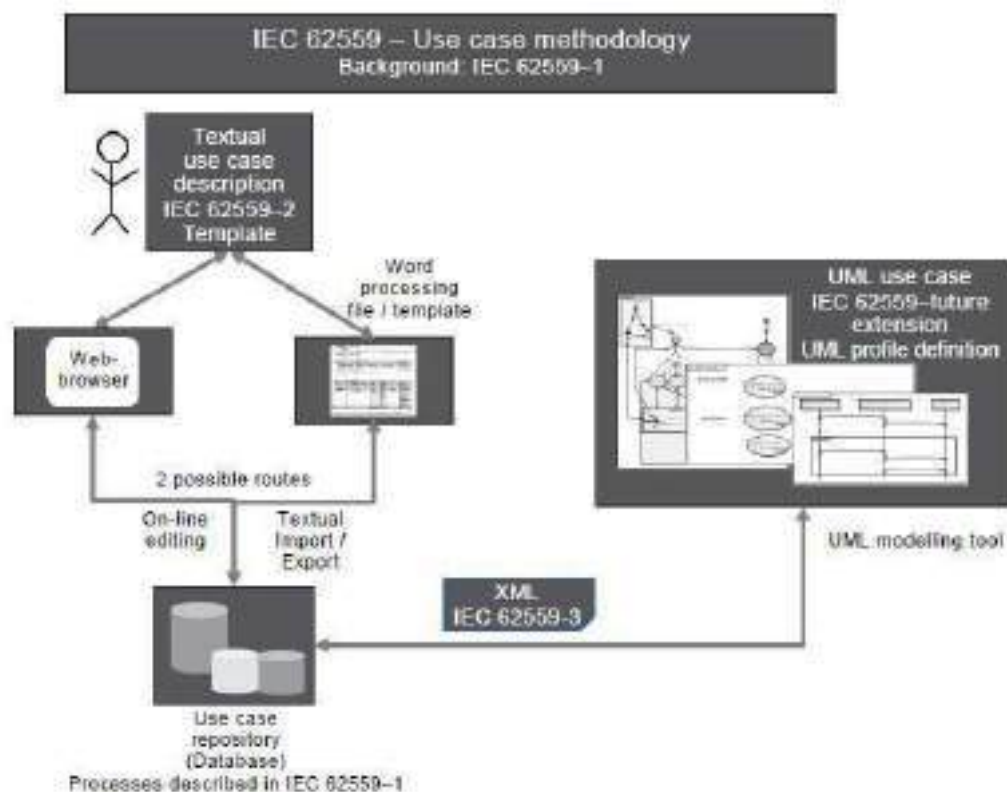


Figure 2 - IEC 62559 standard series [4]

This Project is based on the Use Case Methodology defined in IEC 62559-2:2015 [4]. The Use Case Methodology defines the structure of a use case template, template lists for actors and requirements, as well as their relation to each other.

In this IEC standards, a standardized template for the description of use cases is defined for various purposes like the use in standardization organizations for standards development or within development projects for system development.

This IEC standard was developed for general application in various domains and systems. Figure 2 provides an overview of the IEC 62559. The energy system/smart grid is used as an example in this document as it was one of the first usage areas for this use case template, but this general template can be applied in other usage areas different from energy systems as well (e.g. smart home or electro-mobility).

In this project, the creation of use cases will follow a deliberate and iterative process, which can be split into four main phases presented in Figure 3.



Figure 3 - Use case creation process

4.2.2 Use Case Identification

During the initial phase, the R²D² partners identified potential use cases and described some of the key characteristics, as follows:

- Main objective related to the use case
- Secondary objective related to the use case
- Related project products
- Use case author
- Use case responsible partner
- Possible Demonstration Pilot Site for use case demonstration

In addition, the use case author provided the rationale behind the use case.

Identification of the use case went through several iterations, after which a tentative list of use cases for definition was determined. R²D² partners discussed all proposed use cases during regular conference calls.

Based on the conclusions made, the use case identification list was updated, until there was a complete understanding between the R²D² partners.

It is important to note that care was taken that use cases must cover all tasks related to project products.

4.2.3 Use Case Definition

After an initial list of use cases was determined, each use case was defined using the use case form as defined in IEC 62559-2:2015.



D2.3 – Requirements and Detailed Architecture Design

To make the use case definition easier, some clarifications have been added to the form. The use case definition form consists of the following sections:

- Description of the use case
 - Name of use case
 - Use case ID
 - Area/ Domain(s)/Zone(s) – according to the rules of the SGAM diagram
 - Name of use case
- Version management
 - Version No.
 - Date
 - Name of author(s)
 - Changes
 - Approval status
- Scope and objectives of the use case
 - Scope (Brief description of the use case action perimeter)
 - Objective (Final successful outcome that completes the process described in the use case)
 - Related business case(s) – One or more of the following was chosen for R²D² use cases:
 - BC1. To contribute to the improvement of the overall security and resiliency of the Power System
 - BC2. To deliver a toolkit to model the impact of HILF events on the power system in order to assess its resilience and determine the optimal operational planning measures and investments to enhance power system resilience.
 - BC3. To increase the cyber-security and cyber-resilience in OT and IT of the EPES
 - BC4. To enhance coordination, interaction, and information exchanges at the regional level between TSO- TSO and TSO-DSO during critical and emergency conditions
 - BC5. To deliver a toolkit to improve the reliability of electrical assets and to contribute to the enhancement of the resilience of the network's components through advanced data-driven solutions and automated & robotic technologies
- Narrative of use case
 - Short Description – Description of the goal the use case is supposed to deliver.
 - Complete description – Detailed description of how stakeholders will accomplish a goal by using a system/process – some graphics can be used to support the description.
- Key Performance Indicators KPI
 - Detailed information on KPIs for all UCs is given in Section 7 and Annexes V and VI, so the usual data it includes (name, description and reference to mentioned use case objectives) is omitted in use case definition form attached in Annex I



D2.3 - Requirements and Detailed Architecture Design

- Use case conditions
 - Assumptions – Statements about what is out of scope for the use case
 - Prerequisites – Conditions specification that must hold true before the scenario of the use case starts
- Further information on the use case for classification/mapping
 - Relation to other use cases – The list of use cases that correlate with the use case
 - Level of depth – Use cases can be written at different levels of detail (high, medium, low).
 - Prioritisation – The priority of the use case with respect to the project, can be in the 1 (low) – 5 (high) range.
 - Generic, regional or national relation – Explanation of whether the use case is intended to be used nationally, regionally, or worldwide (generic).
 - Nature of the use case – Use cases can be written for different purposes: to describe a business process, to describe the functional requirements of a system or to document the design of a system...
 - Further keywords for classification – Keywords used in use case description relevant for use case classification.
- General remarks
- Diagrams of use case (UC SGAM diagrams are given in Annex IV, while other diagrams, such as algorithms and similar, are attached in UC definition form)
- Technical details
 - Actors
 - Grouping – Criteria/methodology/rules for grouping actors
 - Group description – Short explanation of actors' groups
 - Actor name – Name of a specific person, job title, company, tool, hardware, software...
 - Actor type – Actor type according to the European electricity market role model or other selected criteria
 - Actor description – Description of the actor's role according to the use case scenario
 - Further information specific to this use case – Any further information needed to clarify an actor's role in use case.
 - References (detailed reference information for all UCs is given in D2.2. deliverable, so the usual data it includes (references type, reference, status, impact on the use case, originator/organisation and link) is omitted in Annex I
- Step-by-step analysis of the use case
 - Overview of scenarios
 - Scenario name – Success scenario or exceptional scenario (extension) with the designation
 - Scenario descriptions – Short description of success scenario or exceptional scenario



D2.3 - Requirements and Detailed Architecture Design

- Primary actor – The primary actor is the stakeholder that interacts with the system to achieve a specific goal; the primary actor is often, but not always the one who triggers the use case
- Triggering event – Event or sequence of events that initiate the use case
- Pre-conditions – Conditions that must be met before the scenario can start
- Post-conditions – Conditions that must be met for a valid end of the scenario
- Steps – Scenarios
 - Step No – Ordinal scenario step number (1, 2, 3...)
 - Event – Event that triggers a scenario step execution
 - Name of process / activity – Name of process / activity executed in a scenario step
 - Description of process / activity – Short description of process / activity executed in a scenario step
 - Service – Service provided in a scenario step
 - Information producer (actor) – Actor (preferably type or name) producing the information
 - Information receiver (actor) – Actor (preferably type or name) receiving the information
 - Information exchanged (IDs) – ID of information exchanged in a scenario step – detailed information description is provided in section 'Information exchanged'
 - Requirement, R-IDs – ID of requirement for execution of this scenario step – detailed requirement description is provided in section 'Requirements'
- Information exchanged
 - Information exchanged, ID – ID of the information exchanged defined in section 'Steps – Scenarios'
 - Name of information – Name of the information exchanged in a scenario step
 - Description of information exchanged – Detailed description of the information exchanged in a scenario step
 - Requirement, R-IDs – Related requirement ID relevant for information exchange (in principle defined in section Steps – Scenarios')
- Requirements (full information about requirements is provided in Section 5 and Annex III, therefore use case definition form in Annex I contains only referenced to requirements ID as set in Volere platform, while requirement name and requirement description are omitted)
- Common terms and definitions
 - Term
 - Definition
- Custom information
 - Key
 - Value
 - Refer to section



Use case definition forms for all identified use cases are attached in Annex I of this Report.

4.2.4 Use Case Revision

All use cases were reviewed and validated by the end-users in order to be included in the final list of use cases. To carry out this revision, for each use case an auditor was selected.

To facilitate this activity, a use case revision form has been prepared that enables the use case revision in a standardized and unified manner.

This form consists of two parts. The first part of the use case revision form was completed by the use case author and covers the following questions, which served as guidelines to the use case auditor while revising a use case (the auditor was required to analyse the use case definition form in detail, and the use case revision form was designed to provide additional necessary information about the purpose of the use case, which was not included in the use case definition form):

- How innovative the use case is?
 - How important the use case is (if the use case is not innovative, is it necessary?)
- Does the use case align with the project environment (business scenarios, objectives and products)?
- Is the use case in line with general EU market principles?
- Is this already done at the ENTSO-E level or in some regions?
 - If already done, why the use case is needed?
- What KPIs might be assigned to the use case?
- Is the use case scalable?
- Is the use case replicable?
- Does the R²D² consortium have sufficient resources to implement and demonstrate the use case (manpower, time, knowledge, available Demonstration Pilot Site, needed equipment...)?

The second part of the form was completed by an auditor (WP2 selected partner). He provided an overall assessment based on the following questions:

- Do you think the use case definition is done correctly (refers to use case definition form)?
- Do you think the additional information about the use case (refers to section 1 of this form) is plausible?
- Do you think the use case should be carried out as part of the R²D² project?
- Do you have any recommendations to improve use case definition?

For each question, the auditor provides a proper explanation and furthermore recommendations to improve the use case.

In addition to filling out the mentioned form, the auditor was obliged to study the use case definition form in detail and enter comments and suggestions for improvements.

During the audit, it was common for the use case author and the auditor to communicate intensively until a common understanding was reached.

The use case revision form is attached in Annex II of this Report.

4.2.5 Use Case Finalization

The use case revision was mainly focused on validating the rationale and the interactions between actors and solutions behind each use case.

Even though the end of the use case revision process provides a final list of use cases, a certain set of activities had to be carried out in order for the list of use cases to be finalized and included in project deliverables.

These activities included the final synchronization of the actors involved with the agreed list of R²D² actors (especially those that represent certain parts of project products), formatting changes, use case re-numbering, adjusting use case priorities, etc....

For instance, to finalize some use cases, it was necessary to start work on the project product WPs (WP3-WP6), that is, to define at least the initial technical specification in cooperation between the creators of use cases and the creators of the products (developers). It is this communication that led to a redefinition of use cases, primarily from the point of view of product creators to respond to defined requirements. Therefore, it is quite normal that by the end of Work Package 2 there are certain changes in already defined use cases.

Besides, the development of the technical specification enabled the creators of use-cases to define requirements more clearly, i.e. to redefine existing requirements and add new ones. The use case definition form suggests establishing a connection between technical requirements and scenario steps and/or information exchanged among use case actors. These requirements are entered in detail in the Volere platform, while the ID of the requirement generated by the Volere platform is entered in the use-case definition form.

The next reason for redefining the use case was the completion of the D2.2 report on Pilot Sites in month 12 of the project. In this report, the ability of the Pilot Sites to provide all support actors (that do not belong to the R2D2 product such as servers, communication links...), that is to enable the exchange of all foreseen information in the required format and according to certain protocols, was examined. If, however, the lack of such actors on the Pilot site was detected, it was necessary to redesign the use case in order to harmonize it with the demonstration capabilities of the Pilot site.

Also, with the progress of the project's products design and after the investigation of the Pilot Sites, it was possible to have a complete picture of the information to be exchanged and create the information layer of the SGAM architecture. As some inconsistencies were observed in the definition of use cases, these inconsistencies were eliminated through use-case redefinition.

And finally, with the overall progress of the project, it was also possible to better look at the remaining available resources and redistribute them according to priorities. In some cases, this has led to the cancelation of certain actors, which have been replaced by existing services provided by the Internet and communication via e-mail and the like and this also was the reason for use-case redefinition.



So to conclude, 20 use cases were modified to a greater or lesser extent after the preliminary report [11]. These changes specifically refers to the following aspects:

- Use cases scenarios and scenario steps
- Involved actors
- Information exchanged between actors
- Requirements for technical specification of the actors and the information exchanged between them

Also, 2 new use cases were created (UC39 and UC40).

4.3 USE CASES ANALYSIS

This section is devoted to the analysis of the created use cases, in terms of their correlation with the project foundations.

The R²D² project proposal defines a palette of complementary solutions synthesised into four products:

- “Multi-risk assessment framework for power system” (P1 – C3P0)
 - C3P0 contributes to a systematic, disciplined, and repeatable approach to evaluating an energy system security strategy. This product will be developed in WP3.
- “Resilience suite for TSO & DSO” (P2 – IRIS)
 - IRIS intervenes when coordination between system operators is needed for security reasons. This product will be developed in WP4.
- “Prevention Systems For Energy Infrastructures Security” (P3 – PRECOG)
 - PRECOG provides a cybersecurity framework to OT and IT. This product will be developed in WP5.
- “Enhanced Assets Maintenance And Management Toolkit” (P4 – EMMA)
 - EMMA contributes to the reliability of the physical assets and expedites a faster grid recovery. This product will be developed in WP6.

The full list of UCs is presented below:

- UC1 – Improvement in overhead power lines inspection and maintenance using IA applied to UAV-captured images and data
- UC2 – Substation component status of health calculation based on SCADA measurements and DGA data
- UC3 – Malfunctioning detection of PV panels through autonomous UAV image acquisition
- UC4 – Detection of NTL through SCADA and AMI data, from a selected portion of the distribution grid
- UC5 – Automated ranking intervention of assets and optimal scheduling (including routing) of intervention workforce to perform maintenance task



D2.3 – Requirements and Detailed Architecture Design

- UC6 – Substation components degradation detection by analysing images (conventional & thermal)
- UC7 – Enhancement in DER control and management systems to participate in flexibility procurement schemes for DSO and TSO to improve network operation security
- UC8 – Outage planning optimization
- UC9 – Automation of power quality parameters emission levels calculation
- UC10 – Improving of LV network observability based on billing metering system by means of secure interface with SCADA-ADMS system
- UC11 – DSO-TSO congestion and power quality coordination in application of system services
- UC12 – Emergency & Restoration – Over-Frequency Protection module
- UC13 – Cost sharing of remedial actions with cross-border impact
- UC14 – Automation of transient stability calculations for operation planning purposes
- UC15 – TSO-DSO cooperation in Individual Grid Model creation
- UC16 – Phasor angles monitoring and prevention of instability
- UC17 – Outage coordination and automated creation of topology files for Individual Grid Models
- UC18 – Optimization of PMU installation points
- UC19 – Emergency & Restoration – System Split module upgrade
- UC20 – Physical security enhancement in core network components (primary substations)
- UC21 – Remedial Action Automation
- UC22 – Prevention and mitigation of cascading effects in case of extreme weather events
- UC23 – Cooperative crisis handling in case of cascading effects
- UC24 – Cyber Security Risk assessment on EPES infrastructure
- UC25 – Dynamic Cyber-Risk Status Evaluation considering existing technical vulnerabilities
- UC26 – Cyber Threat Intelligence knowledge collection/sharing with external sources
- UC27 – Monitor communications behaviour of newly deployed components in an EPES staging environment
- UC28 – Adapt/Develop EPES specific vendor management & suppliers' audit practices
- UC29 – Event simulator of a progressing wildfire and assessment of its impact on distribution system (evaluation of line outages, quantification of spatiotemporal load shedding)



D2.3 - Requirements and Detailed Architecture Design

- UC30 – Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling
- UC31 – DLR integration with IGMs and SCADA/EMS
- UC32 – Planning and operation for a resilient multi-energy Microgrid
- UC33 – Detection of anomalies associated with cybersecurity through the characterization of traffic in the perimeter, levels of control and supervision, operation and in physical environments
- UC34 – Pattern detection and correlation with information from other cyberattacks in order to detect potential threats
- UC35 – Upstream studies to validate the use of TSO/DSO means during crisis situations (OpFab, PowSyBl)
- UC36 – Validation of network model integrity
- UC37 – Energy data tokenization
- UC38 – DSO grid balancing data tokenization
- UC39 – Innovative solution for OPDE Risk Register
- UC40 – IoT data security enforcement

Each product should be composed by several modules loosely coupled among them, to be developed in a dedicated task and addressing one or more specific core-functionalities. These products are intended to solve the difficulties faced by EPES when dealing with physical (including, man-made and equipment), cyber, weather, and natural threats, by enhancing the grid's resilience through tailored solutions supported by machine and human learning, having the following drivers as the central part of their design, development and deployment in order to provide world-class solutions.

The following subsections provide an overview of all created use-cases for each task, providing basic information about the use-case, which refers to the following:

- Use case ID and title
- Use case correlation with product task and business case
- Use case short description
- Use case demonstration pilot site
- Use case R²D² tools (actors)

4.3.1 WP3 (C3P0) Use Cases

C3P0 product is planned to be designed through the following tasks:

- T3.1 Security assessment through advanced IT technologies – Cyber Risk Assessment Tool
- T3.2 Dynamic Cyber-Risk Status Evaluation
- T3.3 Spatial and Temporal Modelling and Quantification of Cascading Physical Events
 - T3.3.1 Spatial and temporal event and fragility modelling



D2.3 – Requirements and Detailed Architecture Design

- T3.3.2 Cascading modelling and quantification
- T3.4 Resilience-driven investment and operational planning to mitigate or prevent cascading effects
- T3.5 Operation and Planning of Advanced Multi-Energy micro-grids for Enhancement of Resilience
 - T3.5.1 Advanced control of mobile power sources in enhancing micro-grids resilience
 - T3.5.2 Resilience-driven optimal design of micro-grids
- Task 3.6 Knowledge sharing – Cyber Threat Intelligence and cascading events

The UCs defined under C3PO product are reported in Table 2:

Table 2 – UCs from C3PO (WP3)

No.	Task	UC ID	Title	BC	Pilot site	Actors
1	T3.1	UC24	Cyber Security Risk assessment on EPES infrastructure	BC3	Greece	System Operator, Cyber Security Experts, C3PO Cyber Risk Assessment Tool
			Short description: The aim of this use case is to demonstrate the use of the developed C3PO Cyber Risk Assessment Tool (T3.1), and its capability to identify and assess risks, measure risks levels and assess the security posture of the target environment, propose risk mitigation measures, including the developed R ² D ² components.			
2	T3.1	UC39	Innovative solution for OPDE Risk Register	BC3 BC4	Serbia	OPDE Risk Register, Party user, ENTSO-E information security body user and Hosting administrator

No.	Task	UC ID	Title	BC	Pilot site	Actors
			Short description: In order to protect operational planning data from cyber-attacks, ENTSO-E developed OPDE platform. Information security protection of OPDE platform is based on the document "OPDE/ATOM Security Plan", where a set of specific information security measures is defined. Each year independent external auditor is reviewing the implementation status of these information security measures at TSO and RCC operational environment (common name for TSOs and RCCs is in this context is Party). Each Party is obligated to provide update of existing information security risks and submission of new risks based on the independent auditor's report. This process of submission and update of information security risks related to the OPDE platform is currently performed based on shared secured repository and exchange of .docx templates, which creates delay in risk review process and perplex communication between ENTSO-E information security bodies and Parties. This UC is focused on developing specialised IT tool that could support and improve monitoring and communication during risk treatment process that is currently established on the ENTSO-E level. OPDE Risk Register will be based on the following functionalities: 1) Enable entry form for risk submission and modification; 2) Display all submitted risks and their information based on the "need to know" principle on centralised place; 3) Enable fast, secure and simple communication between users on the specific risk; 4) Log all changes of data in the system.			
3	T3.2	UC25	Dynamic Cyber-Risk Status Evaluation considering existing technical vulnerabilities	BC3	Greece	System Operator, Deep Learning Data Analytics Software, Cyber Threat Intelligence Collection/Sharing System, Vulnerability Assessment Tool, Cyber Security Experts
			Short description: The C3PO Dynamic Cyber Risk Evaluation Tool will facilitate the dynamic and close to real-time threat detection and mitigation as well as vulnerability management in the targeted IT/OT environment, by (proactively) assessing associated risks for the organization's target environment.			
4	T3.3	UC22	Prevention and mitigation of cascading effects in case of extreme weather events	BC1, BC2	Greece	EMMA GIMAN, C3PO Cascading simulators, operational network planning modules, DSO, Weather service provider, SCADA/DMS
			Short description: This Use Case focuses on the enhancement of the grid's resilience under extreme weather events. The analysis of the network's current state, along with potential cascading effect indicators calculation that derive from a possible extreme weather event, are necessary for the R ² D ² tools to propose the optimal corrective actions for the minimization of potential major outages. A series of actions, like network flexibility capability and reconfiguration actions are utilised for the grid's resilience enhancement. Finally, a faster restoration of outages can be achieved, through the optimal workforce allocation in the critical parts of the network.			

No.	Task	UC ID	Title	BC	Pilot site	Actors
5	T3.3	UC29	Event simulator of a progressing wildfire and assessment of its impact on Distribution System	BC1	Greece	C3PO
			Short description: The purpose of this Use Case is to expand T3.3 event simulator which is mainly focused at windstorms and fragility-based modelling to also include the modelling of wildfire events. The presented scheme will assess the impact of wildfire events on distribution system (such as line outages, spatiotemporal load shedding, wildfire's trajectory assessment, etc.) by using a stochastic programming structure to capture the uncertainties. The goal of this Use Case is to provide an optimal operational scheme and corrective actions for enhancing distribution system resilience considering the varying conditions during the spread of a progressing wildfire.			
6	T3.4	UC23	Cooperative crisis handling in case of cascading event	BC1, BC2, BC4	Greece	C3PO Cascading simulators, operational network planning modules, TS0, DS0
			Short description: This Use Case focuses on the upward or downward signal/alert that must be exchanged between the system and the network operator, in order to prevent a potential cascading effect caused by a failure in the interconnection point between system and network.			
7	T3.4	UC30	Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling	BC1, BC2	Greece	Distribution system management, System Operator, Generator power forecaster, Load power forecaster, Restoration service provider, Repair crew
			Short description: The use case aims to enhance distribution system resilience by determining the optimal operation and restoration activities after the occurrence of catastrophic events. The integrated operation and restoration solution provided by the use case includes a flexible microgrid formation scheme to separate the faulted system into multiple microgrids, a sustainable microgrid scheduling scheme to dispatch the stochastic power of distributed generators and electrical loads, and a frequency-aware restoration scheme to dispatch repair crews and pick up loads.			

No.	Task	UC ID	Title	BC	Pilot site	Actors
8	T3.5	UC32	Planning and operation for a resilient multi-energy micro grid	BC1, BC2, BC5	Greece	Micro grid central controller, Multi-energy micro grid, Mobile power source, Mobile energy storage system, Mobile emergency generator, Electric vehicle, Repair crew, Distributed energy resources, Transportation operator
			Short description: The use case aims to enhance the system resilience of a multi-energy micro grid by planning and operating the mobile sources. Specifically, a three-level defender-attacker-defender model is developed to plan the optimal sizing and pre-positioning of mobile sources in networked micro grids with decentralized control; an advanced learning-based algorithm is developed to control the routing and scheduling of mobile sources in a coupled energy-transportation network to maximize the load restorations of a multi-energy micro grid.			
9	T3.6	UC 26	Cyber Threat Intelligence knowledge collection/sharing with external sources	BC4	Greece	System Operator, C3PO CTI Tool (Cyber Threat Intelligence Collection/Sharing System), R ² D ² Defence Mechanisms, CTI Community (e.g. EE-ISAC), CTI Sources
			Short description: The aim of this use case is to demonstrate the capabilities of the Cyber Threat Intelligence CTI Tool in collecting, correlating, producing added-value data ready to be ingested by security appliances and further disseminating CTI.			

4.3.2 WP4 (IRIS) Use Cases

IRIS product is planned to be designed through the following tasks:

- T4.1 Optimal resources coordination management for TSOs and DSOs during crisis
- T4.2 Emergency and restoration
- T4.3 Multi-energy TSO-DSO planning coordination

The UCs defined under IRIS product are reported in Table 3.

D2.3 – Requirements and Detailed Architecture Design

Table 3 – UCs from IRIS (WP4)

No.	Task	UC ID	Title	BC	Pilot site	Actors
1	T4.1	UC11	DSO-TSO congestion and power quality coordination in application of system services	BC1, BC4	Slovenia	Flexibility procurement system (Flex server), SCADA/ADMS system, RTUs, Meters, TSO, DSO, Aggregator, Balance group responsible party
Short description: DSO and TSO coordinate their activities in case of congestion or power quality issues in the network and consequently imposed limitations in ancillary service availability restrictions in distribution network.						
2	T4.1	UC35	Upstream studies to validate the use of TSO/DSO means during crisis situations	BC1, BC4, BC5	Serbia	DSO, TSO, Power flow software, IRIS Communication platform
Short description: The aim of this UC is to enhance the TSO/DSO coordination by allowing the validation of remedial actions from both sides that could be implemented then within real time operations. The expected final outcome is a common platform where TSO and DSO can exchange network models and related inputs (for instance, remedial actions proposal) and validate them in this platform for real time use.						
3	T4.2	UC7	Enhancement in DER control and management systems to participate in ancillary services procurement schemes for DSO and TSO to improve network operation security	BC1, BC5	Slovenia	SCADA / ADMS system (DSO), SCADA system (DER, RES), Flexibility procurement system (Flex server), RTUs, Meters
Short description: It is becoming necessary for DER to take over certain level of ancillary services including emergency actions. However, DER are limited in their ability when compare them with conventional energy sources. This UC will demonstrate, how DER and flexibility can fulfil these tasks.						
4	T4.2	UC12	Emergency & Restoration - Over-frequency protection module	BC1	Serbia	TSO, Producer, over-frequency protection module (OFPM), SCADA/EMS system
Short description: The Emergency & Restoration - Over-frequency protection module (OFPM) is designed as a replacement for the missing or insufficient controllers on generating units in the power system which can operate in limited frequency sensitivity mode – over-frequency (LFSM-0).						

D2.3 - Requirements and Detailed Architecture Design

5	T4.2	UC16	Phasor angles monitoring and prevention of instability	BC1	Serbia	TSO, SCADA/EMS, PMU
Short description: The possible occurrence of transient instability is monitored through two PMUs, where one is installed in the production centre and the other is installed in the consumption centre. When the critical angle difference is reached, the SCADA or WAMS system activates an alarm, after which the operators in the competent control centre should apply a re-dispatching of the active power injections into the network, which will preserve the stability.						
6	T4.2	UC18	Optimization of PMU installation points	BC1	Serbia	TSO, IRIS OPP (Optimal PMU Placement) Application
Short description: The optimization of PMU installation points means the determination of the minimum number of buses in the system (substations, power facilities etc.) where PMU devices need to be installed in order for the given power system to be fully observable.						
7	T4.2	UC19	Emergency & Restoration - System Split module	BC1	Serbia	Micro grid central controller, Multi-energy micro grid, Mobile power source, Mobile energy storage system, Mobile emergency generator, Electric vehicle, Repair crew, Distributed energy resources, Transportation operator
Short description: The Emergency & Restoration - System Split module shall be used to detect system split and coordinate TSOs and RCC during system stabilization and reconnection.						
8	T4.2	UC 21	Remedial Actions Automation	BC1, BC4	Serbia	TSO, Producer, SCADA/EMS system, Power Flows tool, Remedial Action tool
Short description: Transmission element overload is detected in real-time contingency analysis or when a disturbance has already occurred. In this case, the RA automation tool matches the element overload with predefined lists of RAs and defines a possible solution. After confirmation by the Control Centre operator, the appropriate signals are sent to the SCADA system to perform selected RAs.						

9	T4.3	UC 15	TSO-DSO cooperation in Individual Grid Model creation	BC1, BC4	Serbia	TSO, DSO, TSO-DSO communication platform, Distributed Generation (DG) Database, Load and RES forecasting tool
Short description: In order to create more accurate IGMs, it is necessary to appreciate the production of power plants at the distribution level. Instead of forecasting the power flow at the TSO-DSO interface, it is better to forecast and model the distribution load and the distributed generation separately.						

4.3.3 WP5 (PRECOG) Use Cases

PRECOG product is planned to be designed through the following tasks:

- T5.1 Identification and authentication of energy IoT and edge devices
- T5.2 Energy tokens and trading certificates security
- T5.3 Cybersecurity Events Management tools
- T5.4 Deep learning data analytics for security
- T5.5 Device origin and supply chain

The UCs defined under PRECOG product are reported in Table 4.

Table 4 - UCs from PRECOG (WP5)

No.	Task	UC ID	Title	BC	Pilot site	Actors
1	T5.1	UC36	Validation of network model integrity	BC1, BC3	Serbia	TSO, RCC, Tool for IGM creation, Shared repository, Internal repository, Merging tool
Short description: In order to improve network model cybersecurity, TSOs and RCCs could use KSI Blockchain technology to create KSI signature file, which represents unique cryptographic proof that protects integrity, signing time and signing identity of the network model. Confidential network model is created by file producer, signed, and forwarded to the file receiver together with KSI signature file, which can be then used to solve problems of integrity, provenance, security, immutability, and audit. File receiver uses proofs to validate the model to ensure that it is original and not tampered or changed (accident, malicious change, bit flip, corruption, etc). Even if a single bit in data or in proof has been changed then verification would result in error with corresponding message, allowing the file receiver (or whoever performs verification) to start an investigation.						

D2.3 – Requirements and Detailed Architecture Design

No.	Task	UC ID	Title	BC	Pilot site	Actors
2	T5.1	UC40	IoT data security enforcement	BC1, BC5	Greece	DSO, meter, tokenization tool
<p>Short description: This UC will concentrate on the analysis and enhancement of the tasks related to the IoT devices management, with the focus on the enforcement of the security without breaking the IoT paradigm. To test this UC part, a subsystem of the Greek pilot that use IoT technologies have been selected. This subsystem is composed by some Smart meters deployed across Xanthi and a control centre that receive its measurements. The data is exchanged in a IoT fashion, using MQTT protocol. These data include the real time electrical measurements and the hourly consumption profiles. The UC will change the processes related to the consumption profile data exchange using MQTT between the Smart meters and the IoT control centre. The idea will be to use a mechanism of tokenization of the data 'at the edge' (where it is read, before sending it), and use this token data to check the integrity at the control centre upon reception of data. Any data change or corruption happened during the transmission will result in the rejection of the data received.</p>						
3	T5.2	UC37	Energy data tokenization	BC1, BC5	Greece	DSO, Tokenization tool (PRECOG), DSO data server
<p>Short description: Collected energy measurements data from telemetered clients (AMI - smart meters) and SCADA systems are stored in DSO's internal databases. Measurement interval varies from 15 to 30 minutes depending on measurement point. Collected data is stored for at least a couple of months to several years depending on data type and governing regulations. Data is stored for plenty of purposes, such as analytics, or even billing verification. Consumption data provided by AMI, give the network operator the ability to have increased observability over the power consumed by the customer, and thus contribute to the reduction of fraudulent behaviours. The data from smart meters can also be used by network operators for the utilisation of potential flexibility and demand side management, or even for the participation of a customer to a local flexibility market. Finally, data from SCADA are of utmost importance for the DSO, as power flow analysis over the MV lines and possible necessary remote control commands are strongly dependent on them. It is crucial for DSO to have absolute trust in stored data to perform aforementioned activities and to take decisions based on the results. Blockchain technology is used to deliver the added trust factor for the collected and stored data by applying data registration in blockchain (data itself is not stored on blockchain, instead tokens are issued) and provenance of data registrations (each data entry from specific measurement point is linked together) making the data entries immutable and verifiable, periodically and before use.</p>						
4	T5.2	UC38	DSO grid balancing data tokenization	BC1, BC3	Slovenia	DSO, Tokenization tool (PRECOG), DSOs internal database, Balancing data system

Short description:

Slovenian pilot collects consumption, production and energy quality data and stores it in internal data storage. Energy quality is being assessed periodically and in case of intervention requests to either decrease or increase energy production or balancing is generated and sent out to grid participants. This data is then used for business related activities according to the request by DSO. In that situation, it is important for anyone to trust the data and to be sure the provided data is authentic and has not been changed (by error, intentional, mistake or cyber-attack). GUARD offers tokenization technology that creates unique cryptographic proofs that protects published data integrity, signing time and origin.

5	T5.3	UC10	Improving of LV network observability based on billing metering system by means of secure interface with SCADA-ADMS system	BC1	Slovenia	DSO, active consumer (prosumer), Distributed energy resources, SCADA / ADMS system, Flexibility system, Communication gateway, RTUs
---	------	------	---	-----	----------	---

Short description:

The aim of this use case is improvement of LV network observability and consequently system security and quality of supply based on billing metering data used in SCADA/EMS system by means of secure interface between both systems (billing and SCADA).

6	T5.3	UC33	Detection of anomalies associated with cybersecurity through the characterization of traffic in the perimeter, levels of control and supervision, operation and in physical environments	BC1, BC3	Serbia	CISO operator, DSO, TSO, RCC, System Operator, Carmen product (PRECOG)
---	------	------	---	----------	--------	--

Short description:

The goal of this use case is to monitor EPES to detect advanced threats. The monitoring system from a cybersecurity landscape will correlate the perimeter, control and supervision, operation and environment levels by collecting data from sensors, critical equipment and information systems, both structured and unstructured, to detect anomalies that may be capable of causing events, such as blackouts, effects on human health, loss of supervision, unmet demand, interruptions of operations and communications at different levels of national and transnational interconnected systems.

7	T5.4	UC34	Pattern detection and correlation with information from other cyberattacks in order to detect potential threats	BC1, BC3	Serbia	CISO operator, DSO, TSO, System Operator, Carmen product, Intelligent Cybersecurity Module, Firewall
Short description: Development of an intelligent module capable of characterizing different cyber threats based on the information collected from the different parts of TSO/DSO/RCC by the various Cybersecurity tools deployed in the system. The intelligent module will make use of various ML algorithms and techniques for calculating a similarity degree between a potential threat and previously seen threats, so that the Cybersecurity team of the TSO/DSO receives an alarm when the above mentioned similarity is high enough.						
8	T5.5	UC27	Monitor communications behaviour of newly deployed components	BC3	Greece	TSO/DSO, Sandbox Tool software, Communications Monitoring System (SIEM), Deep Learning System, Blockchain software
Short description: The aim of this use case is to demonstrate the capabilities of the “Sandbox Tool” of the PRECOG Supply Chain Assessment Toolkit (T5.5 - Device Origin and Supply Chain Toolkit), and its ability to monitor the communication of newly deployed components, and to use them to classify them as safe or unsafe prior to deployment in a production environment.						
9	T5.5	UC28	Adapt/Develop EPES specific vendor management & suppliers' audit practices	BC3	Greece, Spain, Slovenia, Serbia	TSO/DSO, EPES representative, Vendors'/Suppliers' representatives, Self-Assessment tool
Short description: This use case aims to demonstrate the use of the EPES specific vendor management & suppliers' audit practices to evaluate current practices and propose necessary enhancements.						

4.3.4 WP6 (EMMA) Use Cases

EMMA product is planned to be designed through the following tasks:

- T6.1 Equipment inspection through autonomous images acquisition
- T6.2 Optimal Asset management
- T6.3 Resource management in case of critical events
- T6.4 Maintenance coordination and planning

The UCs defined under EMMA product are reported in Table 5

D2.3 – Requirements and Detailed Architecture Design

Table 5 – UCs from EMMA (WP6)

No.	Task	UC ID	Title	BC	Pilot site	Actors
1	T6.1	UC1	Improvement in overhead power lines inspection and maintenance using IA applied to UAV-captured images and data	BC1, BC5	Spain	EMMA ARGOS, UAV inspection operator, UAV, System Operator
			Short description: UC01 is aimed at automatically and autonomously inspecting through UAV the overhead lines and identifying different phenomena and anomalies that might compromise the integrity of the overhead lines. The anomalies to detect depends on the payload the UAV will be equipped and the configuration of the analytic processes.			
2	T6.1	UC2	Substation component status of health calculation based on SCADA measurements and DGA data	BC1, BC5	Spain, Greece, Slovenia	EMMA DYML, SCADA, System Operator
			Short description: The UC02 will test the effectiveness of EMMA tool to detect degradation or malfunctioning in different substation components and supporting preventive and corrective maintenance. The detection will consider the analysis of continuously available SCADA data as well as data obtained periodically from the field (as in the case of transformer temperature and DGA measurements acquired through the Gas Chromatography Transformer Oil Analyser for maintenance).			
3	T6.1	UC3	Malfunctioning detection of PV panels through autonomous UAV image acquisition	BC1, BC5	Greece*	EMMA ARGOS, UAV inspection operator, UAV, Producer
			Short description: UC03 aims at detecting anomalies in PV panels using deep learning techniques analysis on imagery data captured by autonomous UAV vehicles.			
4	T6.1	UC6	Substation components degradation detection by analysing images (conventional & thermal)	BC1, BC5	Spain, Greece	EMMA ARGOS, DSO, Thermal camera, Robot Inspection, Inspection operator

			Short description: This use case is based on the acquisition and processing of optical and thermal images at substations to detect potential anomalies, failures and security menaces. Through thermal and optical cameras properly positioned or captured by inspection robots, the automatic detection of electric defects in selected components will be verified as well as events that may affect the security of the installation.			
5	T6.1	UC20	Physical security enhancement in core network components (Primary HV/MV Substations and Secondary MV/LV substations)	BC1	Greece	EMMA ARGOS, Surveillance cameras, Sensor devices, SCADA/DMS
			Short description: This UC focuses on physical substation security enhancement through the installation of equipment on either HV/MV or MV/LV substations. In case of a vandalism/theft attack to primary or secondary substation infrastructure, the DSO could be instantly notified by surveillance or metering equipment and proceed to the necessary actions. Moreover, in the event of a physical phenomenon or a natural disaster, which may affect the primary or secondary substation infrastructure, the installation of the aforementioned equipment could lead to the faster mitigation of possible damage to critical substation components, as well as to quicker power restoration.			
6	T6.2	UC4	Detection of non-technical losses through SCADA and AMI data, from a selected portion of the distribution grid	BC1, BC3	Spain, Slovenia	EMMA ETER, Advanced metering infrastructure, SCADA, System Operator
			Short description: This UC is aimed at detecting non-technical losses in distribution grids. UC covers intrusion detections from a cyber perspective and from an equipment perspective (through firmware integrity), so this UC covers potential physical tampering on the metering and electric energy thefts.			
7	T6.3	UC5	Automated ranking intervention of assets and optimal scheduling (including routing) of intervention workforce to perform maintenance task	BC1, BC2, BC3, BC5	Greece	EMMA GIMAN, System Operator

			Short description: This UC aims at generating a ranking intervention of assets considering the failure criticality, probability and consequences. Based on this ranking, individual maintenance tasks for the identified asset interventions are created and scheduled for being carried out by the workforce, prioritizing the most critical ones according to the different criteria and reducing the time wasted travelling.			
8	T6.4	UC8	Outage planning optimization	BC1	Serbia	TSO, Outage planning participant (Distributor, Producer), EMMA Outage Planning Optimization tool, EMMA communication platform, Outage planning server, Grid Model server
			Short description: This use case defines an Outage Planning Optimization (OPO) process on the basis of which a TSO can decide whether all requested outages in a given period can be approved, i.e. which requested outages cannot be accepted (and must be rescheduled) from the point of view of transmission grid operation security. The Outage Planning Optimization process is organized in three time frames: yearly, quarterly and weekly. In each time frame (interval), a TSO must coordinate and optimize outage requests and outage planning.			
9	T6.4	UC9	Automation of calculation of emission levels of electricity quality parameters	BC1, BC4	Serbia	TSO/DSO, EPES representative, TSO, Grid Model Server, Power Quality Server, EMMA Power Quality Emission Levels (PQEL) Application
			Short description: The Automation of calculation of emission levels of electricity quality parameters will be used in the connection process (for the purposes of compliance simulation checks), as well as in permanent operation (in the compliance testing/monitoring process). The calculation of emission levels according to the relevant IEC standards is very complex and requires the development of a software application.			
10	T6.4	UC13	Cost-sharing of remedial actions with cross-border impact	BC1, BC4	Serbia	TSO, RSS, EMMA RA cost-sharing software, EMMA communication platform, Power flow software, Electronic Highway
			Short description: Cost-sharing methodology for the remedial actions (RAs) costs with cross-border impact between transmission system operators (TSOs) is one of the most important mechanisms applied in the coordinated regional cross-border capacity calculation and regional operational security coordination. The cost-sharing methodology (CSm) is used in the Coordinated Regional Operational Security Assessment (CROSA) process after optimizing remedial actions (RA) at the regional level. This methodology is necessary to define the reallocation of RA costs (and revenues) after activation of RAs in national balancing mechanisms. This methodology relies on strong socialization of RA costs between involved TSOs.			

11	T6.4	UC14	Automation of transient stability calculations	BC1	Serbia	EMMA Transient Stability Calculations (TSC) Script, TSO
			Short description: With the increase in the share of RES in the power system, it is necessary to automate the compatibility check of the bus protection settings with the transient (rotor angle) stability of synchronous generators, i.e. daily calculate the critical time for fault clearing for all selected buses.			
12	T6.4	UC17	Outage coordination and automated creation of topology files for Individual Network Models	BC1, BC4	Serbia	TSO, EMMA Topology Transfer Application (TTA), Server, Outage planning application
			Short description: The basic idea of this use-case is to demonstrate the possibility of automating the creation of a topology file when approving works on network elements (outage planning) through the Topology Transfer Application (TTA), which is the subject of this use case. It should be noted here that the topology file is one of the 4 input files used to create the IGM in the CGMES format.			
13	T6.4	UC31	DLR integration with IGMs and SCADA/EMS	BC1, BC4	Serbia	TSO, EMMA DLR Application, DLR Server, SCADA/EMS, IGM server
			Short description: Automatic updating of current dynamic limits in SCADA/EMS system and updating of current limits in IGM models allows maximum use of available transmission capacities.			

* Even though the Greek pilot does not formally include a PV plant (for unbundling regulation), it has been imagined UC3 can be validated there due to the presence of PV sites just aside to the pilot.

4.3.5 Additional information about Use Cases

The goal of this section is to visually show the correlation of use-cases with the project environment, that is, that the use-cases fulfil their purpose. All this information is listed either in the previous text or in Annex I, but in a different form that does not allow immediate insight into this correlation.

Therefore, the following tables show the correlation of use cases with:

- Business-cases
- Tasks of work packages related to project products (work packages WP3, WP4, WP5 and WP6)

Other correlations of use cases with other aspects of the project environment (for example with Pilot sites) are the subject of other reports of the R²D² project, and it will not be discussed here.

4.3.5.1 Use Cases and Business Cases

Table 6 shows the correlation between use cases and business cases. It should be noted here that one use case can refer to several business cases.

Table 6 - Use Cases and business cases correlation

UC \ BC	BC				
	BC1	BC2	BC3	BC4	BC5
UC1	x				x
UC2	x				x
UC3					x
UC4	x				x
UC5	x	x	x		x
UC6	x				x
UC7					x
UC8	x				
UC9	x			x	
UC10	x				
UC11	x				
UC12	x				
UC13	x			x	
UC14	x				
UC15	x			x	
UC16	x				
UC17	x				
UC18	x				
UC19	x			x	
UC20	x				
UC21	x			x	
UC22	x	x			
UC23	x	x		x	
UC24			x		
UC25			x		
UC26				x	
UC27			x		
UC28			x		
UC29	x				
UC30	x	x			
UC31	x				
UC32	x	x			x
UC33	x		x		
UC34	x		x		
UC35	x			x	x
UC36	x		x		
UC37	x		x		
UC38	x		x		
UC39	x			x	
UC40	x				x



From this table, we can see the number of use-cases that have a primary or secondary business case as follows:

- Business-case 1 (To contribute to the improvement of the overall security and resiliency in the power system):
 - 33 use cases
- Business-case 2 (To deliver a toolkit to model the impact of HILF events on power system in order to assess its resilience and determine the optimal operational planning measures and investments to enhance power system resilience):
 - 5 use cases
- Business-case 3 (To increase the cyber-security and cyber-resilience in OT and IT of the EPES):
 - 10 use cases
- Business-case 4 (To enhance coordination, interaction, and information exchanges at regional level between TSO-TSO and TSO-DSO during critical and emergency conditions):
 - 9 use cases
- Business-case 5 (To deliver a toolkit to improve the reliability of electrical assets and to contribute to the enhancement-driven solution and automated robotic technologies):
 - 10 use cases

From the previous text, we can conclude that all the relevant business cases (not considering in this case BC6 and BC7 as explained in Section 3.2) are covered by appropriate use-cases. The number of use cases per BC varies from 5 to 30.

4.3.5.2 Use Cases and Project Tasks

The following Table 7 shows for each use case, its affiliation to one or more tasks of the corresponding work package. Use cases are listed in rows, while tasks are listed in columns and grouped according to their respective work packages. Each use case is associated with exactly one task. From this figure, we can conclude that all tasks related to project products are covered by appropriate use cases. The number of use cases per task varies from 1 to 6.

D2.3 - Requirements and Detailed Architecture Design

Table 7 - Correspondence between UCs and WPs

UC \	C3PO						IRIS			PRECOG					EMMA			
	T3.1	T3.2	T3.3	T3.4	T3.5	T3.6	T4.1	T4.2	T4.3	T5.1	T5.2	T5.3	T5.4	T5.5	T6.1	T6.2	T6.3	T6.4
UC1															X			
UC2															X			
UC3															X			
UC4																X		
UC5																	X	
UC6															X			
UC7								X										
UC8																		X
UC9																		X
UC10												X						
UC11							X											
UC12								X										
UC13																		X
UC14																		X
UC15									X									
UC16								X										
UC17																		X
UC18								X										
UC19								X										
UC20															X			
UC21								X										
UC22			X															
UC23				X														
UC24	X																	
UC25		X																
UC26						X												
UC27														X				
UC28														X				
UC29			X															
UC30				X														
UC31																		X
UC32					X													
UC33												X						
UC34													X					
UC35							X											
UC36										X								
UC37											X							
UC38											X							
UC39	X																	
UC40										X								
SUM	2	1	2	2	1	1	2	6	1	2	2	2	1	2	5	1	1	6
TOTAL	9						9			9					13			

5. REQUIREMENTS

5.1 INTRODUCTION AND METHODOLOGY

Considering the heterogeneity and the multidisciplinary approach of the R²D² project, the VOLERE methodology has been selected for discovering and defining the requirements. As stated in [5], the VOLERE Requirements Techniques are a language used for the discovery, communication and management of requirements, and to design solutions for those requirements

The VOLERE methodology is quite familiar from other EU projects. It was initially used by several project partners in previous research and innovation European projects where it was used mainly because of its simplicity. It aided in the explicit and unambiguous articulation, formalization, and tracking of the project requirements by the project partners. The VOLERE methodology was chosen in addition to being effectively implemented in the aforementioned past projects for the following three reasons:

- Simple procedures must be followed to clearly identify and formalize the needs.
- It offers a simple method for monitoring and assessing the project's development.
- It is already known and adopted by other partners in the project.

As a result, using the VOLERE technique to establish requirements is helpful not only in the early stages of the project but also when defining a reference point for the later ones. It can be used, for instance, during the use case analysis to make sure that various use cases address various components of the requirements and that they address all significant requirements. It can be used to monitor and assess the advancement of the individual work packages and the project as a whole during implementation and management. The VOLERE technique offers a way for all partners to describe their needs in a uniform manner in addition to being effective and simple to apply.

Figure 4 represents the overall methodology followed by project Consortium during the requirements' definition following the VOLERE methodology. The process is based on an iterative process, where each loop includes a revision step before finalising the requirement. After several iterations, the final list of requirements is available,

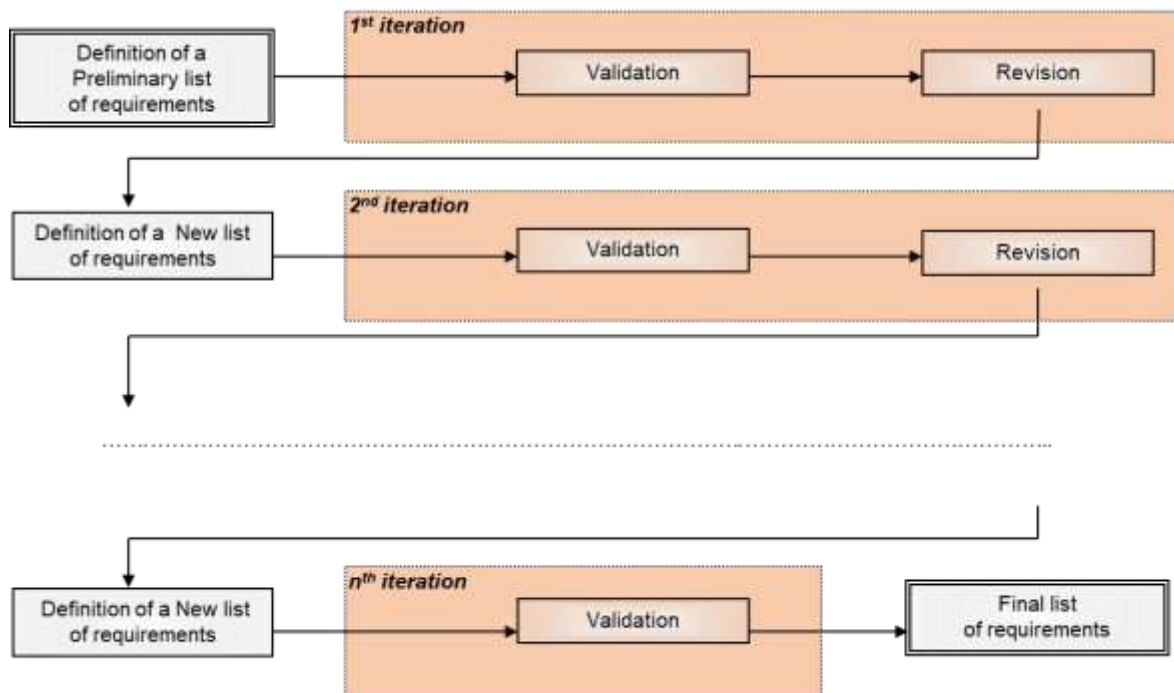


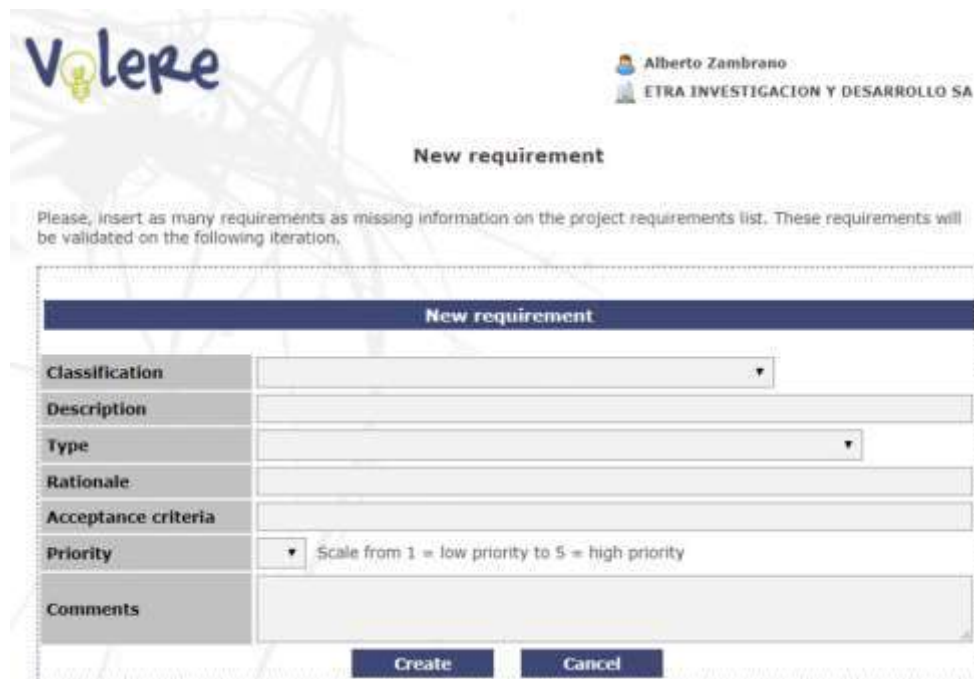
Figure 4 – Process of requirement definition, validation and revision

The process is included in the “*Volere*” tool, a web application developed by ETRA and used to manage the entire lifetime of requirements along the project. The “*Volere*” tool was initially created by ETRA with the goal of defining an ideal and comprehensive set of requirements. Since then, it has been utilized effectively in other projects. The definition, validation, and prioritizing of the R²D² requirements have all been made easier thanks to this web tool. Access to the web tool has been restricted to authorized users for security reasons, in this case, project partners have been authorised. Using the tool, the administrator is able to manage the validation process's progress from original definition to final requirement list, passing through necessary validation and modification status.

5.1.1 Requirement Definition

A screenshot of the new requirement definition window from “*Volere*” tool is shown in Figure 5. To introduce a new requirement the following information is needed:

- Classification (general, architectural, product-related, etc.)
- Textual description
- Type (functional, operational, legal, security, usability, etc.)
- Rationale (motivation behind the requirement)
- Acceptance criteria (condition to mark the requirement as fulfilled)
- Priority of implementation (1 to -5)
- Additional comments



Volere

Alberto Zambrano
ETRA INVESTIGACION Y DESARROLLO SA

New requirement

Please, insert as many requirements as missing information on the project requirements list. These requirements will be validated on the following iteration.

New requirement	
Classification	<input type="text"/>
Description	<input type="text"/>
Type	<input type="text"/>
Rationale	<input type="text"/>
Acceptance criteria	<input type="text"/>
Priority	<input type="text"/> Scale from 1 = low priority to 5 = high priority
Comments	<input type="text"/>

Create Cancel

Figure 5 – Screenshot of new requirement definition in “Volere” tool

Moreover, authors often lack formal training on writing requirements, using often unconstrained natural language. To overcome this problem, the Easy Approach to Requirements Syntax (EARS) method has been adopted in R²D² for a proper definition of requirements. EARS is an effective method of expressing requirements [6].

Here is a generic syntax for functional requirements (optional items are in square brackets):

[Trigger] [Precondition] Actor Action [Object]

The EARS identifies 5 different patterns of requirements: i) Ubiquitous (always occurring), ii) Event-driven, iii) Unwanted behaviours, iv) State-driven, and v) Optional features. As this information can be easily available in the literature and their extensive description is out of the scope of this document, it is worth mentioning the reference adopted by the consortium for this specific activity [7].

5.1.2 Validation and Revision

The validation process in the “Volere” tool starts after the initial specification of requirements. Every user must approve each one of the requirements. Conflicts and dependencies among requirements must be found at this stage. Additionally, any objections must be clarified, in particular, three different categories of issues are defined:

- Dependency: Conditions that are somewhat dependent on other conditions.
- Conflict: When one needs to prevent the implementation of another or when there is a conflict because the requirement is not defined sufficiently.
- Objection: justification or defence offered in opposition to, refusal of, or disapproval of the demand.

The authors of the requirement must review and address all dependencies, conflicts, and objections that the experts pointed forth during the validation step. The authors may, however, provide their own explanations and clarifications of the requirements in the "Revisor's comments" section if they disagree with the validator's remarks. Note that comments can only be added to the dependence, conflict, or objection sections by the person who wrote the requirements that need to be changed.

There are four phases in the revision process:

1. The author should first note which needs have been contested or are linked to any dependencies or conflicts.
2. After analysis of the validator's perspective:
 - The author concurs with the validator and moves to change or remove the requirement.
 - The author disagrees with the validator; in this case, additional relevant comments must be provided by the author to further explain or defend the requirement's objective.
3. The author must tick the box that indicates the requirement has been changed.
4. The author's efforts to resolve the dependence, conflict, or objection should be approved by the validator, who should be informed of the amended criteria.

According to the VOLERE methodology, all partners must take place in the process of definition, validation and revision process; following this principle, every user of the "*Volere*" tool is able to see the history of changes in requirements.

5.2 R²D² REQUIREMENTS

The list of the 355 requirements defined and reviewed in R²D² is reported in Table 8, with the IDs and descriptions. It is important to remark that only the requirements that have passed the validation and revision process are reported. While the full information for all requirements, as shown in Figure 5, is extensively reported in Annex III, through an export directly from the "*Volere*" tool. It is expected that in the next version of this deliverable (D2.3), the list of requirements will be updated, after the input from the design of the applications and a complete definition of the pilots' characteristics.

Table 8 – List of requirements

Req. ID	Description
C3P_001	Data of historical experiences with extreme weather.
C3P_002	Switches available in the feeders must be controllable
C3P_003	The topology of the grid at pilot sites must be known in advance
C3P_004	Pilot sites must identify critical nodes of the grid
C3P_005	EMMA ETER component shall be able to import historical supply point information read from Smart meters
C3P_006	C3PO must have access to weather forecast of the pilot site locations
C3P_007	The topologies of pilot site networks must be well known and modelled



D2.3 - Requirements and Detailed Architecture Design

C3P_008	In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the dispatchable DGs, RES and ESS units
C3P_009	The location and technical characteristics of DERs must be known
C3P_010	The characteristics of distribution lines must be known
C3P_011	Protection Settings for customising cascading simulators (T3.3)
C3P_012	The C3PO investment planning tool (T3.4) will require the investment costs of different infrastructure solutions, such as undergrounding lines and flood protection.
C3P_013	The C3PO tool to be developed in T3.4 requires the portfolio of operational flexibility options available at the demo sites.
C3P_014	Historical performance indicators of the system under extreme events
C3P_015	C3PO Static Risk Assessment Tool should perform a comprehensive cyber security risk assessment of the EPES environment, considering cyber threats, vulnerabilities and attack scenarios.
C3P_016	C3PO Static Risk Assessment Tool should allow users (DSO/TSO operators) to define existing assets, assets criticality, and security controls to create an accurate representation of the system's security posture.
C3P_017	C3PO Static Risk Assessment Tool should assess risk considering: asset criticality, threats likelihood and identified vulnerabilities criticality.
C3P_018	C3PO Static Risk Assessment Tool should provide guidance and recommendations (including countermeasures) for mitigating identified risks and vulnerabilities.
C3P_019	C3PO Static Risk Assessment Tool should provide access control to ensure that only authorized users have access to the system.
C3P_020	C3PO Static Risk Assessment Tool should be accessible through standard web browsers and compatible with different devices, such as desktops, tablets, and smartphones.
C3P_021	C3PO Dynamic CyberRisk Evaluation tool shall evaluate dynamically the EPES' Cyber-Risk Status considering assets' criticality, identified existing and emerging cyber threats as well as existing technical vulnerabilities.
C3P_022	C3PO Dynamic CyberRisk Evaluation tool should consume threat related information and technical vulnerabilities from the Cyber Threat Intelligence tool.
C3P_023	C3PO Dynamic CyberRisk Evaluation tool should consider DSO/TSO's assets' criticality, controls and their topology to assess risk values.
C3P_024	C3PO Dynamic CyberRisk Evaluation tool should provide near real-time alerts / notifications to experts when new technical vulnerabilities are identified, allowing for timely response and mitigation.
C3P_025	C3PO Dynamic CyberRisk Evaluation tool should evaluate risks utilizing T5.4 Deep Learning Data Analytics Module.
C3P_026	Access to Dynamic CyberRisk Evaluation tool will be authenticated and web-based
C3P_027	The Cyber Threat Intelligence Tool should collect cyber threat information from external sources to share with R2D2 components.



D2.3 - Requirements and Detailed Architecture Design

C3P_028	The Cyber Threat Intelligence Tool should disseminate sanitized indicators of compromise identified by R2D2 components, to the CTI community.
C3P_029	The Cyber Threat Intelligence Tool should enforce a sharing policy abiding to the DSO/TSO's information classification policies.
C3P_030	The Cyber Threat Intelligence Tool should support widely accepted formats of cyber threat information sharing.
C3P_031	The Cyber Threat Intelligence Tool should be able to generate alerts and notifications based on predefined rules.
C3P_032	Access to Cyber Threat Intelligence Tool will be authenticated and web-based.
C3P_033	SCADA S, V, I measurements availability over the main feeders of pilot MV lines
C3P_034	Metering equipment up-running, available data via DLMS/COSEM protocol
C3P_035	Output of T3.4 Operational planning module is sent to DSO via MQTT protocol
C3P_036	The characteristics of mobile sources must be well known and modelled
C3P_037	The outage scenarios of power lines and electrical components must be well observed
C3P_038	The characteristics of critical/non-critical loads must be known
C3P_039	OPDE RR – User management - Log in using user name and password, including possibility to create user groups.
C3P_040	OPDE RR – Risk entry form aligned with ENTSO-E practise.
C3P_041	OPDE RR – Dashboard for displaying statistical risk information using bar charts and pie charts.
C3P_042	OPDE RR – E-mail notification after saving information in tool.
C3P_043	OPDE RR – Restriction of data access/modification based on the “need to know” principle.
C3P_044	OPDE RR – Log list that displays all changes of data in the tool.
C3P_045	OPDE RR – Communication channel between appointed users for each risk separately.
C3P_046	OPDE RR – Simplified view of all submitted risks in tabular form.
C3P_047	OPDE RR – Detailed view of each submitted risk separately.
C3P_048	OPDE RR – Export of risk data in .csv file format
EMM_002	Maintenance UAV shall flight in manual or autonomous
EMM_003	the recorded flight path of the AUV shall be presented over a map
EMM_004	EMMA GUI shall feature a credential validation screen allowing opening
EMM_005	To have access to a historical dataset of substations measurements (mainly P,Q,V,I)
EMM_006	To receive Real-Time measurements (or simulated Real-Time data) from substations (mainly P,Q,V,I)
EMM_007	if abnormal high temperatures are captured by UV camera pointing to a transformer an alarm shall be sent in MQTT protocol
EMM_008	To acquire images



D2.3 - Requirements and Detailed Architecture Design

EMM_009	(OPC tool) Collection of outage plans from stakeholders (TSOs, RCCs, PES users)
EMM_010	EMMA ARGOS component must feature a web application for upload images and videos
EMM_011	EMMA ARGOS component shall trigger the image processing task upon reception of new data
EMM_012	EMMA ARGOS image processing component shall trigger events and sent to EMMA component when the images analysed contain problems according to the ML models
EMM_013	EMMA shall receive periodically a selected set of SCADA signals for grid assets and substations
EMM_014	EMMA ARGOS component shall identify when new images or videos have been uploaded and then triggering the image processing process
EMM_015	EMMA shall feature a web interface to present the maintenance results and KPIS
EMM_016	EMMA signals processing component shall trigger events and store relevant data when the analysis of the signals indicates about problems according to the ML models
EMM_017	EMMA signal processing component ML models must support identifying active and future problems in the substation assets
EMM_018	EMMA ARGOS image processing component ML models must support identifying active and future problems in the substation assets and overhead lines
EMM_019	EMMA component shall generate a ranked list of interventions prioritized according to its criticality
EMM_020	EMMA GIMAN component shall schedule the workforce duties according to the information received from EMMA
EMM_021	EMMA GIMAN component shall generate workforce activities routing to carry out the duties in the most optimal way
EMM_022	Pilot site must deploy metering devices.
EMM_023	Pilot sites must identify critical nodes of the grid
EMM_024	Grid operator must configure in EMMA GIMAN the details of personnel involved in incident management.
EMM_025	Maintenance UAV could be controlled in remote
EMM_026	EMMA ARGOS ML models should identify problems linked to the presence of forest near the overhead lines according to the images
EMM_027	EMMA ARGOS ML models should identify physical (structural or mechanical) problems on tower/poles, conductors and insulators based on the images
EMM_028	EMMA ARGOS ML models should identify electrical problems on the conductors and insulators based on the images
EMM_029	EMMA DYML component shall import data from DGA analysis
EMM_030	EMMA DYML component shall support OPC-UA protocol to gather SCADA measurements
EMM_031	EMMA ETER shall be able to import grid topology in CIM format



D2.3 – Requirements and Detailed Architecture Design

EMM_032	EMMA ETER component shall import historical substation feeder data
EMM_033	EMMA ETER component shall be able to identify abnormal or suspicious behaviours of supply points based on data
EMM_034	EMMA GIMAN component should feature a web GUI
EMM_035	EMMA ETER component should feature a web GUI
EMM_036	EMMA must contain a communication platform to provide the following services: 1) All participants can upload and download files 2) files are kept for a certain period of time 3) A conference call can be started
EMM_037	EMMA shall contain a tool to calculate the cost sharing related to remedial actions with cross-border impact between the TSOs involved
EMM_038	EMMA product must contain outage planning optimization tool (EMMA OP)
EMM_039	EMMA product must contain an application to transfer topology file
EMM_040	EMMA product must contain dedicated script created in DiGSILENT environment (DiGSILENT Programming Language) to perform calculations related to transient stability.
EMM_041	EMMA product must contain application to perform calculations related to power quality
EMM_042	EMMA product must contain an application to transfer Dynamic Line Rating limits into IGMs and SCADA/EMS system
EMM_043	test
EMM_044	Surveillance equipment installed in HV/MV substation must provide 24h live streaming image to EMMA ARGOS
EMM_045	EMMA PQEL script should be created within the PowerFactory DiGSILENT programming environment in the appropriate programming language.
EMM_046	After running the EMMA PQEL script, a dialog box opens in which the operator selects which scenario will be executed.
EMM_047	The EMMA PQEL operator must have capability to make changes to the planned levels for the Compliance simulation scenario and the Equivalent grid parameters calculation scenario.
EMM_048	In the case of the Compliance simulation scenario, the EMMA PQEL operator can: 1) Define a path to the simulation network model; 2) Mark the nodes for which emission values are calculated; 3) Define the path to the folder where the output file is saved.
EMM_049	For the Compliance monitoring scenario, the EMMA PQEL operator can: 1) Define the path to the file with emission limits & measured data 2) Mark the nodes for which the comparison is made 3) Define the path to the folder where the output file is stored.
EMM_050	For the Equivalent grid parameters calculation scenario, the EMMA PQEL operator can: 1) Define the path to the simulation grid model; 2) Mark the nodes for which parameters are calculated; 3) Define the path to the folder where the output file is stored.



D2.3 - Requirements and Detailed Architecture Design

EMM_051	After defining the input parameters through .SetSelect objects within DigSILENT framework, the EMMA PQEL script needs to perform in Compliance simulation scenario operations provided in the requirements comments section.
EMM_052	After defining the input parameters through .SetSelect objects within DigSILENT framework, the EMMA PQEL script needs to perform in Compliance monitoring scenario the operations provided in the requirement comments section.
EMM_053	After defining the input parameters through .SetSelect objects in the DigSILENT framework, the EMMA PQEL script in the Equivalent grid parameters calculation scenario executes the operation given in the requirement comments section.
EMM_054	The EMMA TSC script needs to be created within the PowerFactory DigSILENT programming environment.
EMM_055	Upon entering the EMMA TSC script, a menu opens so that the operator can run a calculation related to a fault which is: 1) switched off by a circuit-breaker 2) of transient type.
EMM_056	The EMMA TSC script should have a configurable set of input data (parameters) with the default values provided in the requirement comments section
EMM_057	Before opening the EMMA TSC script, the operator must have the ability to: 1) create a "set" of type .SetSelect object 2) fill the set with elements 3) assign the set to the script.
EMM_058	The EMMA TSC script allows the operator to define initial conditions in the network.
EMM_059	The EMMA TSC script allows the operator to select synchronous machines to be observed in the calculations by creating an "OutOfStep" set of variables (the value of the variable must be selected for each generator).
EMM_060	When starting a new calculation, the EMMA TSC script a) clears the output window of previous results b) reset the previously calculated critical fault time values for all network nodes
EMM_061	The EMMA TSC script calculates the critical fault time for each of the buses from the defined set.
EMM_062	The EMMA TSC script internally stores the result of the calculation to one of the variables belonging to the bus structure.
EMM_063	The EMMA TSC script displays calculation results in the output window and stores the calculation results inside the "dpl1" buses variable (pTerm:dpl1).
EMM_064	The EMMA TSC script automatically or manually after completion of the calculation creates an output file with the results in ".txt" format and stores the file in the predefined folder.
EMM_065	EMMA DLR Application must be capable to read analogue values and quality flags of DLR limits and quality of DLR system calculation from SCADA/EMS.
EMM_066	EMMA DLR Application must be capable to read real-time and forecasted limits and quality of DLR system calculation from CSV file.
EMM_067	EMMA DLR Application must be capable to write values into SCADA limits for each line with DLR sensor.
EMM_068	EMMA DLR Application must be capable to write forecasted limits into OPL file.



D2.3 - Requirements and Detailed Architecture Design

EMM_069	EMMA TTA shall read an input file containing network element type, network element designation, period, time and type of switching (off/on), description of switching state change
EMM_070	EMMA TTA shall update the default topology file for the selected date/hour according to the approved planned outages.
EMM_071	EMMA TTA shall export the topology file to the predefined server (grid model server)
EMM_072	The topology report shall list all network elements whose topology status differs from the topology in the default topology file
EMM_073	The list of elements that are subject to planned outages must contain: network element type, network element designation, disconnection period, time and type of switching, and description of switching state change (continuous/daily)
EMM_074	EMMA TTA shall create a default topology file in .csv format
EMM_075	EMMA TTA shall create an updated topology file in TOP file (format used by eTNA power flow calculation software)
EMM_076	EMMA TTA shall create a topology report file in .xls or .pdf format
EMM_077	If RA has a positive effect on XNEC unloading and the price of RA is positive (TSO activating the RA pays to balancing entity) then EMMA RA CSS will distribute RA.TSO costs between CNT.TSO and XNEC.TSO equally.
EMM_078	If RA has positive effect on XNEC unloading and RA price is negative (balancing entity pays to TSO activating RA) then EMMA RA CSS will distribute equally RA.TSO income between RA.TSO, CNT.TSO and XNEC.TSO.
EMM_079	If RA has negative effect on XNEC unloading and RA price is negative then EMMA RA CSS will distribute equally RA.TSO income between CNT.TSO and XNEC.TSO
EMM_080	If RA has negative effect on XNEC unloading and RA price is positive (TSO activating RA pays to balancing entity) then EMMA RA CSS will not distribute any costs between involved TSOs (CNT.TSO, XNEC.TSO, RA.TSO).
EMM_081	If there is a constraint without contingency, RA has positive effect on XNEC unloading and RA price is positive (TSO activating RA pays to balancing entity) then EMMA RA CSS will distribute all RA.TSO costs to XNEC.TSO.
EMM_082	If there is a constraint without contingency, RA has positive effect on XNEC unloading and RA price is negative (balancing entity pays to TSO activating RA) then EMMA RA CSS will distribute RA.TSO income equally between RA.TSO and XNEC.TSO
EMM_083	If there is a constraint without contingency, RA has negative effect on XNEC unloading and RA price is negative (balancing entity pays to TSO activating RA) then EMMA RA CSS will distribute all RA.TSO income to XNEC.TSO.
EMM_084	If there is a constraint without contingency, RA has negative effect on XNEC unloading and RA price positive (TSO activating RA pays to balancing entity) then then EMMA RA CSS will not distribute any costs between involved TSOs (XNEC.TSO, RA.TSO).
EMM_085	For each RA applied in one market interval, RA costs EMMA RA CSS will distribute proportionally to all XNECs that are positively affected by an RA (unloading). This way pairs RA-XNEC are created.



D2.3 - Requirements and Detailed Architecture Design

EMM_086	After EMM_085 requirement is applied, RA costs in one market interval previously allocated to specific XNEC is furthermore decomposed for each CNT proportionally to the percentage of overload caused by contingencies (included base case constraints).
EMM_087	After EMM_086 requirement is applied, for each RA-CNT-XNEC triplet, EMM_077 - EMM_084 requirement is applied by EMMA RA CSS. This way costs are allocated to all involved TSOs.
EMM_088	After EMM_087 requirement is applied, EMMA RA CSS will sum all costs/incomes for each TSOs.
EMM_089	RAs costs must be submitted by TSO that activated RAs in its Control Area, in an excel file or similar format, with the costs indicated for each market interval during the day, date and costs. Costs must be expressed in euros.
EMM_090	Common Grid Model must be in CGMES or ucte format
EMM_091	EMMA RA CSS must be capable to import PTDF file, RA costs file and base case flows file (all in excel format).
EMM_092	EMMA RA CSS must be capable to create report in .txt, .csv, .doc, .xsl or other widely used format.
EMM_093	Cost-sharing report is created on daily basis with the granulation equal to the basic market interval.
EMM_094	EMMA RA CSS shall have 3 modules: 1) Cost sharing calculation module, 2) database modules (RAs, CNTs and XNECs) and 3) Cost sharing calculation parameters setting module.
EMM_095	EMMA RA CSS main form must have command buttons to direct to each module and navigation command buttons
EMM_096	'EMMA RA CSS - Cost-sharing calculation / Date and time' form must have fields to enter date and market time interval and navigation buttons
EMM_097	'RA CSS - Cost-sharing calculation / Information on RAs' form must have fields to enter RA node label, RA direction, RA cost, command button for new RA and navigation buttons
EMM_098	'EMMA RA CSS - Cost-sharing calculation / Information on CNTs and XNECs' form must have fields to enter CNT label, XNEC label, XNEC overload percentage for CNT, command buttons for new CNTs and XNECs and navigation buttons.
EMM_099	'EMMA RA CSS - Cost-sharing calculation / Base Case flows import' form must have command button for base case flows file import from the predefined folder
EMM_100	'EMMA RA CSS - Cost-sharing calculation / PDTF matrix import' form must have command button for PDTF file import from predefined folder
EMM_101	'EMMA RA CSS - Cost-sharing calculation / Results' form must have fields to display, date and market time interval and RA cost sharing calculation results
EMM_102	'EMMA RA CSS - RAs, CNTs and XNECs database' form must have command button to open RAs, CNTs and XNECs databases
EMM_103	EMMA RA CSS - RA database must contain data on RA ID, activating TSO and RA label (generation or demand node)



D2.3 - Requirements and Detailed Architecture Design

EMM_104	EMMA RA CSS - CNTs & XNECs database must contain the following data on network elements representing CNTs & XNECs: ID, label, starting node, ending node, TSO operating starting node and TSO operating ending node
EMM_105	EMMA RA CSS - TSOs database must contain the following data on participating TSOs: ID and TSO name
EMM_106	EMMA RA CSS - Cost-sharing calculation parameters settings database must contain data on TSO activating RA, TSO operating CNT (both nodes), TSO operating XNEC (both nodes), RA cost/impact quadrant and cost sharing factors between TSOs
EMM_107	'EMMA RA CSS - Cost-sharing calculation sensitivity' form must have a field to enter PTDF sensitivity threshold.
EMM_108	EMMA RA CSS must be capable to read, delete, create and update data stored in RA, TSOs and CNTs & XNECs databases
EMM_109	EMMA OP tool must create UAP file, export this file to server, and import the manually reconfigured UAP file.
EMM_110	EMMA OP tool must create Gantt charts showing the period of network elements planned outages with the following granularity: a) the whole year by hours, b) the whole year by days
EMM_111	EMMA OP tool Gantt charts will contain horizontal and vertical sliders to allow good visibility of outage periods. The parts of the chart that contain the date/time and network element label will be fixed on the screen.
EMM_112	EMMA OP tool must have automatic and manual mode for performing OPI assessment.
EMM_113	EMMA OP tool should control eTNA offline instance using API.
EMM_114	EMMA OP tool will store OPI results in a database and display them in appropriate manner
EMM_115	EMMA OP tool should calculate certain indicators based on OPI results
EMM_116	EMMA OP tool administrator must have supervisor access and will be able to change all locations for file import/export.
EMM_117	EMMA OP tool must import EIC vs CIM ID cross-reference table periodically.
EMM_118	EMMA OP tool must allow the operator to delete OPC CON files on a dedicated server.
EMM_119	EMMA OP tool must export the UAP file in XML format.
EMM_120	EMMA OP tool must allow OP operator to manually create initial UAP files for specific periods (yearly, quarterly, weekly).
EMM_121	EMMA OP tool must limit in automatic mode, the number of elements which can change status (ON and OFF) should be chosen in a way that eTNA calculations are executed in a reasonable time
EMM_122	EMMA OP tool must have access to CGM, CON and MON files for each hour for which the calculations are performed. If that is not the case, the user should be informed with the appropriate message.
GEN_001	All products GUIs should present results in English language



D2.3 - Requirements and Detailed Architecture Design

GEN_001	All products GUIs should present results in English language
GEN_001	All products GUIs should present results in English language
GEN_002	EMMA should consider the legislative constraints regarding the limited presence of drones near critical infrastructure
GEN_004	Bidirectional communication between DSO and involved energy stakeholders is established. Supported protocols mainly MQTT/AMQP (via RabbitMQ broker)
GEN_005	Adequate measuring equipment is installed for proper monitoring of the grid
GEN_006	Historical data from smart meters, sensors, metering devices etc. should be available.
GEN_007	Metering data by all involved metering devices (AMI, SCADA, storage systems, etc.) should be anonymised
GEN_008	The tools developed should be compatible with different operating systems (Windows, Linux, MacOS, etc.).
GEN_009	Server/virtual machine technical requirements for tools support must be known as soon as possible.
GEN_010	R2D2 will represent alerts from different products
GEN_011	A communication channel between DSO - TSO must be existent
IRI_001	IRIS application should be available and accessible to end-users
IRI_002	When the user log into IRIS application, IRIS application should get the information who is connected and his affected organization/company and roles in the application to apply the correct rights to functionalities
IRI_003	The ICL tools shall list conditions when electricity load cannot be met by supply
IRI_004	IRIS solution shall use standards in the different components (CIM models, OPC format, etc.)
IRI_007	IRIS should ensure interoperability between shared / redundant components
IRI_008	IRIS DSO "Flexibility system" should operate as protocol communication gateway supporting different standard communication protocols like IEC 60870-5-104, MQTT, ICCP/TASE.2
IRI_009	IRIS DSO "Flexibility system" must be able to receive data from multiple source types
IRI_010	IRIS DSO "Flexibility system" should contain a database to store the received and processed data
IRI_011	IRIS DSO "Flexibility system" database should be scalable
IRI_012	IRIS DSO "Flexibility system" should automatically trigger commands/alerts based on rules/algorithms
IRI_013	IRIS DSO "Flexibility system" system should send identified commands/alarms to different destinations based on a configuration
IRI_014	IRIS DSO "Flexibility system" should have the Web GUI
IRI_015	IRIS DSO "Flexibility system" GUI access should be secure.
IRI_016	IRIS must provide phasors angle difference monitoring



D2.3 - Requirements and Detailed Architecture Design

IRI_017	The IRIS product must contain Emergency and Restoration – Over-frequency protection module (OFPM)
IRI_018	The IRIS product must contain Emergency and Restoration – System Split module (ER-SSM)
IRI_019	The IRIS product must include RES and end-load forecasting tool
IRI_020	IRIS product must contain a communication platform
IRI_021	IRIS product must contain Remedial Action tool
IRI_022	IRIS product must contain an application to optimize PMU installation points in the transmission network
IRI_023	IRIS DSO "Flexibility system" should contain service for voltage profile and loading calculation
IRI_024	IRIS DSO "Flexibility system" should detect if voltages and/or loadings are outside the expected limits
IRI_025	IRIS DSO "Flexibility system" should enable checking of execution of control actions
IRI_026	IRIS DSO "Flexibility system" should contain DER operation optimization for ancillary services, taking into account voltage profile and loadings
IRI_027	IRIS DSO "Flexibility system" should contain state estimation functionality
IRI_028	IRIS DSO "Flexibility system" should contain service for defining restrictions in ancillary service control actions to prevent voltage and loadings outside the expected limits
IRI_029	IRIS DSO "Flexibility system" should be able to send restriction to all service providers (TSO, Aggregator, Balancing responsible, Consumer, DER)
IRI_030	The alarm on critical angle difference between two observed points by PMUs must be in sound form, accompanied by information about the angle difference, and the places where PMUs are installed. It must be ensured that operator can acknowledge the alarm.
IRI_031	The alarm on lack of adequate measurements of any PMU must be in sound form, accompanied by information about the place where the faulty PMUs is installed. It must be ensured that the operator can acknowledge the alarm.
IRI_032	IRIS OPP application must allow the user to draw a network graph (branches and nodes) using a computer mouse or to enter all network branches in a table with two columns (start and end nodes) defining connectivity matrix.
IRI_033	IRIS OPP must allow the user to select the optimization criteria for the selection of the installation points of the PMUs as follows: Basic optimisation, N-1 optimisation, Optimisation with already installed PMUs
IRI_034	If the user selects the optimization option with PMUs already installed, IRIS OPP opens a new window where the user can enter the buses where PMUs are already installed.
IRI_035	After starting the calculation for the selected optimization process, IRIS OPP displays in a new window (or popup window) all solutions of the applied optimization.



D2.3 - Requirements and Detailed Architecture Design

IRI_036	IRIS OPP must calculate and display with each optimal solution the SORI parameter to describe the quality of optimization solution
IRI_037	IRIS OPP creates an optimization report in .docx or .csv format, which contains all relevant input data and all optimization results, as well as the optimization quality parameter. The report is saved in a predefined folder.
IRI_038	It must be possible to record all communication during a single session for system split (all records must be time-stamped) in the E&R - System Split module.
IRI_039	The Emergency & Restoration - System Split module communication tool displays must have a header with the inscription System Split throughout the procedure described in steps 1 – 35 and the name of the step currently being executed.
IRI_040	The Emergency & Restoration - System Split module communication tool displays must contain a bar graph of all System Split procedure steps with the currently active step highlighted.
IRI_041	After the system split is detected, the Emergency & Restoration - System Split module communication tool is automatically started at all TSOs and RCC with a corresponding sound alarm.
IRI_042	The RCC must have the ability to manually jump to any step of the system split scenario. In this case, a corresponding message and a sound alarm are generated at all TSOs.
IRI_043	Each Emergency & Restoration - System Split module display must contain a message field that is editable for each user and in which all previous messages can be viewed during one procedure.
IRI_044	When opening each new Emergency & Restoration - System Split module display, a sound alarm should be activated, which is deactivated by manual action of the operator receiving the information.
IRI_045	All displays of Emergency & Restoration - System Split module should show the responses of all TSOs/RCCs to the requested actions.
IRI_046	When a declaration in Emergency & Restoration - System Split module (agree/disagree) is required, then there should be two declaration check boxes, one for agree (YES) and one for disagree (NO).
IRI_047	After acting on some control of Emergency & Restoration - System Split, it is necessary to open a dialog box asking for confirmation of activation/change of control status.
IRI_048	When a System Split procedure step requires a response from TSOs/RCC, such displays should have a countdown timer visible to all participants to see how much time is left to respond. Time periods must be configurable (default value is set to 2 min).
IRI_049	The RCC as the administrator of the System Split procedure must have the ability to communicate instead of TSOs who cannot do so for technical reasons (e.g. to change statuses, make confirmations, etc.)
IRI_050	When all requested parties have performed the actions required in a particular step, the next display is automatically opened). Note: some steps can be shown on the same display, which is defined by other requirements.



D2.3 - Requirements and Detailed Architecture Design

IRI_051	At each System Split procedure step, a button for starting the teleconference must be available, in which case the corresponding audio message about the requested teleconference is activated for all participants.
IRI_052	When a system break is detected, a visual and sound warning is created that a system break has been detected. The visual information must contain the number of islands detected, and which TSO is in which island.
IRI_053	One display opens for System Split procedure steps 1 and 2 with appropriate warning on system split detection and contains a separate check box for confirmation by all TSOs.
IRI_054	One display opens for System Split procedure steps 3 and 4 with appropriate information on identified affected TSOs warning and contains a separate check box for confirmation by all TSOs.
IRI_055	One display opens for System Split procedure steps 5 and 6 with appropriate warning on required frequency deviation management actions and contains a separate check box for confirmation by all TSOs.
IRI_056	System Split procedure display for steps 5 and 6 contains warning on required EAS communication on system state and a separate check box for confirmation by all TSOs.
IRI_057	One display opens for steps System Split procedure 7, 8 and 9 with information on Frequency Leader determination results, nominated Frequency Leader and contains a separate check box for confirmation by all TSOs.
IRI_058	One display opens for steps System Split procedure 10 and 11 with appropriate warning on required frequency deviation management actions and contains a separate check box for confirmation by all TSOs.
IRI_059	One display opens for steps System Split procedure 12 and 13 with appropriate warning on required further frequency deviation management actions and contains a separate check box for confirmation by all TSOs.
IRI_060	One display opens for steps System Split procedure 14, 15 and 16 with appropriate information on ongoing telco with SAM, nominated Resynchronisation Leader and contains a separate check box for confirmation by all TSOs.
IRI_061	The RCC manually enters the name of the TSO designated as the frequency leader in the display for steps System Split procedure 14, 15 and 16
IRI_062	One display opens for System Split procedure steps 17 and 18 with appropriate warning on required Resynchronization Leader announcement on EAS and contains a separate check box for confirmation by the Resynchronization Leader.
IRI_063	One display opens for System Split procedure steps 19 and 20 with appropriate warning on upcoming resynchronisation and contains a separate check box for confirmation by all TSOs and RCC.
IRI_064	One display opens for System Split procedure steps 21 and 22 with appropriate warning on executed resynchronisation and contains a separate check box for confirmation by all TSOs and RCC.



D2.3 - Requirements and Detailed Architecture Design

IRI_065	One display opens for System Split procedure steps 23 and 24 with appropriate warning on cancelation the Resynchronization Leader status on EAS and contains a separate check box for the cancelation confirmation by the Resynchronization Leader.
IRI_066	One display opens for System Split procedure steps 25, 26 and 27 with appropriate information on ongoing telco to select Frequency Leader after resynchronisation, nominated Frequency Leader and contains a separate check box for TSO/RCC confirmation.
IRI_067	The Frequency Leader of the region manually enters the name of the TSO designated as the Frequency Leader after resynchronisation in the display opened for System Split procedure steps 25, 26 and 27.
IRI_068	One display opens for System Split procedure steps 28 and 29 with appropriate warning on confirmation or cancelation of the Frequency Leader status on EAS after resynchronisation.
IRI_069	Display for System Split procedure steps 28 and 29 contains a separate check box for the cancelation confirmation by the Frequency Leader after resynchronisation.
IRI_070	One display opens for System Split procedure steps 30 and 31 with appropriate warning on Frequency Deviation Management after Resynchronisation and contains a separate check box for confirmation by all TSOs.
IRI_071	One display opens for System Split procedure steps 32 and 33 with appropriate warning on Return of the Frequency Restoration Controller to Normal Operation Mode and contains a separate check box for confirmation by RCC.
IRI_072	One display opens for System Split procedure steps 34 and 35 with appropriate warning on Return of the Frequency Restoration Controller to Normal Operation Mode and update of EAS status regarding Frequency Restoration Controller operation mode.
IRI_073	Display for System Split procedure steps 34 & 35 contains a separate check box for confirmation of Frequency Restoration Controller Operation Mode and for Frequency Restoration Controller Operation Mode on EAS, both by all TSOs except the Frequency Leader
IRI_074	One display opens for steps System Split procedure 36 & 37 with appropriate warnings on Return of the Frequency Restoration Controller to Normal Operation Mode and adjustment of system state status on EAS.
IRI_075	Display for System Split procedure steps 34&35 contains a separate check box for confirmation of Frequency Restoration Controller Operation Mode and for Frequency Restoration Controller Operation Mode on EAS, both by Frequency Leader.
IRI_076	IRIS RA tool must be able to receive the list of CA results in .xml format
IRI_077	IRIS RA tool must be capable to recognize and offer applicable RAs for CA results and alarms from real time violation.
IRI_078	IRIS RA tool must allow the operator to select applicable RAs using checkboxes.
IRI_079	The list of applicable RAs in IRIS RA tool must contain name of RAs, priority index, short and detailed description



D2.3 – Requirements and Detailed Architecture Design

IRI_080	IRIS RA tool must have access to the SCADA/EMS power flow database and must be able to enter changes in this database according to the applied RAs.
IRI_081	IRIS RA tool must be designed to provide the end user with a dialog with Yes/No/Cancel buttons for the final decision whether to perform RA or not
IRI_082	IRIS RA tool must have established connection with the SCADA system to execute RAs.
IRI_083	IRIS RA tool must be able to access the list of constrained (overloaded) network elements from SCADA/EMS database.
IRI_084	IRIS RA tool must allow the operator to select the relevant constraints (overloads) from a list using a check box
IRI_085	IRIS RA tool must be able to send signals to SCADA system in order to change status on European Awareness System platform.
IRI_086	IRIS RA tool, in case of real time security violations, must be able to automatically use available RAs according to priority index.
IRI_087	IRIS RA tool must be able to access SCADA/EMS Contingency Analysis reports.
IRI_088	IRIS OFPM must be active if frequency exceeds 50.2 Hz
IRI_089	IRIS OFPM must calculate total needed decrease of active power generation in case of over-frequency P_{dec} [MW] as follows (for LFSM-O droop of 5%): $P_{dec} = P_{total} \cdot (40 \cdot f - 2008)$
IRI_090	For each generator available for active power decrease, IRIS OFPM must calculate: $P_{dw} = P - P_{min}$. In addition the sum of P_{dw} for all generators shall be calculated – $SUM(P_{dw})$.
IRI_091	IRIS OFPM must recalculate total active power decrease, available downward reserves and generators base (set) points in time interval set by OFPM operator.
IRI_092	IRIS OFPM operator must be able to set available downward active power reserve threshold ($P_{threshold}$) and frequency threshold ($f_{threshold}$).
IRI_093	IRIS OFPM will firstly activate reduction of active power on generators if $f > 50.2$ Hz and secondly disconnection of the generators if the following condition is met: $SUM(PH_{dw}) + SUM(PT_{dw}) + SUM(PW_{dw}) < P_{threshold}$ or $f > f_{threshold}$
IRI_094	IRIS OFPM will reduce generators active power according to the following priority: Hydro Power Plants, Thermal Power Plants, Wind Parks (according to the Serbian pilot site characteristics).
IRI_095	Based on IRI_090 requirement, IRIS OFPM must calculate $SUM(PH_{dw})$, $SUM(PT_{dw})$ and $SUM(PW_{dw})$. In the event of an outage of a generator that is in this mechanism, $SUM(PH_{dw}) / SUM(PT_{dw}) / SUM(PW_{dw})$ is reduced by the P_{dw} of this generator.
IRI_096	If $P_{dec} + SUM(P_{var}) < SUM(PH_{dw})$, for each hydro generator IRIS OFPM must calculate new base point P_b as follows: $P_b = P - [P_{dec} + SUM(P_{var})] \cdot P_{dw} / SUM(PH_{dw})$. Thermal and wind generators get a base point equal to their active power when OFPM is activated.



D2.3 - Requirements and Detailed Architecture Design

IRI_097	If $SUM(PH_{dw}) < P_{dec} + SUM(Pvar) < SUM(PH_{dw}) + SUMA(PT_{dw})$, for each thermal generator IRIS OFPM must calculate new base point P_b as follows: $P_b = P - [P_{dec}SUM(Pvar) - SUM(PH_{dw})] \cdot P_{dw} / SUM(PT_{dw})$. All hydro generators get P_b equal to their technical minimum.
IRI_098	If $SUM(PH_{dw}) + SUM(PT_{dw}) < P_{dec} + SUM(Pvar) < SUM(PH_{dw}) + SUM(PT_{dw}) + SUM(PW_{dw})$, for each wind generator IRIS OFPM must calculate new base point $P_b = P - [P_{dec} - SUM(PH_{dw}) - SUM(PT_{dw})] \cdot P_{dw} / SUM(PW_{dw})$
IRI_099	If $SUM(PH_{dw}) + SUM(PT_{dw}) + SUM(PW_{dw}) < P_{dec} + SUM(Pvar)$, IRIS OFPM must calculate for all generators new base point P_b equal to their technical minimum.
IRI_100	IRIS OFPM shall communicate generators base point signal through: 1) Thermal power plant and wind park gateway 2) TSO connection facility gateway and GRAS devices installed in hydro power plants
IRI_101	All generators in IRIS OFPM disconnection mechanism, will be sorted in array according to local security criteria and additional criteria set by generator owners according to the following priority: Hydro Power Plants, Thermal Power Plants, Wind Parks.
IRI_102	IRIS OFPM must calculate disconnection frequency for all generators as follows: $f_{disci} [Hz] = (2008 + SUM(Pvar) + 0,5 \cdot P_i + SUM(P1 \rightarrow i-1)) / 40$
IRI_103	IRIS OFPM must recalculate disconnection frequency for all generators in time interval set by OFPM operator.
IRI_104	IRIS OFPM must communicate generators disconnection signal to circuit breaker of the generators connection line in TSO connection substation
IRI_105	IRIS OFPM must provide to operator observability of generators participating in active power generation decrease mechanism and generators disconnection mechanism.
IRI_106	IRIS OFPM operator must be able to include/exclude generators for one or both mechanism (active power generation decrease mechanism / generators disconnection mechanism) before or during OFPM activation.
IRI_107	When over-frequency higher than 50.2 Hz is detected, IRIS OFPM must generate sound alarm that can be cancelled by operator.
IRI_108	When over-frequency is detected, OFPM must generate summary display presenting: 1) actual frequency 2) time relapsed from over-frequency detection 3) calculated total active power to be reduced 4) total reduced power after over-frequency detection
IRI_109	When OFPM active power generation decrease mechanism is activated, OFPM must generate a display presenting all data given in comments section.
IRI_110	If IRIS OFPM generators disconnection mechanism is active, OFPM must generate a display presenting: Generators' active power at the moment of over-frequency detection, identification if generator is disconnected by OFPM / Generators disconnection mechanism
IRI_111	IRIS OFPM and SCADA must communicate through IPC (inter-process communication).



D2.3 - Requirements and Detailed Architecture Design

PRE_001	Relevant changes in data which may affect ML-based components must be detectable
PRE_002	Web service for signing and verification
PRE_003	Command line solution for signing and verification
PRE_004	Connections to KSI Gateway
PRE_005	Connections to KSI Block chain
PRE_006	Sample data sets for tools available as soon as possible after UC-s are defined and agreed
PRE_007	KSI tool detects 100% of changed in signed data during verification.
PRE_008	KSI tool confirms integrity of original files on 100% of cases, when verification function is applied on originally signed data.
PRE_009	Tokenization tool provides tokens, which verify originality of tokenized data in 100% of cases
PRE_010	Model (IGM, CGM) shall be available.
PRE_011	Data format must be agreed to run data registration and integrity validation.
PRE_012	Tokenized data and its token must be stored in the same or different database, a link between them must be maintained.
PRE_013	CARMEN product must be able to comprehend and analyse ICS protocols
PRE_014	PRECOG Supply Chain Assessment Tool must provide management guidelines for EPES to secure supply chain
PRE_015	PRECOG Supply Chain Assessment Tool must provide guidelines for EPES' vendors to use to secure their supply chain and their product development
PRE_016	PRECOG Supply Chain Assessment Tool must provide guidelines in HTML and PDF format
PRE_017	PRECOG Supply Chain Assessment Tool shall support a self-assessment for EPES Operator vendors/suppliers to evaluate their current supply chain and development practices
PRE_018	PRECOG Supply Chain Assessment Tool shall support a self-assessment for EPES Operator to evaluate their own supply chain management practices
PRE_019	PRECOG Supply Chain Assessment Tool should provide scoring mechanisms to assess and evaluate vendor and EPES practices, providing an overall rating or score.
PRE_020	PRECOG Supply Chain Assessment Tool should be accessible through standard web browsers and compatible with different devices, such as desktops, tablets, and smartphones.
PRE_021	PRECOG Supply Chain Assessment Tool shall be accessible to registered/authorised users to enforce proper access control on the provided information and the assessment results.
PRE_022	PRECOG Supply Chain Assessment Tool should generate comprehensive reports summarizing the assessment results for vendors and EPES practices.
PRE_023	Supply Chain Assessment Toolkit must get access to T5.1 tool to register and validate data and its associated proofs



D2.3 - Requirements and Detailed Architecture Design

PRE_024	CARMEN product will automatically detect new devices connected to the network
PRE_025	CARMEN will detect potential threats using pattern detection
PRE_026	CARMEN product will detect anomalies based on traffic characterization
PRE_027	CARMEN product will detect anomalies based on control, operation and supervision levels
PRE_028	CARMEN will detect operational alerts from IT/OT devices
PRE_029	PRECOG Supply Chain Assessment Tool should monitor new components communications in an isolated (staging/test) environment and for a specific period of time, to identify suspicious communications
PRE_030	PRECOG Supply Chain Assessment Toolkit should identify suspicious communications utilizing T5.4 Deep Learning Data Analytics Module
PRE_031	PRECOG Supply Chain Assessment Toolkit shall utilise the R2D2 block chain to protect the integrity of the assessment results
PRE_032	PRECOG Supply Chain Assessment Toolkit should maintain a list of evaluated components on the Device Origin and Supply Chain Toolkit available to the EPES community.
PRE_033	PRECOG should assure secure communication between DSO "Flexibility system" and devices
PRE_034	PRECOG should alarm DSO IT security department in case of detected attack
PRE_035	Validation environment for should be offline.
PRE_036	Environment will be established using virtual machines.
PRE_037	Claudia tool has to be installed in a windows device to detect anomalies to act as EDR
PRE_038	Claudia tool needs dependencies for installation
PRE_039	Carmen needs internet connection to S2 servers

The whole number of requirements is then organised per Product (or WP) and per type. There are requirements defined for each WP, while others are generic, and they are valid for all Products. Moreover, during the definition stage, several types of requirements have been identified. Table 9 presents the distribution of requirements and how they are organised per Product and per Type.

D2.3 – Requirements and Detailed Architecture Design

Table 9 – Number of requirements per Product/WP and per Type

Type of Requirements	C3PO / WP3	IRIS / WP4	PRECOG / WP5	EMMA / WP6	Generic	Total Number per Type
Functional and Data	30	65	27	81	4	207
Look and feel		32		11		32
Naming conventions		1				1
Maintainability and support			1			1
Legal				1	2	3
Operational	7	2		3	2	14
Performance	1	1				2
Security	1	2	1	1		5
Scope of product/work	4	4	8	20	1	37
Usability and humanity	5	2	2	3	3	15
Total Number per Product	48	136	39	120	12	355

Finally, the quantities of requirements according to the priority levels, as appear in “*Volere*” tool, are presented in Table 10.

Table 10 – Number of requirements per priority level

Priority	Top priority 5	High Priority 4	Medium Priority 3	Poor Priority 2	Lower Priority 1
Number of requirements	237	66	16	7	2

6. SYSTEM ARCHITECTURE DEFINITION

6.1 METHODOLOGY AND SGAM ARCHITECTURE

Developing systems and components has become more complex these days as systems in different domains are more connected to other local systems through Internet-based communications. This means that more and more interfaces are created between systems from different manufacturers. This increases the overall complexity of system integration from a requirement's engineering perspective. To overcome this interoperability problem, the Smart Grid Architecture Model (SGAM) has been developed as a general lookout of an overall architecture in the Smart Grid domain [2]. The SGAM considers different perspectives and methodologies regarding the development and conceptualisation of the Smart Grid.

Considering the holistic approach at the basis of the R²D² project and the variety of technologies and assets involved, the SGAM model represents a useful and effective solution to map the process described in R²D² UCs and obtain a project architecture aligned with the reference model. This will facilitate the identification of data flows and the role of each component (whether HW or SW) and actors involved.

The standardised model proposes a structure for eight interoperability levels, organised into three components namely: organisational, informational and technical. Overall, the structure proposes eight interoperability layers, as shown in Figure 6. The three categories of organizational, informational, and technological are used to categorize the eight interoperability levels. The organizational component is composed of economics, business procedure, and the business objective, and it provides support to develop business functions and to identify the components of these functions that are within or beyond the scope of the company. The informational component includes the business Context and the semantic understanding with the aim of converting the organizational features into a suitable information model. The technical component contains the syntactic interoperability, the network interoperability and the basic connectivity levels that are needed to establish networked communication between distributed assets and applications.

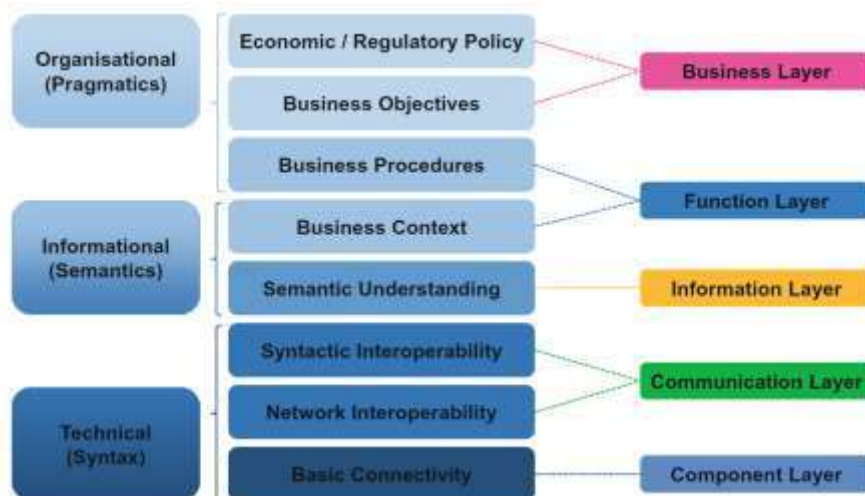


Figure 6 – SGAM interoperability layers: Source: [8]

In order to allow a clear presentation and simple handling of the architecture model, the interoperability levels are aggregated into five abstract interoperability layers described below, following the definition of the “Smart Grid Reference Architecture” document of the CEN-CENELEC-ETSI Smart Grid Coordination Group [2]

Business Layer. The business layer represents the business view on the information exchange related to smart grids. SGAM can be used to map regulatory and economic (market) structures and policies, business models, and business portfolios (products & services) of market parties involved. Also, business capabilities and business processes can be represented in this layer. In this way, it supports business executives in decision-making related to (new) business models and specific business projects (business cases) as well as regulators in defining new market models.

Function Layer. The function layer describes functions and services including their relationships from an architectural viewpoint. The functions are represented independently from actors and physical implementations in applications, systems and components. The functions are derived by extracting the use case functionality which is independent of actors.

Information Layer. The information layer describes the information that is being used and exchanged between functions, services and components. It contains information objects and the underlying canonical data models. These information objects and canonical data models represent the common semantics for functions and services in order to allow an interoperable information exchange via communication means.

Communication Layer. The emphasis of the communication layer is to describe protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service and related information objects or data models.

Component Layer. The emphasis of the component layer is the physical distribution of all participating components in the smart grid context. This includes system actors, applications, power system equipment (typically located at the process and field level), protection and tele-control devices, network infrastructure (wired / wireless communication connections, routers, switches, servers) and any kind of computers.

The five interoperability layers compose the so-called SGAM framework which is a kind of three-dimensional environment (see Figure 7) resulting from the merging of:

- The different power system portions called Domains (generation, transmission, distribution, DER and Customer/Premises),
- The hierarchical levels of power system management are called Zones (process, field, station, operation, enterprise and market) and
- The aforementioned five layers

The description of the domains and the zones are given in the literature, starting from [2] and [8], they are well consolidated in the smart grid projects for many years; therefore the reader can easily refer literature for a full description of such elements.

In addition to the SGAM layers, a final recommendation can be added to facilitate the development phase. In Annex VII a methodology to systematically integrate security and quality measures into software development process is proposed, in order to reduce the likelihood of vulnerabilities and ensuring a higher level of security for the applications. This is not intended to be considered a formal procedure rather than a guidance to Secure

Software Development Life Cycle (SSDLC) that can be eventually applied by partners involved in the development phase.

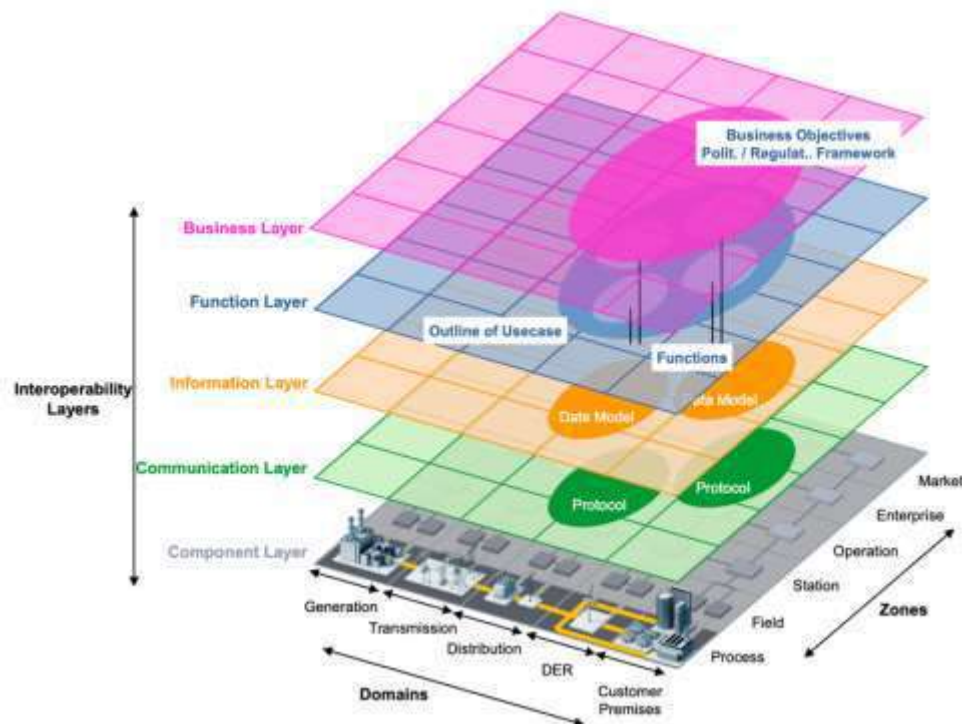
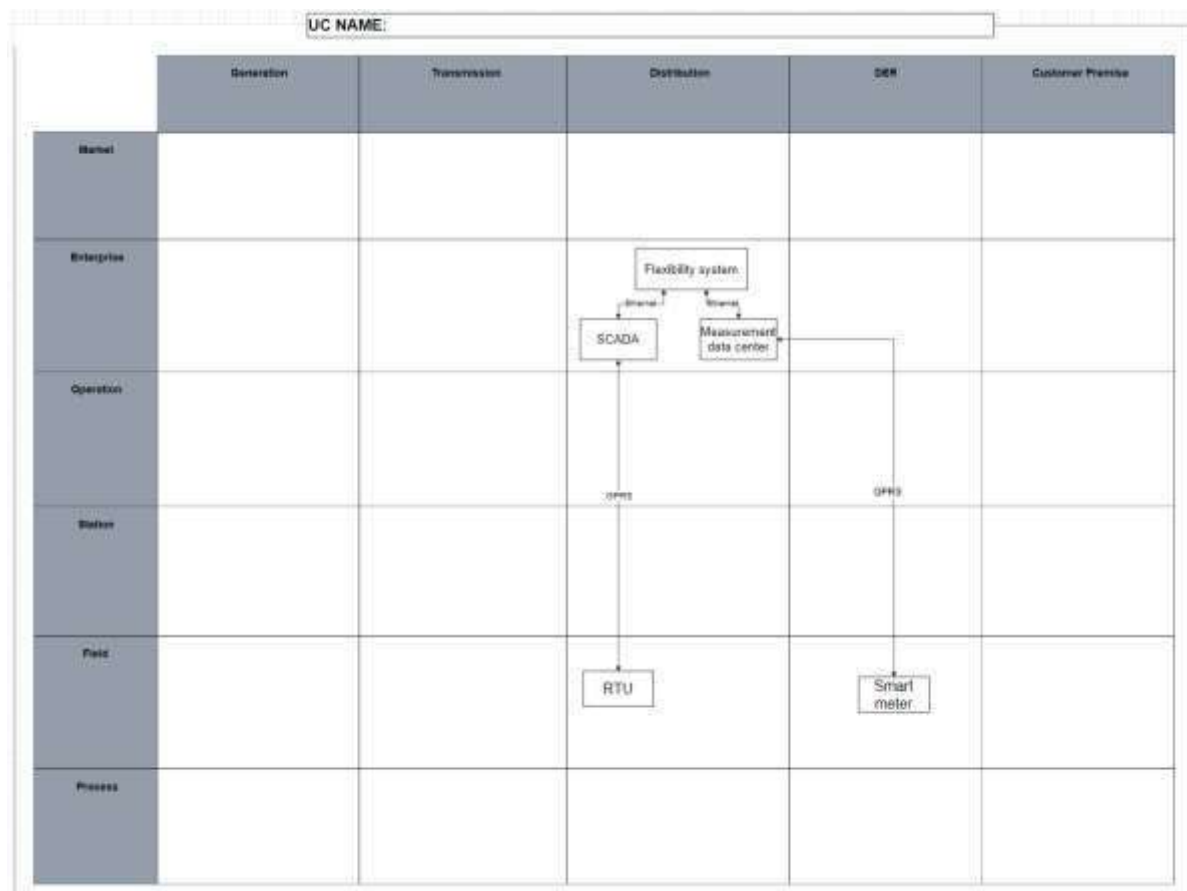


Figure 7 – SGAM Framework

6.1.1 Inputs for the architecture

According to the methodology explained in Section 3, the architecture design of the R²D² solutions will be derived from the SGAM diagrams for each use case presented in Section 4. The representation of all layers for each of the UCs is a process that requires the acquisition of different types of input and information from all partners involved and therefore needs strong coordination and formal rules for representation. In this case, since there are 38 use cases, it was decided to adopt the same domain/zones matrix, as the SGAM framework described before, on which to map the various components and infrastructures included in the UC. These are then related to each other by means of arrows corresponding to a data flow to which the information of the adopted communication standard is added.

For each UC, a diagram similar to the one shown in Figure 8 was created by the partners responsible for that specific UC. The diagrams are for internal use only and they only represent an intermediate step to achieve a full SGAM representation for the UCs. Through these diagrams and the description of the scenarios and steps in the corresponding UCs, it is possible to create the component and communication layers charts for all UCs. A cloud-based free tool was adopted for this activity in order to allow full participation and commitment by all partners.

Figure 8 – Sample of input diagram adopted in R²D²

6.2 SGAM AND USE CASES - COMMUNICATION LAYER DIAGRAMS

With the input information described in previous section (input diagrams and scenarios and steps description from UC definition forms), it has been possible to start sketching the architectural diagrams for all UCs.

As anticipated in section 3, in this version of the deliverable, only the business, component and communication layers diagrams are provided, while the functional and information layer will be included in the second version of Deliverable 2.3.

6.2.1 Business Layer

Specifically, the Use Case Mapping Process goes from the mapping of project objectives into Business Cases (BCs), already presented in section 3.2, to the description of each element defined in the different SGAM layers. As a starting point, the project's objectives are analysed, defining logical actors and business goals for each of them, and this information is the basis for the definition of the BCs.

Under these assumptions and following the description of this layer from section 6.1, in this layer, the business goals, business actors and business use cases are identified. According to [2] a business actor “represents a party that participates in a business

transaction. Within a given business transaction an actor assumes a specific role or a set of roles". In R²D² the following Business Actors (BA) have been identified:

- BA1: Coordination centre operator: "The operator in charge of the activities a regional security centre is responsible for".
- BA2: System Operator: "A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity" [9].
- BA3: Producer: "A natural or legal person who generates electricity" [10].
- BA4: R²D² security actor: A person or a Party responsible for the cybersecurity of IT and OT in a system. Given the specific goals of this project, it has been decided to introduce this actor, dealing with critical BCs and UCs in the project.

Regarding the business goals, R²D² projects tend to coincide with the innovation challenges defined in the DoA. Figure 9 presents Business Goals (BG), BA and BCs in one unique chart.

Furthermore, in R²D² architecture the business layer is the only layer which is not mapped against the typical domains/zones plane explained before, while it follows a more generic UML representation to represent the interactions among BCs, goals and actors. Given the multiple interactions that are established among BCs, BAs, and BGs in the following diagrams (Figures 9 to 13) the interdependencies are shown from the point of view of the Actors; so for each BA, the BGs are represented along with dependencies of BCs, while the relationships between BCs and UCs have been already reported in

Table 6.

BUSINESS GOALS		BUSINESS CASES		BUSINESS ACTOR	
BG1	Demonstration of measures to minimize TSO and DSO risks, vulnerabilities and of priority strategies and measures against nature and man-made hazards.	BC1	To contribute to the improvement of the overall security and resiliency in power system	BA1	Coordination centre operator
BG2	Application of advanced information technologies in system development, operation and asset management.	BC2	To deliver a toolkit to model the impact of high-impact low-probability events, such as natural disasters, on power system in order to assess its resilience and determine the optimal operational planning measures and investments to enhance power system resilience	BA2	System operator
BG3	Application of digital technologies for ensuring operational data quality and demand patterns recognition improving data access and information acquisition for maintenance operators	BC3	To increase the cyber-security and cyber-resilience in OT and IT of the EPES	BA3	Producer
BG4	Development of shared knowledge basis within European area concerning threats, vulnerabilities, methods, not only for components but for entire systems and energy system technologies	BC4	To enhance coordination, interaction and information exchanges at regional level between RSC-TSO, TSO-TSO and TSO-DSO during critical and emergency conditions	BA4	R2D2 Security actor
BG5	Development and application of technology for the identification and authentication of energy IoT devices, authentication of origin in spare part management, trading certificate infrastructures, protection relay configuration and microgrid management	BC5	To deliver a toolkit to improve the reliability of electrical assets and to contribute to the enhancement of the resilience of the network's components through advanced data-driven solution and automated & robotic technologies		
BG6	Development, testing and demonstration of advanced intrusion detection and prevention systems for energy infrastructures including security-related data and deep learning methods	BC6	To demonstrate project impact and replicability potential during the project and beyond the project activities		
BG7	formulate recommendations for standardisation and certification, and propose policy recommendations on EU exchange of information	BC7	To contribute to the development of a shared knowledge		
BG8	Development and application of methodologies for automation of grid maintenance, advanced human-machine interfaces, and of data validation processes automation by applying emerging technologies				

Figure 9 – Representation of R²D² Business Goals, Actors and Business Cases

D2.3 - Requirements and Detailed Architecture Design

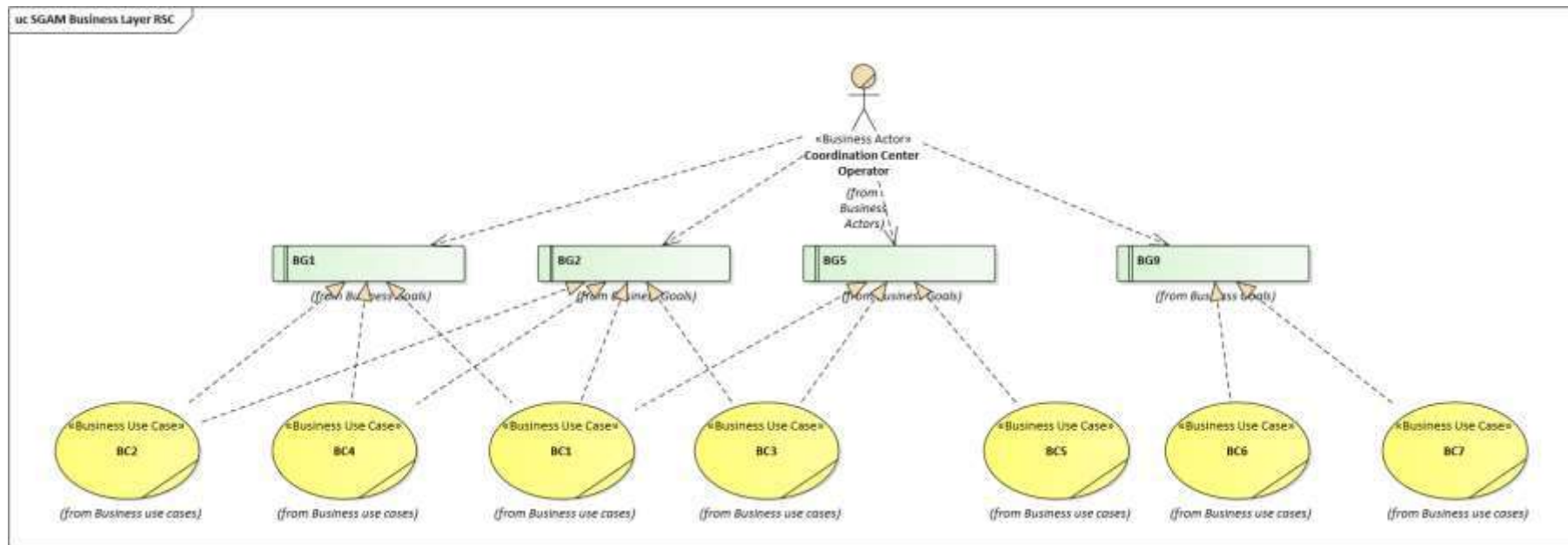


Figure 10 – BA1-centric business layer diagram

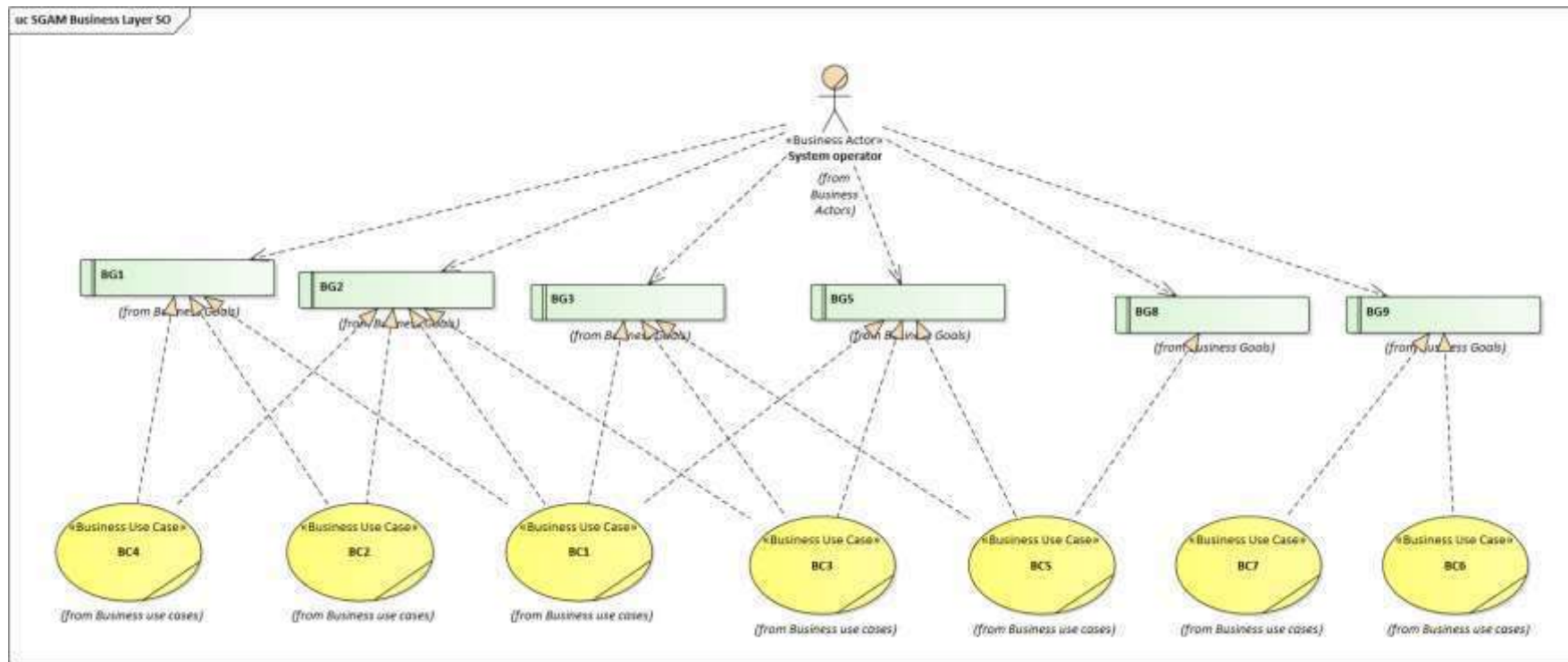


Figure 11 – BA2-centric business layer diagram

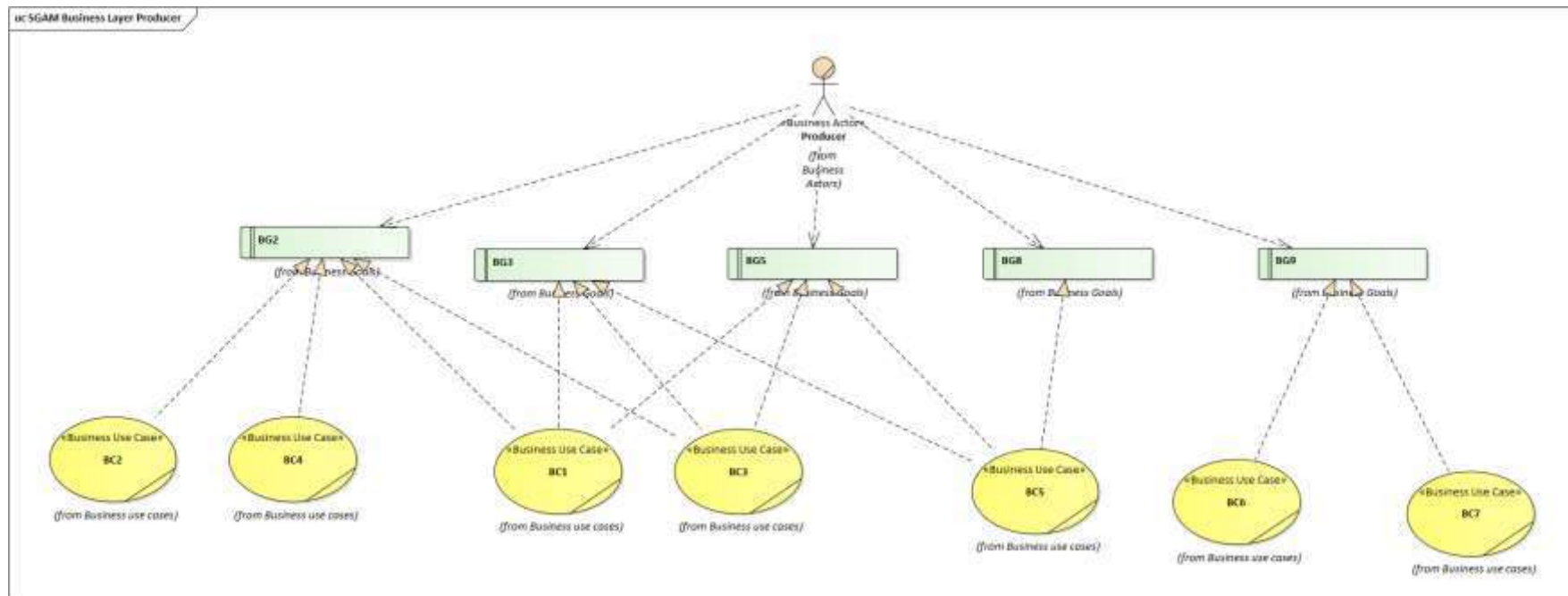


Figure 12 – BA3-centric business layer diagram

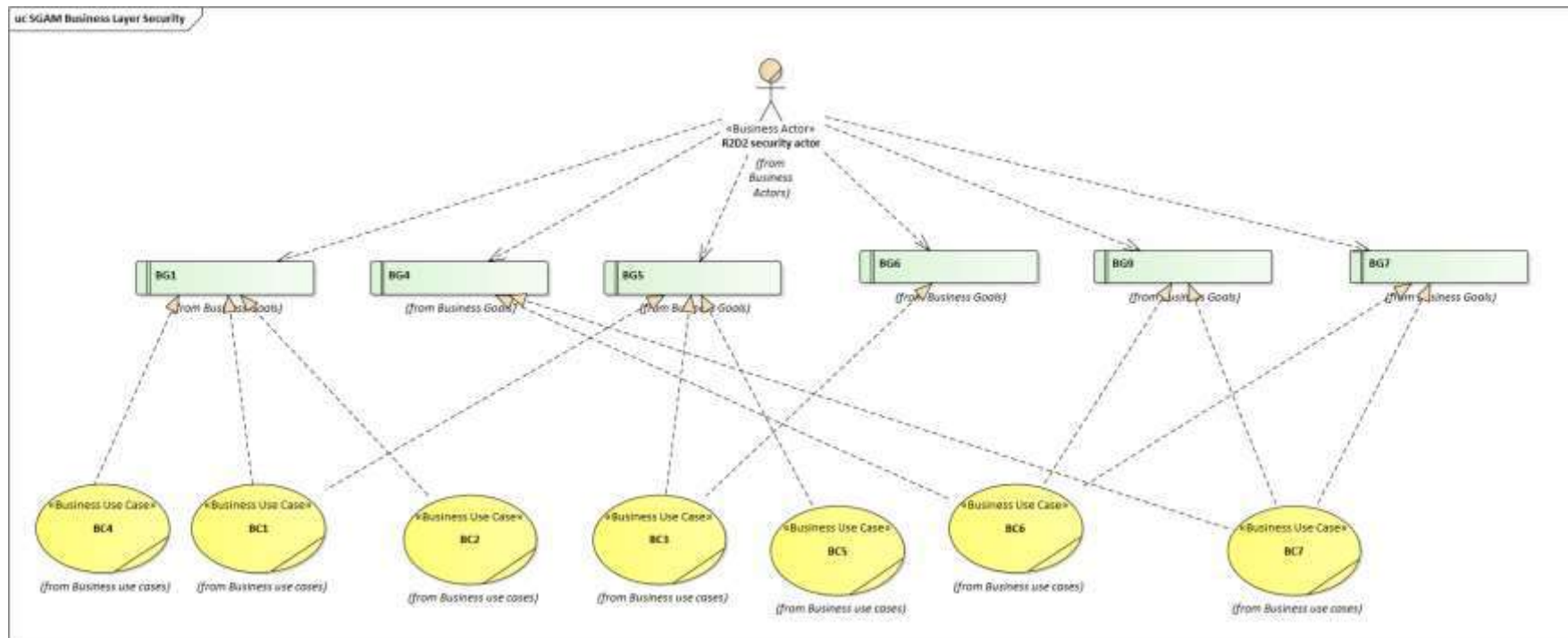


Figure 13 – BA4-centric business layer diagram

6.2.2 Component Layer

In the component layer, all the physical elements participating in the UC are mapped in the SGAM plane, whether they are ICT or electrical components, according to the domain and zone they belong to. Both electrical and communication flows are also depicted in the layer, and it is possible to use different colours to differentiate the connections. In Figure 14 an example of a component layer diagram is shown with a zoom on components in the bottom. For a matter of space in the body of this report, the component layer diagrams for all UCs are presented in Annex IV. UC 28 is the only one without architectural diagrams because it does not include any development or testing activity, but it is aimed at providing best practices in its application field.

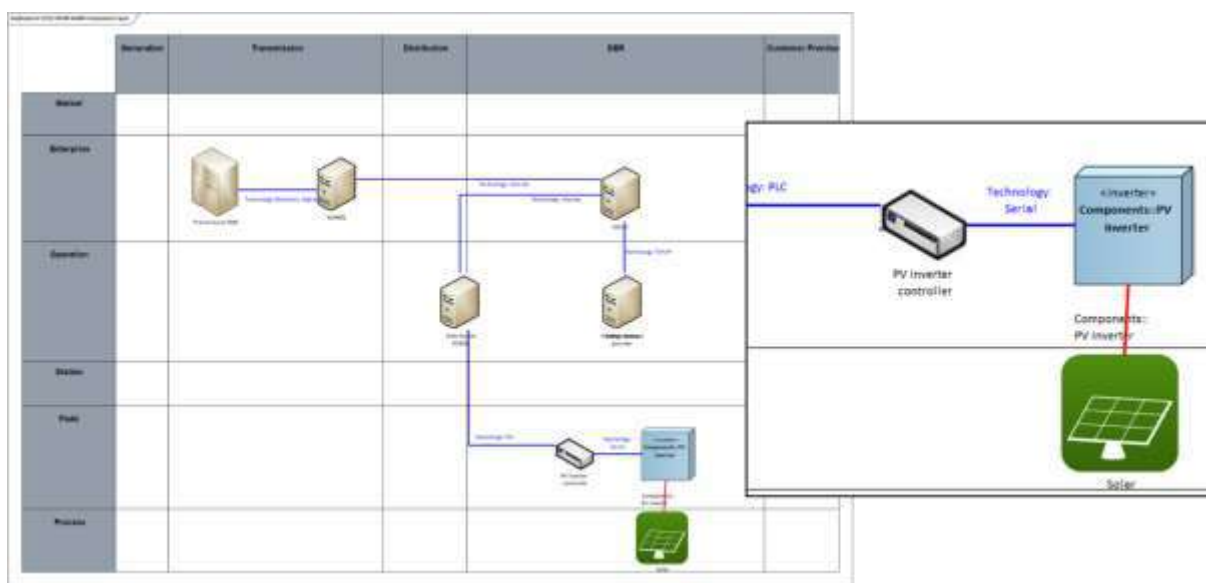


Figure 14 – Example of Component layer diagram

6.2.3 Communication Layer

The communication layer diagram aims at representing all the ICT communications and transmission protocol information against the infrastructure included in the UC (typically represented at the bottom of the diagram in the process domain). It has been possible to complete this category of layer thanks to the information from the input required to partners (see previous section) and the description of the procedural steps of the scenarios included in all UCs (section 4.2.2). In Figure 15 an example of a communication, layer diagram is shown with a zoom on components on the left side of the chart.

For a matter of space in the body of this report, the communication layer diagrams for all UCs are presented in Annex IV. UC28 is the only one without architectural diagrams, because it does not include any development or testing activity, but it is aimed at providing best practices in its application field.

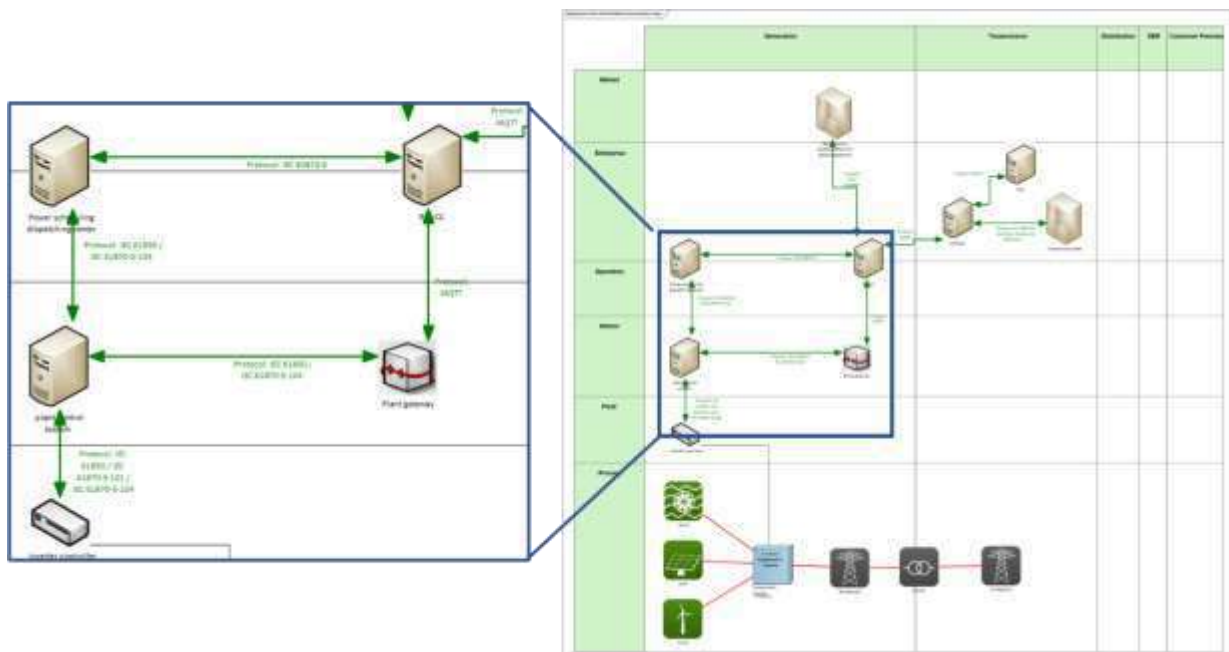


Figure 15 – Example of communication layer diagram

6.2.4 Function Layer

The Function Layer aims to define functions and services from an architectural point of view. It basically includes all services and algorithms that a specific use case provides. These services depend on the corporate vision, and they are not decoupled from the actors involved and the physical implementation in applications, systems and components [2].

In order to complement the function layer diagram two more types of diagrams have been provided (not specific to SGAM modelling):

- i) The activity diagrams and
- ii) The sequence diagrams are depicted in Annex IV.

In Figure 16 an example of a function layer diagram is shown, while in Figure 17 - Example of Sequence Diagram under the Function layer

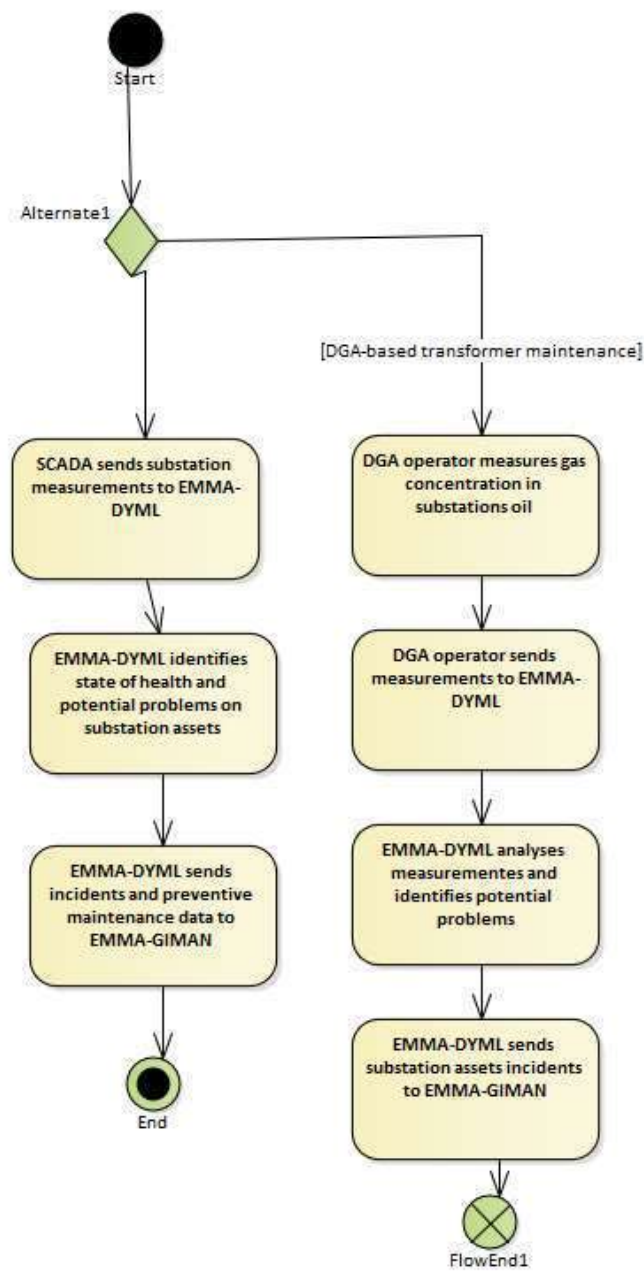


Figure 18 - Example of the Activity Diagram under the Function Layer
and 18 sequence and activity diagrams are provided.



D2.3 - Requirements and Detailed Architecture Design

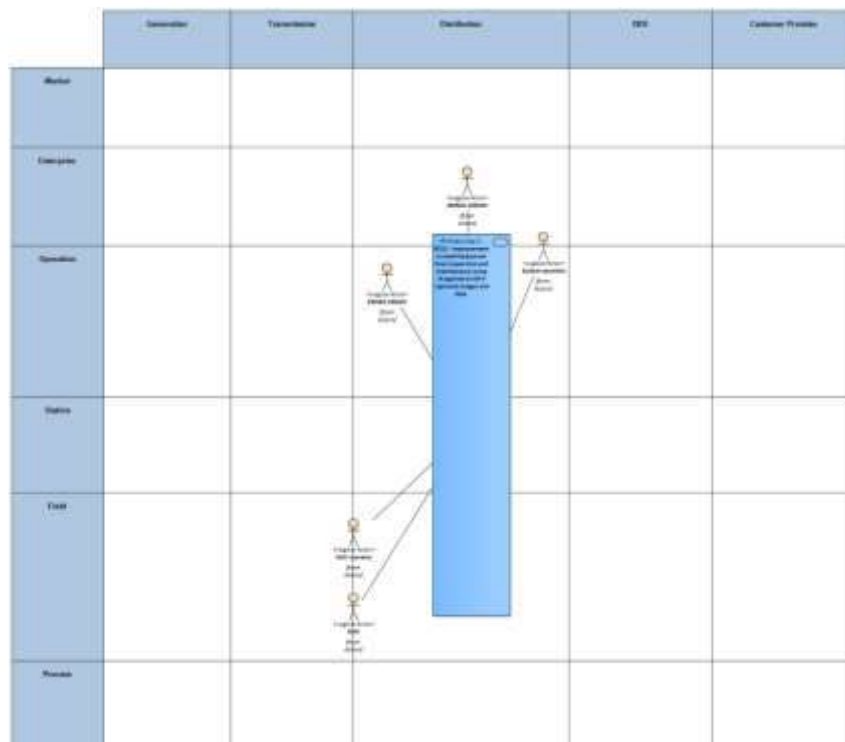


Figure 16 - Example of Function layer diagram

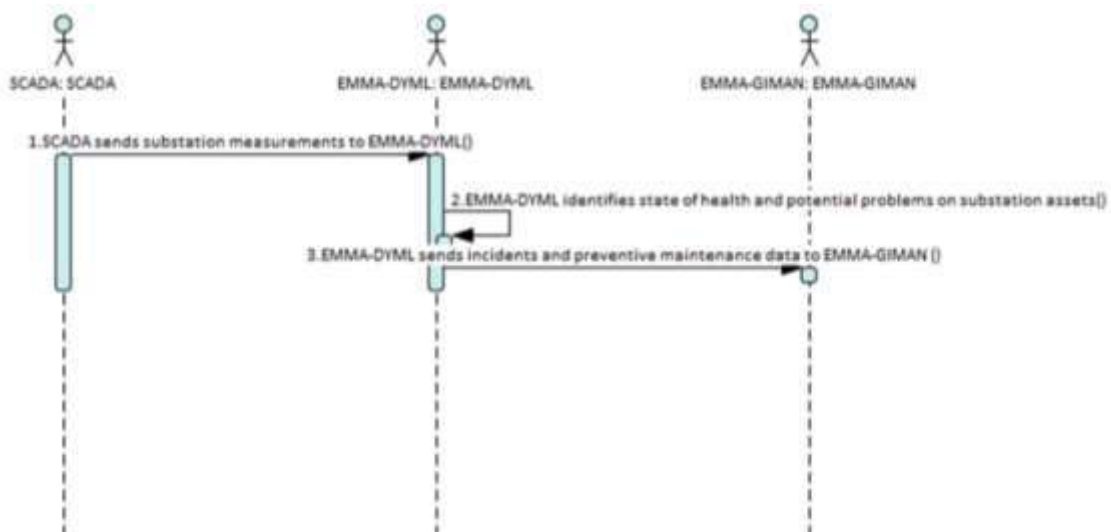


Figure 17 - Example of Sequence Diagram under the Function layer

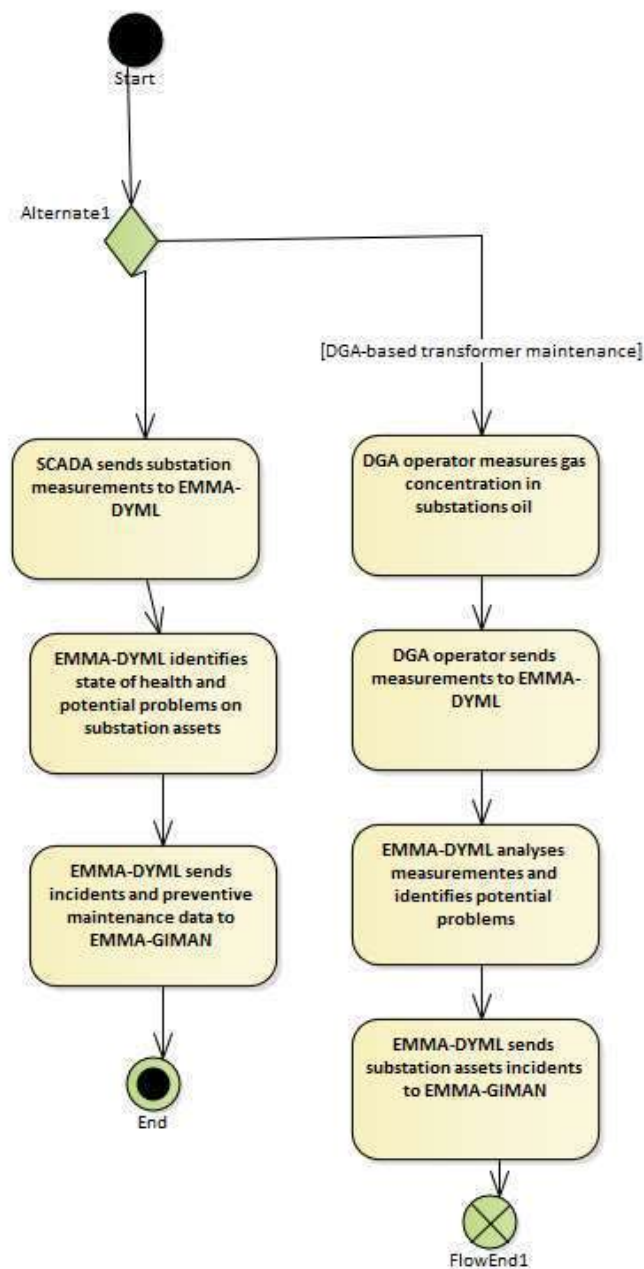


Figure 18 - Example of the Activity Diagram under the Function Layer

6.2.5 Information Layer

This layer aims to describe the information that is exchanged between actors (more precisely, systems and components). It includes information objects and their canonical data models that represent the common semantics for functions and services to enable interoperable exchange, e.g. CIM and EDIFACT for network and client data exchange.

Two SGAM diagrams are reported for the information layer:

- Business Context view and the Standard (Figure 19) and

- Information Object Mapping within the SGAM framework (Figure 20)

Finally, an additional diagram has been added in the information layer to facilitate the representation of the information flows: i.e. the canonical data model representation, represented given in Figure 21, will be added in the information layer.

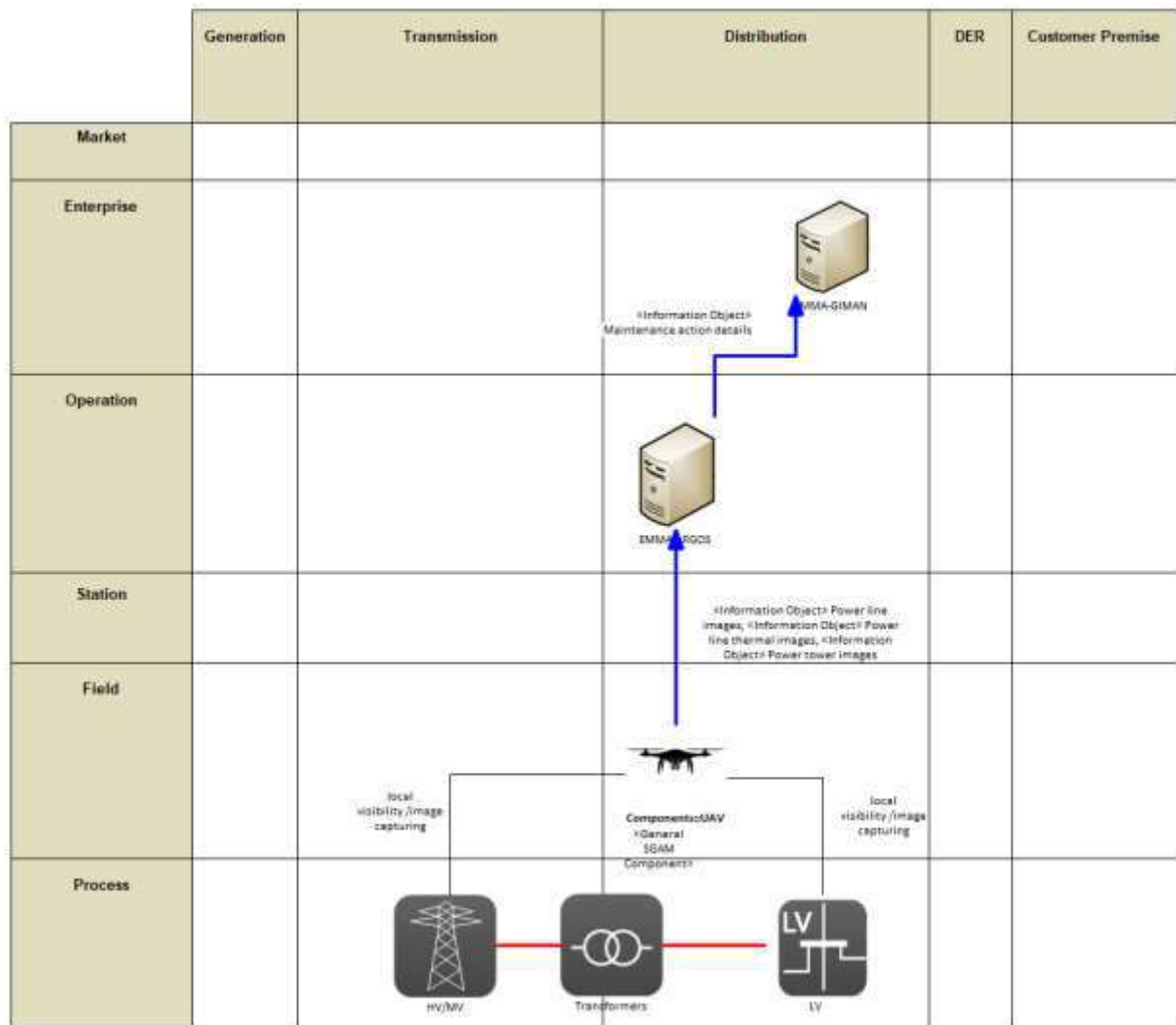


Figure 19 - Example of Information layer diagrams: Business Context view within the Information Layer

D2.3 - Requirements and Detailed Architecture Design

	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 20 - Example of the Standard and Information Object Mapping diagram within the Information Layer

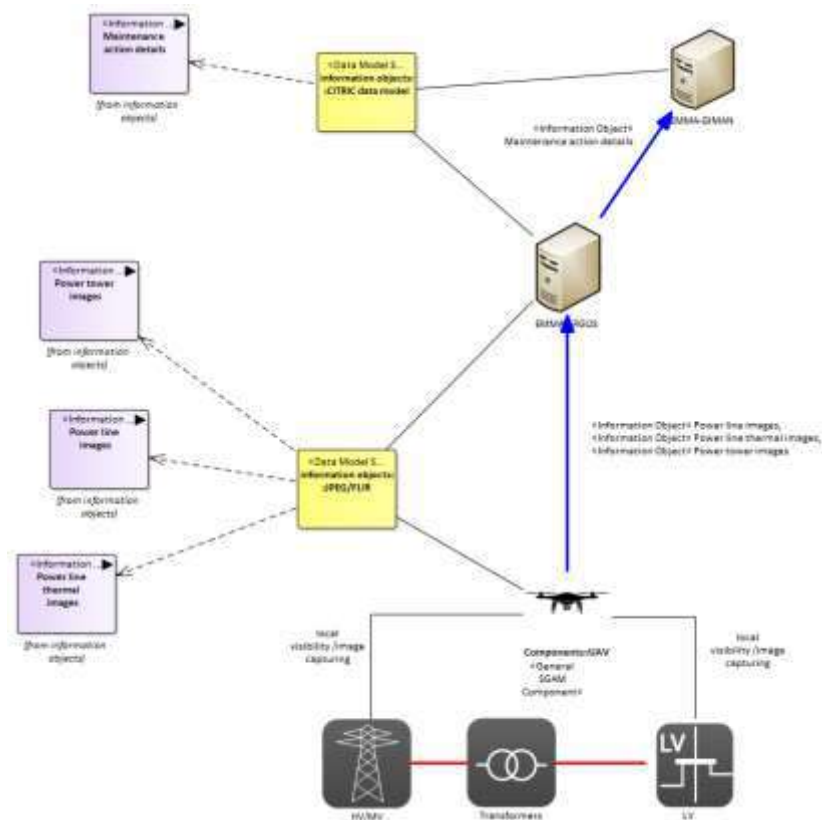


Figure 21: Example of a canonical data model representation within the Information Layer

7. KPI IDENTIFICATION AND MONITORING PREPARATION

7.1 INTRODUCTION AND METHODOLOGY

The objective of this task is to define and develop the quantification method of specific key performance indicators (KPIs) that will evaluate the success of the demonstrations throughout R²D². The KPIs will also be used to calculate the project impact and to elaborate on the replication and scaling-up of the project results in WP7 and WP8.

To achieve the objective of this task, it is essential to closely coordinate with the work on the definition of the R²D² use cases (Section 4) in order to clearly define the KPIs to be proposed and quantified by the respective leaders of the use cases. Hence, there is a strong interrelation with Section 4 in order to develop a consistent framework for first defining the project use cases and then collectively agreeing on the KPIs to be defined and quantified by the products and demo pilot sites of the project.

7.2 METHODOLOGY FOR DEFINING, QUANTIFYING AND MONITORING KPIS

The methodology applied for identifying, quantifying, monitoring and reporting KPIs is shown in Figure 22. First, the output of the use case creation process (Section 4) is utilized for defining the KPIs by the lead partners of each use case. These KPIs are linked to specific products and demo pilot sites of the project. As such, they are next reviewed by the product and demo leaders in order to define and agree on their relevance, practicality and feasibility.

Once the KPIs are agreed upon, the use case leaders have completed a comprehensive template that has been explicitly developed for gathering the information needed for quantifying, monitoring and reporting their respective KPIs. This process is critical in order to ensure consistency in the practices applied in the project regarding the reporting of KPIs. This template (Annex V), among other information, includes the following:

- **Basic KPI information:** This includes the fundamental information and description of the specific KPI, including name, demo/product/use case it applies, description, mathematical formulation, unit of measurement, target/threshold, and reporting period. This information is utilized in the next part of the template to define the KPI calculation steps.
- **KPI calculation methodology:** This part of the template outlines a step-by-step process on how to calculate the defined KPI, with a clear indication of the person and partner responsible for specific steps in KPI calculation methodology, etc. This is very important in the process of allocating clear responsibilities and accountability to the partners in order to ensure the smooth and seamless KPI calculation.
- **KPI data collection:** This section of the KPI template refers to the methodology and tools to be deployed for collecting the necessary data for the KPI quantification. In this context, in this section the data type, methodology for data collection,

source/tools/instruments for data collection, location of data collection, frequency of data collection, responsible person/partner, etc. are described in detail. This allows the collection of the relevant and necessary data for deploying the mathematical quantification of the KPI as defined in the first section of the template.

- **KPI baseline:** In order to demonstrate the effectiveness of a tool, product, etc. a baseline value is necessary. This section of the template aims to provide this baseline value of the KPI explicitly to allow a constructive comparison and benefit quantification of the proposed R²D² solutions. In this context, literature values of the KPI are first provided, accompanied by company historical values, if available. Also the KPI values measured at the start of the project are also provided to enable the effective comparison by the end of the project.

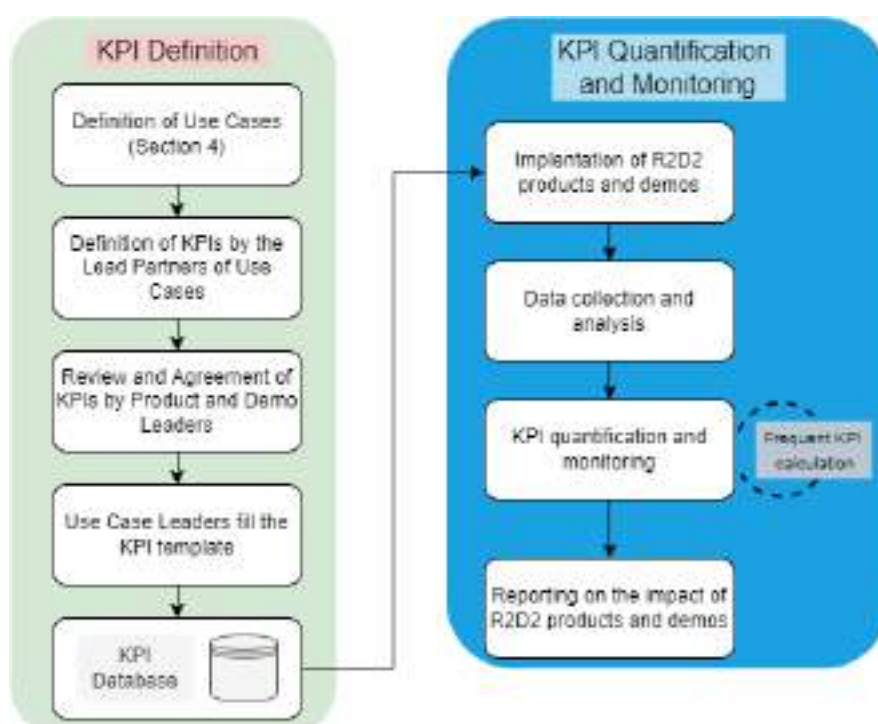


Figure 22 - Methodology for defining, quantifying, monitoring and reporting KPIs

Once the use case leaders fill their respective KPI templates, the database containing all the R²D² KPIs was developed. This KPI database will then be used in the "KPI Quantification and Monitoring" phase which will be performed in WP7 (T7.4) and WP8 (T8.4). This includes the data collection and analysis from the implementation of the R²D² products and demos. Based on the details imported by the use case leaders in the KPI template, the procedure for collecting, processing and analysing the data will be applied. This process will be repeated at the frequency defined in the template in order to ensure the continuous quantification and monitoring of the defined KPIs. Finally, the findings of the KPI quantification and monitoring will be reported in order to showcase the impact of the R²D² products and demos.

It is important to note that the R²D² KPIs are preliminarily classified as follows:

- **Physical infrastructure KPIs**, such as SAIFI, average response time for customer re-electrification under extreme weather events, and restoration time of a damaged component under extreme weather events
- **Cyberinfrastructure KPIs**, such as attack detection rate for new assets to be integrated into the EPES, Mean Time to Detect cyber-security issues, and Mean Time to Resolve cyber-security issue
- **Dissemination and communication KPIs**, such as number of scientific publications, Number of newsletters published, participation in events/workshops/conferences at local/national/international level and workshop organization with stakeholders
- **Wider impact KPIs**, such as the number of potential customers of the R²D² products, creation of new jobs (contractors, equipment manufacturers) and implementation of a shared knowledge repository

7.3 LIST AND ANALYSIS OF KPIS

Building on the preliminary KPI analysis outlined in [11], the full template of the defined KPIs have been completed in this period of the project. As shown in Table 11, in total 40 KPIs have been defined for the R²D² use cases as in the project proposal ("Project KPIs"), while 5 complementary KPIs were defined to holistically capture the performance of the R²D² technological solutions. Annex VI provides the completed information for the quantification of all the R2D2 KPIs as prepared by the respective UC and KPI partner leaders. This KPI database (as seen in Fig. 22) provides a comprehensive methodology for quantifying a wide range of KPIs.

This provides a holistic measurement and demonstration of the importance and real-world impact of R²D² demonstrations, products and tools. The demo site of each KPI has been commonly discussed and agreed with the demo leaders to ensure the successful delivery of the defined KPIs for each use case.

It is important to note that these KPIs span across a wide range of activities and outputs from R²D², including for example:

- Cyber and physical KPIs
- Energy efficiency
- Policy outputs
- Social impacts
- Commercialization opportunities, etc.

Also, each use case has been allocated a minimum of one KPI with some use cases being allocated up to several KPIs to provide a comprehensive understanding and impact quantification of the use cases. It is also possible that some of the KPIs will be demonstrated using more than one demo site in order to enhance the possibility of successful delivery.

Table 11 below summarizes the mapping of use cases on the KPIs defined in the project proposal and the complementary KPIs. It is apparent that each KPI is assigned to at least one use case, which demonstrates the efficiency of the systematic approach for developing the R²D² use cases so as to quantify all R²D² KPIs. Table 12 below summarizes the KPIs across all use cases defined for each of the R²D² products. It can be clearly seen that each product has

D2.3 – Requirements and Detailed Architecture Design

been allocated a large number of KPIs in order to holistically quantify and demonstrate their impact.

Table 11 – Use Cases vs KPIs mapping

ID	KPI	Business Case	Use Cases
PROJECT KEY PERFORMANCE INDICATORS			
1	SAIDI (reduction in minutes)	BC1	1, 2, 8, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22
2	SAIFI	BC1	2, 8, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22
3	CAIDI	BC1	2, 8, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22
4	Average Service Availability Index	BC1	1, 2, 8, 10, 11, 12, 13, 14, 15, 16, 17, 19, 21, 22
5	Customers Experiencing Multiple Interruptions	BC1	2, 6, 8, 12, 13, 14, 15, 16, 17, 19, 20, 21, 22, 29, 30
6	Average response time for customer re-electrification under extreme weather event	BC1	1, 12, 19, 22, 30, 32
7	ENS (MWh/year)	BC2	6, 7, 8, 9, 10, 11, 13, 15, 16
8	AIT (minutes/year)	BC2	8, 12, 13, 14, 15, 16, 17, 29, 21, 22
9	Restoration time of a damaged component under extreme weather events	BC2	2, 5, 6, 22, 30, 32
10	Increase of the data availability and easier data exchange among system operators during emergencies	BC2	7, 11
11	Number of internet-connected devices to be protected by R ² D ² s solutions	BC3	4
12	Number of SCADA and ICS networks used in control centres and related control and monitoring facilities that will be made cyber resilient	BC3	27
13	Number of smart meters and edge devices that will be made cyber secure with R ² D ²	BC3	4, 7, 10, 25
14	Attack detection rate for new assets to be integrated into the EPES	BC3	20, 39, 40
15	Mean Time to Detect cyber-security issue (MTTD)	BC3	25, 33, 34, 39, 40
16	Mean Time to Resolve cyber-security issue (MTTR)	BC3	25, 39, 40



D2.3 – Requirements and Detailed Architecture Design

17	Number of notifications exchanged with R ² D ²	BC4	11, 23, 40
18	Number of security constraints treated with R ² D ²	BC4	20, 24
19	Number of inadequacy cases resorbed	BC4	24
20	Number of notifications exchanged with flexibility providers (RES producers and dispatchable loads)	BC4	6, 11, 12, 21
21	Increase of renewables in the energy mix	BC4	12, 13, 14, 15, 21, 31
22	Increase of distributed RES capacity	BC4	1, 3, 7, 12, 14, 15
23	Reduction of greenhouse gases emissions	BC4	12, 13, 14, 15, 21, 31
24	Number of assets analysed through R ² D ²	BC5	1, 2, 3, 4, 6
25	Accuracy of predictive maintenance estimation	BC5	1
26	Assets Down-time Reduction	BC5	1, 6, 8
27	Detection of NTL patterns	BC5	4
28	Cost of the activities related to equipment maintenance	BC5	1, 2, 6, 9, 32
29	Creation of new jobs (contractors, equipment manufacturers)	BC6	2
30	CAPEX Reduction or deferral in upgrading grid infrastructures	BC6	4, 6
31	OPEX Reduction	BC6	1, 2, 4, 6
32	Number of new commercial opportunities and cooperation among stakeholders analysed	BC6	2, 13, 19, 24
33	Number of potential customers of the R ² D ² products	BC6	4, 6, 7, 8, 9, 12, 13, 14, 15, 16, 17, 18, 19, 21, 31
34	Number of recommendations provided to replicate project solutions and ensure scalability / repeatability beyond the project	BC6	32, 36
35	Implementation of a shared knowledge repository	BC7	25
COMPLEMENTARY KEY PERFORMANCE INDICATORS			
36	Number of DSO/TSOs and vendors to be evaluated by the Supply Chain Assessment Toolkit/Self Assessment Tool.	BC4	28
37	Number of supply chain Cyber Security best practices to be considered	BC3	28
38	Measurement of the TSO/DSO cooperation for common grid model creation	BC4	36



D2.3 – Requirements and Detailed Architecture Design

Input situations for crisis analysis and aligned forecasts for adequacy situations

39	KSI tool must confirm integrity of original files on 100% of cases, when verification function is applied on originally signed data.	BC5	37
40	Accuracy of tokenization tool	BC6	38

Table 12 – Products vs KPIs mapping

R ² D ² Product	Product Description	Relevant KPI IDs
P1 – C3PO	C3PO contributes to a systematic, disciplined, and repeatable approach for evaluating an energy system security strategy	1, 2, 3, 4, 5, 6, 7, 8, 14, 15, 16, 18, 19, 21, 22, 23, 24, 29, 30, 31, 32, 33, 34, 35
P2 – IRIS	IRIS intervenes when coordination between system operators is needed for security reasons	10, 17, 20, 22, 23, 29, 31, 32, 33, 34, 35, 36, 38
P3 – PRECOG	PRECOG provides a cybersecurity framework to OT and IT	11, 12, 13, 14, 15, 16, 17, 18, 19, 24, 27, 29, 32, 33, 34, 35, 37, 39, 40
P4 – EMMA	EMMA contributes to the reliability of the physical assets and to expedite a faster grid recovery	1, 6, 9, 19, 25, 26, 28, 29, 30, 31, 32, 33, 34, 35

8. CONCLUSIONS

According to the R²D² project plan, this report is prepared in month 16 (M16) of the project life, which is the final month of the Work Package 2, as a final report on Requirements and Detailed Architecture Design. Therefore, this section presents the main conclusions on the results of Work Package 2 related to this topic.

The following paragraphs briefly describe conclusions related to:

- Use cases
- Requirements
- System Architecture
- KPIs

It can be said that all necessary use cases have been identified and defined in detail manner. In order to define these use cases, the relevant methodology provided within the international IEC 62559 standard was used, which refers to Unified Modelling Language. This standard contains a structured use case definition form that contains all the key information about use cases, such as: general information, use case purpose, actors involved, use case scenarios, diagrams, KPIs, definition of used terms... The R²D² project team decided to use these forms as an expression of best practice in this field and based on the recommendations of the relevant organizations under whose auspices this project is taking place.

The experience of the project team with the use of these forms is positive, because they greatly facilitated further activities, because based on them, data and relationships between them, which are necessary for defining requirements and SGAM diagrams, were easily extracted. In addition, it was noticeable that through these forms, communication between future R²D² product users and developers was facilitated. In this way, the work in WP2 fulfilled its purpose because it laid a good foundation for further R²D² products development, which is the subject of WP3-WP6.

It has already been noted in the previous text that use cases cover all relevant business cases and all products, that is, all tasks that R²D² products should fulfil. The distribution of use-cases between R²D² products is relatively uniform. Thus, 2 products, C3PO, IRIS each have 9 use cases, PRECOG has 10 use cases, while the product EMMA has a slightly higher number of use hours - 13 in total.

The development of the electricity market is in full swing, and in the last decade the EU has produced numerous documents (the Third Energy Package including network codes and guidelines, Clean Energy Package). All this obliged the key actors on the market, and above all the system operators, to establish new business processes, or to significantly reshape the existing ones. In order to do this, it is necessary to create a large number of tools, and a significant number of UCs relate to these tools, in order to accompany the energy transition towards the Green Agenda (RES, DER...). On the other hand, cyber security was not so much in focus, but recent events on the global political scene have led to the fact that this type of security must be paid much more attention in the future.

After the completion of products' design in deliverables D3.1, D4.1, D5.1 and D6.1, in parallel with the refinement of the UCs the finalization of the requirements has been performed as well, resulting in the final version of the list of the requirements. When defining

the requirements, the Volere methodology was adopted, and the application of the methodology was facilitated by the web-oriented Volere tool. In principle, we can say that the requirements were created through two perspectives. The first perspective is related to the definition of requirements through the definition of use cases. Such requirements can be also found in Annex I of the use case definition forms. The second perspective is related to global requirements for R2D2 products, and such requirements were only entered into the Volere tool. All partners were asked to study all requirements in order to identify and eliminate potential deficiencies, conflicts, and the like. Special attention was also paid to whether a specific requirement is in conflict with the technical capabilities of the demonstration pilot site. Of course, during the final verification of requirements, it was very important to establish direct communication between the creators of use cases and product developers. This kind of work resulted in a very detailed list of requirements, the number of which reached 355. However, as WP2 ends with this Report, and work on product development continues through WP3 - WP6, it will inevitably happen that some of the requirements will be modified, others will be abandoned, and numerous other requirements will also be defined (before only the so-called non-functional requirements related to the design of the user interface and the feel of the system).

Similarly, with the refinements of use cases and requirements it was possible to complete the SGAM architecture for R²D² solutions. SGAM diagrams were used in the context of the general application of Unified Modelling Language in this project (it has already been mentioned that even use-cases represent only one of many diagrams). SGAM diagrams were used as a best practice for communication between creators of use cases and product developers, but also between members of the developer teams themselves. The work on SGAM diagrams led to a review and eventual correction of both the definition of use classes and individual requirements. In the first phase of work, which is covered by [11], SGAM Component Layer and SGAM Communication Layer were created. In the period between the release of [11] and this report, the SGAM architecture was completed with SGAM Information, Business and Function layers, along with the activity and sequence diagrams that were needed to describe properly each one of the use cases. If a use case contains several scenarios, all these scenarios are covered by the corresponding SGAM diagrams. This approach led to the fact that 40 use cases are described through 355 SGAM diagrams, which are attached to this document.

With regards to the KPI definition, it is necessary to outline in detail the required steps for collecting, processing and reporting key data from the demo sites of R²D². This process is described in detail in deliverable D2.3 which includes the KPI calculation methodology and KPI data collection methodology. A clear definition of each KPI is developed, including its description and mathematical formulation. This enables the completion of the KPI database which will then be used in WP7 and WP8 for measuring and demonstrating the impact of the R²D² demos. During this procedure, the responsibilities of the partners are clearly defined to enable the seamless collection of the necessary data for quantifying the R²D² KPIs. In order to achieve this, the UC and demo leaders worked very closely and effectively to analyse the KPIs and define the main steps needed for performing the research and demo tasks required. The benchmarks for each of the KPIs are also defined in order to quantify in a practical manner the improvement achieved through the project on the defined KPIs.

9. References

9.1 REFERENCES

- [1] "R²D² Description of Action," in Annex I to the Grant Agreement. EC, 2022.
- [2] CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart Grid Reference Architecture", Standard, Nov. 2012, available at https://syc-se.iec.ch/wp-content/uploads/2019/10/Reference_Architecture_final.pdf website accessed on February 2023.
- [3] ISO/IEC 19501:2005 Information technology — Open Distributed Processing — Unified Modelling Language (UML) Version 1.4.2, available at <https://www.iso.org/standard>
- [4] IEC 62559-2:2015 "Use case methodology - Part 2: Definition of the templates for use cases, actor list and requirements list", International Electrotechnical Commission, TC8, available at: <https://webstore.iec.ch/publication/22349Webstore>
- [5] S. Robertson, "VOLERE – the evolution of successful requirements techniques", 2019, available at https://www.volere.org/wp-content/uploads/2019/07/2019_volere_history.pdf
- [6] A. Mavin, P. Wilkinson, A. Harwood and M. Novak, "Easy Approach to Requirements Syntax (EARS)", *2009 17th IEEE International Requirements Engineering Conference*, Atlanta, GA, USA, 2009, pp. 317–322, doi: 10.1109/RE.2009.9.
- [7] J. Terzakis, "EARS: The Easy Approach to Requirements Syntax" July 21, 2013, ICCGI Conference, Nice, France
- [8] Gottschalk, Marion, Mathias Uslar, and Christina Delfs. "The use case and smart grid architecture model approach: the IEC 62559-2 use case template and the SGAM applied in various domains". Springer International Publishing, 2017.
- [9] ENTSO-E, "THE HARMONISED ELECTRICITY MARKET ROLE MODEL" vers. 2022-01, available at: [Harmonised_Role_Model_2022-01.pdf](https://www.entsoe.eu/~/media/Files/Electricity%20Markets/Harmonised_Role_Model_2022-01.pdf) (entso.eu)
- [10] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU
- [11] D2.1 - Requirements and detailed Architecture design

9.2 ACRONYMS

Table 13 - Acronyms

Acronym	Meaning
AMI	Advanced metering infrastructure
BA	Business Actor
BC	Business Case
BG	Business Goal
CISO	Chief Information Security Officer
CTI	Cyber Threat Intelligence
DER	Distributed energy resources
DGA	Domain Generation Algorithm



D2.3 – Requirements and Detailed Architecture Design

DMS	Distribution Management System
DoA	Description of Action
DSO	Distribution System Operator
EMS	Energy Management System
ENTSO-E	European Network of Transmission System Operators for Electricity
EPES	Electrical Power Energy Systems
EU	European Union
HILF	High Impact Low Frequency
HV	High Voltage
IGM	Individual Grid Model
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicator
KSI	Key Set Identifier
LFSM-O	Limited Frequency Sensitive Mode – Over-frequency
LV	Low Voltage
MV	Medium Voltage
PMU	Phasor Measurement Unit
RA	Remedial Action
RES	Renewable Energy Sources
RCC or RSC	Regional Coordination Centre / Regional Security Coordinator
RTU	Remote Terminal Unit
SCADA	System Control and Data Acquisition
SGAM	Smart Grid Architecture Model
SO	System Operator
TSO	Transmission System Operator
UAV	Uncrewed Aerial Vehicle
UC	Use Case
UML	Unified Modelling Language
WAMS	Wide Area Monitoring System



10. ANNEX I: USE CASE DEFINITION FORMS

In the following subsections of Annex I, the definition forms of the UCs are available.

As mentioned in section 4.2.3, information about KPIs (section 1.5 of the form), diagrams (section 2 of the form) and requirements (section 6 of the form), are missing or partially completed. Full information on these three sections is reported in other parts of this document (requirements in Annex III; SGAM diagrams in Annex IV, and KPIs in Annex VI).

10.1 USE CASE 1 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
UC1	TSO/DSO, overhead lines inspection, maintenance	Improvement in overhead power lines inspection and maintenance using IA applied to UAV-captured images and data

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	18/01/2023	Ugo Stecchi		
0.2	18/01/2023	Sergi Grau		
0.3	23/01/2023	Lucas Pons		
0.4	14/02/2023	Lucas Pons	Steps details	
0.5	08/05/2023	Srđan Subotić	Review	Approved
0.6	30/05/2023	Ugo Stecchi	Improvements after review	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	<p>This use case is aiming at identifying different phenomena at the overhead lines infrastructure that might require some maintenance action from the system operator.</p> <p>The UC covers the identification of:</p> <ul style="list-style-type: none"> - Forest and vegetation that might cause faults in the overhead lines. - Physical (mechanical and/or structural) anomalies. It will consider towers/poles, conductors, and insulators. - Electric “anomalies”. It does not include all the infrastructure composing the overhead lines, but only the conductors (no ground-wire-strands) and insulators <p>The reconnaissance is made by autonomous UAV units configured to work autonomously with predefined reconnaissance mission loaded. The resulting images will be automatically analyzed towards identifying different problematic or dangerous phenomena and pass this information to system operator.</p>
Objective(s)	<ul style="list-style-type: none"> - Autonomous inspection of overhead lines - Develop a tool combining multi-spectral images acquired through different cameras - Identification of electric anomalies in overhead lines as: arcing, partial discharge, imbalance and overheating) - Identification of physical anomalies in overhead lines; - Automatic Identification on the images of forest and vegetation that could compromise the integrity of the overhead lines <p>Improvement of the maintenance activities (faster and more effective procedure)</p>
Related business case(s)	BC1, BC5

1.4 Narrative of use case

Narrative of use case
Short description
UC1 is aimed at automatically and autonomously inspecting through UAV the overhead lines and identifying different phenomena and anomalies that might compromise the integrity of the overhead lines. The anomalies to detect depends on the payload the UAV will be equipped and the configuration of the analytic processes.
Complete description
<p>UC#1 is aimed at testing and validating some functionalities of the EMMA product developed in WP6, T6.1. In particular this UC will take advantage of the algorithm for image detection developed in T6.1 and for the autonomous flight of drones to detect some phenomena in the electric overhead lines that may indicate an upcoming failure or fault.</p> <p>Three different types of phenomena can be identified:</p> <ul style="list-style-type: none"> - Forest and vegetation identification that might compromise the integrity of the overhead lines. Normally this means that vegetation is detected breaking the distance security of the power lines. - Electrical anomalies. Depending on the type of image acquired, the following phenomena can be identified: <ul style="list-style-type: none"> o Optical camera: short circuits or faults o Thermal camera: <ul style="list-style-type: none"> ▪ lines overheating (matching of thermal images and SCADA data), ▪ hot spot on insulators indicating damaged or potential faults ▪ partial discharge ? corona effect - Physical (mechanical and/or structural) anomalies: Damage of towers or poles, mechanic deterioration of supports and insulators, presence of obstacles, element deterioration, or “foreign bodies”. <p>The current state of technology and the regulations of aviation law has led to the development of methods involving the use of a flying system with the following configuration:</p> <ul style="list-style-type: none"> • drone (multirotor) with at least an RGB camera, a thermal camera and a Lidar, equipped with autopilot hardware that allows for autonomous operation, • ground control station (GCS) – a computer running mission planning and mission control software, • radio link with an antenna on a short mast located next to the GCS (for the transmission of telemetry data from the drone to the ground segment). <p>An operator can plan the flight route using GCS software and upload it via radio link to the drone. Once launched, the drone will automatically navigate along this route using GPS positioning and inertial measurement unit.</p>

D2.3 - Requirements and Detailed Architecture Design

The GCS is usually located in the middle of the planned section of the mission, which allows one to observe the multirotor flying in both directions and thus extend the distance of the mission, in those case where the flight is allowed only within the sight limit of the operator.

During the flight, cameras collect videos and/or photos and after the mission is completed, they are streamed to GCS.

After the set of images are stored at the GCS, they can be analysed towards identifying the presence of dangerous forest or vegetation.

This analysis is not (normally) done in the field, close to the mission, but on a second stage, when the GCS returns to the secure infrastructure at the utility premises, the set of images (potentially, several GB of imagery data) is analysed and eventually maintenance warnings and alarms are triggered based on the results of the analysis.

Image processing will be based on multiple segmentation models, where the first one will identify the overhead line infrastructure asset (power lines, insulator, poles, etc.) and the other will detect the potential problems.

The predicted warnings and alarms, as well as the mission details, will be shown in a dedicated graphical user interface.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
UAV can flight over overhead lines to capture images. The appropriate legal permissions have been obtained and a person with appropriate skills can is available to fight the UAV
Prerequisites
The geographical location of the overhead line poles is known in advance

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
n/a
Level of depth
Detailed
Prioritisation
5 (High)
Generic, regional or national relation
generic
Nature of the use case
Technical use case
Further keywords for classification

1.8 General remarks

General remarks
ARGOS: IA image-based maintenance EMMA module

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
System operator	Role	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity	For this UC, a DSO is covering the role of a System Operator actor. In case the UC is focused on HV lines, it can perfectly works with TSO as well.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
UAV	Device	An autonomous self-moving device that is guided autonomously, by remote control, or both and that carries sensors, cameras for surveying, monitoring and inspection purposes	
UAV inspection operator	Human	Person in charge to supervise the mission of the inspection robot, mainly in charge of starting, cancelling, finishing and supervising the mission	
EMMA ARGOS	Application	IA image-based maintenance EMMA module SW platform developed under R2D2 with capabilities to acquire and analyse multi spectral images to monitor PV panels and identify possible failures.	

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Forest and vegetation reconnaissance	Forest and vegetation reconnaissance that may cause possible faults with overhead lines, through autonomous images and lidar UAV acquisitions	UAV inspection operator	UAV inspection operator performs a flight over an overhead line	Mission details are pre-loaded in UAV (flight details, capturing details, etc...)	Utility obtains precise location of potentially dangerous forest and vegetation that might damage the overhead lines or poles
2	Damages detection	Damages detection in overhead MV lines through autonomous UAV multi-spectral image acquisition	UAV inspection operator	UAV inspection operator performs a flight over an overhead line	Mission details are pre-loaded in UAV (flight details, capturing details, etc...)	Utility obtains precise location of phenomena in the physical structure of towers/poles, conductors, and insulators that may indicate an upcoming failure or fault
3	Electric anomalies detection	Electric anomalies detection in overhead MV lines (arcing, partial discharge, imbalance, overheating) through autonomous UAV multi-spectral image acquisition	UAV inspection operator	UAV inspection operator performs a flight over an overhead line	Mission details are pre-loaded in UAV (flight details, capturing details, etc...)	Utility obtains precise location of some phenomena in the electric overhead lines that may indicate an upcoming failure or fault (arcing, partial discharge, imbalance, overheating)

4.2 Steps – Scenarios

Scenario								
Scenario name:		Forest and vegetation reconnaissance						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	UAV flight starts	UAV image/data capture	UAV equipped with appropriate sensors performs a flight over an overhead line using a pre-loaded mission details with the support of an operator in the field. UAV captures as much images and data as possible and returns to the GCS. At the GCS, UAV inspection operator retrieves media with data and images captured (memory, disk...)	inspection	UAV	UAV inspection operator	1	
2	UAV images/data obtained by UAV inspection operator	UAV image/data upload to image maintenance software	UAV inspection operator uploads media with data and images captured to IA image-based maintenance EMMA module	Data upload	UAV inspection operator	EMMA ARGOS	1	
3	UAV images/data uploaded to EMMA	UAV image/data IA processing	IA image-based maintenance EMMA module	Data processing	EMMA ARGOS	System Operator	2	



D2.3 - Requirements and Detailed Architecture Design

			triggers the appropriate process to analyze the set of images and data (in this case for Forest and vegetation reconnaissance). Data is processed and details of potential problems are obtained					
--	--	--	--	--	--	--	--	--

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Damages detection						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	UAV flight starts	UAV image/data capture	UAV equipped with appropriate sensors performs a flight over an overhead line using a pre-loaded mission details with the support of an operator in the field. UAV captures as much images and data as possible and returns to the GCS. At the GCS, UAV inspection operator retrieves media with data and images captured (memory, disk..)	inspection	UAV	UAV inspection operator	1	
2	UAV images/data obtained by UAV inspection operator	UAV image/data upload to image maintenance software	UAV inspection operator uploads media with data and images captured to IA image-based maintenance EMMA module	Data upload	UAV inspection operator	EMMA ARGOS	1	
3	UAV images/data uploaded to EMMA	UAV image/data IA processing	IA image-based maintenance EMMA module triggers the appropriate process to analyze the set of images and data (in this case for Damages detection). Data is processed and details of potential problems are obtained	Data processing	EMMA ARGOS	System Operator	3	

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Electric anomalies detection						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	UAV flight starts	UAV image/data capture	UAV equipped with appropriate sensors performs a flight over an overhead line using a pre-loaded mission details with the support of an operator in the field. UAV captures as much images and data as possible and returns to the GCS. At the GCS, UAV inspection operator retrieves media with data and images captured (memory, disk..)	inspection	UAV	UAV inspection operator	1	
2	UAV images/data obtained by UAV inspection operator	UAV image/data upload to image maintenance software	UAV inspection operator uploads media with data and images captured to IA image-based maintenance EMMA module	Data upload	UAV inspection operator	EMMA ARGOS	1	

D2.3 – Requirements and Detailed Architecture Design

3	UAV images/data uploaded to EMMA	UAV image/data IA processing	IA image-based maintenance EMMA module triggers the appropriate process to analyze the set of images and data (in this case for Electric anomalies detection). Data is processed and details of potential problems are obtained	Data processing	EMA ARGOS	System Operator	4	
---	----------------------------------	------------------------------	---	-----------------	-----------	-----------------	---	--

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Images and data (geo-located)		
2	Location and details of forest and vegetation potentially dangerous for the overhead lines		
3	Location and details of structural damages in the infrastructure of the overhead lines		
4	Location and details of electrical anomalies in the infrastructure of the overhead lines		

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.2 USE CASE 2 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
UC02	TSO/DSO, substation transformers, maintenance	Substation component status of health calculation based on SCADA measurements and DGA data

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	20/01/2023	Ugo Stecchi		
0.2	18/01/2023	Pablo Bort		
0.3	23/01/2023	Lucas Pons		
0.4	08/05/2023	Srđan Subotić	Review	Approved
0.5	30/05/2023	Ugo Stecchi		Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	The UC02 is aimed at estimating the status of health, degradation or under performance of substations components based on sensor data gathered (SCADA and/or other field measurements as DGA through the Gas Chromatography Transformer Oil Analyzer).
Objective(s)	<ol style="list-style-type: none"> 1. Integrate with substation automation SCADA systems 2. Predict the stress conditions in critical power transformers based on DGA measurements 3. Predict the probability of failure in different timespans for power transformers based on DGA measurements 4. Automatic detection of component (serious) degradation in real time based on the SCADA measurements 5. Alerting and informing operators when a replacement or a maintenance intervention is required through a proper UI 6. Increase the reliability and efficiency of the substation
Related business case(s)	BC1, BC5

1.4 Narrative of use case

Narrative of use case
<p>Short description</p> <p>This UC02 will test the effectiveness of EMMA tool to detect degradation or malfunctioning in different substation components and supporting preventive and corrective maintenance. The detection will consider the analysis of continuously available SCADA data as well as data obtained periodically from the field (as in the case of transformer temperature and DGA measurements acquired through the Gas Chromatography Transformer Oil Analyzer for maintenance).</p>
<p>Complete description</p> <p>This UC02 will test the effectiveness of EMMA tool to detect degradation or malfunctioning in different substation components and supporting preventive and corrective maintenance. The detection will consider the analysis of continuously available SCADA data as well as data obtained periodically through analysis of DGA measurements acquired through the Gas Chromatography Transformer Oil Analyzer for the maintenance of the transformers.</p> <p>The substations are monitored and controlled through SCADA systems continuously collecting plenty of signals and measures from field equipment substation assets. Additionally and given the size and power MV transformers, they are typically filled in with oil, producing gas when subjected to thermal and electric stress. The system will also include results of DGA (Gas Chromatography Transformer Oil Analyzer) analysis, that could be carried out by system operator upon request.</p> <p>R2D2 EMMA component will connect to the substation automation SCADA system for monitoring and continuously analyze real-time measurements of different types. Also the results of DGA analysis will be used. The data acquired for the analysis comprises:</p> <ul style="list-style-type: none"> • Electrical measurements: current, voltage, phasors, etc. • Instrumental data, such as temperature, errors or statuses. • Configuration data, such as working mode, set-points, etc. • The concentration of gases and the ratio of their mixture from DGA analysis, that can suggest the type of faults typically organized in the following three categories: <ul style="list-style-type: none"> ○ partial discharges (PD) that connect conductors only partially through insulation system (low temperature plasma discharges); ○ - low-energy discharge (D1) in oil and/or paper due to the flow of electricity through the disrupted insulation; ○ - high-energy discharge (D2) in oil and/or paper with high current level; this fault is usually accompanied by large disruptions, burns and device shutdown; ○ thermal faults due to overheating of the insulation. <p>The idea is to detect, making use of ML/DL techniques, signs of degradation or malfunctioning in substation components such as transformers, circuit breakers, and power lines.</p> <p>For each of the substation's components considered; a DL model will be built based on the historical measurements observed. The historical data set should be tagged with failures and situations identified in the past, and the DL models will try to establish complex relations among the</p>

D2.3 - Requirements and Detailed Architecture Design

different recorded signals and the failures observed. Later on, these models will be used to predict potential failures based on the real-time values.

EMMA will help the maintenance operators by providing the probability and the magnitude of failure in different time frames.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
SCADA measurements are available
DGA data is available
Assets vendor recommendations and instructions for maintenance. Nominal levels/thresholds, etc.
Prerequisites

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC 6, 22, 23
Level of depth
specialised
Prioritisation
5 (high)
Generic, regional or national relation
regional
Nature of the use case
technical
Further keywords for classification

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
System operator	Role	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity	For this UC the system operator will be a distribution system operator having full responsibility of the HV/MV substation. Nevertheless, the UC can be confirmed as it is in those cases where a TSO is operating the HV side -including the transformer- of a HV/MV substation.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
EMMA DYML	application	Signal-based maintenance module based on IA. It is an EMMA component	
SCADA	System	Substation SCADA	

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	SCADA-based substation asset maintenance	Data coming from SCADA is used to periodically and automatically identify status of health, degradation or under performance of substations components, including the type of problem and the severity	System operator	periodic	Some substation assets might be damaged, deteriorated or under-performing	System operator obtains details of potentially harmful substation assets conditions, including the type of problems and the severity
2	DGA-based transformer maintenance	Data eventually available from DGA analysis is used to identify status of health, degradation or under performance of transformers, including the type of problem and the severity.	System operator	DGA data available	Some transformers might have a hidden damage of be under-performing	System operator obtains details of potentially harmful transformer conditions, including the type of problems and the severity



D2.3 - Requirements and Detailed Architecture Design

4.2 Steps – Scenarios

Scenario								
Scenario name:		SCADA-based substation asset maintenance						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Periodic	SCADA data gathering	EMMA component receives from SCADA the latest measurements acquired from substation assets	Substation monitoring	SCADA	EMMA DYML	1	
2	New SCADA data available	SCADA data analysis	EMMA analyses the new measurements, along with the historical data and try to identify potential problems in the assets. Eventually problems are detected based on ML/DL models and details are given for them	Data analysis	EMMA DYML	System operator	2	

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		DGA-based transformer maintenance						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	DGA data available	DGA data importing	System operator uploads DGA data to EMMA	DGA data importing	System operator	EMMA DYML	3	
2	New DGA data available	DGA data analysis	EMMA analyses the new measurements, along with the historical data and try to identify potential problems in the assets. Eventually problems are detected based on ML/DL models and details are given for them	Data analysis	EMMA DYML	System operator	4	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Substation assets measurements		
2	Substation assets' problems detected with details		
3	DGA data	Dissolved gas analysis measurements acquired through the Gas Chromatography Transformer Oil Analysis	
4	Transformers' problems detected with details		



6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.3 USE CASE 3 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
UC3	(Renewable) Bulk generation, field maintenance	Malfunctioning detection of PV panels through autonomous UAV image acquisition

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	18/01/2023	Sergi Grau	First draft	
0.2	23/01/2023	Lucas Pons	UC completion	
0.3	08/05/2023	Srđan Subotić	Review	Approved
0.4	30/05/2023	Ugo Stecchi	Improvements after review	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	This UC will focus on the image-based maintenance of PV fields, using autonomous UAV vehicles. The images captured during the autonomous flights will be analysed for identifying different type of anomalies and eventually trigger maintenance alarms.
Objective(s)	<ul style="list-style-type: none"> - Autonomous inspection of PV fields - Identify PV problems based on the images captured - Improvement of the maintenance activities (faster and more effective procedure)
Related business case(s)	BC5

1.4 Narrative of use case

Narrative of use case
Short description
UC4 is aiming at detect anomalies in PV panels using Deep learning techniques analysis on imagery data captured by autonomous UAV vehicles.
Complete description
<p>UC4 is aiming at detect anomalies in PV panels using Deep learning techniques analysis on imagery data captured by autonomous UAV vehicles. The current state of technology and the regulations of aviation law has led to the development of methods involving the use of a flying system with the following configuration:</p> <ul style="list-style-type: none"> • drone (multirotor) with at least an RGB camera and an IR camera, equipped with autopilot hardware that allows for autonomous operation, • ground control station (GCS) – a computer running mission planning and mission control software, • radio link with an antenna on a short mast located next to the GCS (for the transmission of telemetry data from the drone to the ground segment). <p>An operator can plan the flight route using GCS software and upload it via radio link to the drone. Once launched, the drone will automatically navigate along this PV field using GPS positioning and inertial measurement unit.</p> <p>During the flight, cameras collect a set of thermal photos and after the mission is completed, they are streamed to GCS.</p> <p>GCS eventually uploads the set of images (potentially, several GB of imagery data) to the analytical pipeline, where it will be analyzed by Deep learning techniques, specifically using a segmentation technique to extract each independent module in the PV plant from each photo. Next, each of this independent PV modules will be analyzed by a convolutional neural network which will be able to detect if the current PV module contains an anomaly or not.</p> <p>Finally, if the PV module contains an anomaly, it will be analyzed in more detail by another convolutional neural network to classify this anomaly in one of these following types:</p> <ul style="list-style-type: none"> - Cell anomaly - Cracking anomaly - Diode anomaly - Hot-spot anomaly - Offline-module anomaly - Shadowing anomaly - Soiling anomaly. - Vegetation anomaly. <p>After processed, results of the analysis will be sent to relevant databases and shown in a dedicated graphical user interface.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
UAV can flight over PV fields to capture images. The appropriate legal permissions have been obtained and a person with appropriate skills can is available to fight the UAV
Prerequisites

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC1
Level of depth
Specialised
Prioritisation
3 (medium)
Generic, regional or national relation
generic
Nature of the use case
technical
Further keywords for classification
RES operation and maintenance

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Producer	Role	A party that generates electricity.	This UC applies to PV producers only. Even if it is applicable in theory applicable to all PV categories, it is more feasible for large PV sites with fixed supports (no tracking systems)

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
UAV	Device	An autonomous self-moving device that is guided autonomously, by remote control, or both and that carries sensors, cameras for surveying, monitoring and inspection purposes	

D2.3 - Requirements and Detailed Architecture Design

UAV inspection operator	Human	Person in charge to supervise the mission of the inspection robot, mainly in charge of starting, cancelling, finishing and supervising the mission	
EMMA ARGOS	Application	SW platform developed under R2D2 (WP6, T6.1) with capabilities to acquire and analyse multi spectral images to monitor PV panels and identify possible failures.	

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	PV cells anomaly detection	UAV drone images are used to detect anomalies in PV cells	Producer (RES operator)	UAV Flight is planned for PV inspection	RES operator might have PV field cells with anomalies (damages, under-performance, etc)	RES operator has detailed information of PV plant cells affected with anomalies (damages, under-performance, etc)

4.2 Steps – Scenarios

Scenario								
Scenario name:		PV cells anomaly detection						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	UAV flight starts	UAV image/data capture	UAV equipped with appropriate sensors performs a flight over a PV field using a pre-loaded mission details with the support of an operator in the field. UAV captures as much images and data as possible and returns to the GCS. At the GCS, UAV inspection operator retrieves media with data and images captured (memory, disk..)	inspection	UAV	UAV inspection operator	1	
2	UAV images/data obtained by UAV inspection operator	UAV image/data upload to image maintenance	UAV inspection operator uploads media with data and images captured to IA image-based	Data upload	UAV inspection operator	EMMA ARGOS	1	

D2.3 - Requirements and Detailed Architecture Design

		ce software	maintenance EMMA module					
3	UAV images/data uploaded to EMMA	UAV image/data IA processing	IA image-based maintenance EMMA module triggers the appropriate process to analyze the set of images and data for identifying cells anomalies. Data is processed and details of potential problems are obtained	Data processing	EMMA ARGOS			

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Images and data (geo-located)		
2	Location and details of PV plant cells affected with anomalies (damages, under-performance, etc)		



6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.4 USE CASE 4 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
4	Distribution System / Metering System	Detection of NTL through SCADA and AMI data, from a selected portion of the distribution grid

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	24/01/2023	Ugo Stecchi		
0.2	08/05/2023	Srđan Subotić	Review	Approved
0.3	30/05/2023	Ugo Stecchi	Improvements after review	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	LV lines under the same MV/LV secondary station
Objective(s)	<ol style="list-style-type: none"> 1. Obtain pattern of load profiles from SCADA and AMI 2. Developing a DL algorithm for detecting consumption anomalies in LV nodes or lines 3. Mapping potential thefts over the distribution system (identification of node/line and meter) and inform the operators
Related business case(s)	BC1, BC5

1.4 Narrative of use case

Narrative of use case
Short description
Complete description
<p>This use case is aimed at detecting Non Technical Losses (NTL) in distribution grids. UCs are covering intrusion detections from a cyber perspective and from an equipment perspective (through firmware integrity), so this UC covers potential physical tampering on the metering and electric energy thefts.</p> <p>The main idea is to apply to NTL tool developed in EMMA to the portion of the distribution grids participating as pilot sites.</p> <p>The NTL tool within EMMA will be based on a hybrid approach including data analytics on smart metering data and power system simulations (load flow or state estimation) on the considered portion of the grid.</p> <p>As a result the tool will be able to identify areas of the network with higher mismatch between simulation results and smart meters data (heatmap of affected nodes) or even the alerted smart meters in the most critical cases.</p> <p>(more information are needed from pilot to better address this UC).</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Grid Topology is known
Prerequisites
Historical data is available to build the models

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
n/a
Level of depth
Specialised
Prioritisation
3
Generic, regional or national relation
Local, regional
Nature of the use case
Technical, economic (reducing economic losses for energy thefts)
Further keywords for classification

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
System Operator	Role	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity	This UC can be applied to DSO only as it is based on smart meters data from LV final users
Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
EMMA ETER	Application	A SW platform developed by ETRA with advanced distribution management system functionalities	State estimation and load flow calculation will be needed by ETER

D2.3 - Requirements and Detailed Architecture Design

AMI	System	Advanced metering infrastructure	
SCADA	System	Distribution system SCADA	Measures acquired by SCADA from MV feeder and lines are needed.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Normal scenario		DSO	periodic	Smart meter data is available	List of potential fraudulent smart meters
2	Normal scenario with substation data		DSO	periodic	Smart meter data is available, feeder data at substation level is available	List of potential fraudulent smart meters or alternatively identification of the line(s) or bus where NTL has higher probability to occur



D2.3 - Requirements and Detailed Architecture Design

4.2 Steps – Scenarios

Scenario								
Scenario name:		Normal scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	periodic	Data gathering	Smart meter data is imported	Data gathering	AMI	EMMA ETER	1	
2	periodic	Data analysis	Smart meter data is analysis towards identifying unusual /suspicious patterns	Data analysis	EMMA ETER	DSO	3	

Scenario								
Scenario name:		Normal scenario with substation data						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	periodic	Data gathering	Smart meter data is imported	Data gathering	AMI	EMMA ETER	1	
2	periodic	Data gathering	feeder historical data is obtained	Data gathering	SCADA	EMMA ETER	2	
3	periodic	Data analysis	Smart meter and feeder data are analyzed towards identifying unusual /suspicious patterns	Data analysis	EMMA ETER	DSO	3	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Smart meter consumptions		
2	Feeder data		
3	List of suspicious smart meters		

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.5 USE CASE 5 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
UC5	TSO/DSO/generation, all zones, maintenance	Automated ranking intervention of assets and optimal scheduling (including routing) of intervention workforce to perform maintenance task.

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	24/01/2023	Lucas Pons		
0.3	05/04/2023	Lucas Pons		
0.4	08/05/2023	Srđan Subotić	Review	Approved
0.5	30/05/2023	Ugo Stecchi, Lucas Pons	Improvements after review	Approved
0.1	24/01/2023	Lucas Pons		Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	<p>This use case is aiming at generating a ranking intervention of assets considering the failure criticality, probability and consequences. The use case does not describe how to identify the interventions required, but it makes use of the interventions identified by other analytical use case (UC1, UC2, UC4 & UC12).</p> <p>Based on this ranking, individual maintenance tasks for the identified asset interventions are generated and scheduled for being carried out by the workforce, prioritizing the most critical ones according to the score and reducing the time wasted travelling.</p>
Objective(s)	<ul style="list-style-type: none"> - Gather intervention generated by other the relevant UCs. Each intervention may also include probability of the failures and other relevant data. - Automatically identify the cascading effects in case of failure or attack on a given asset and quantification of the damages. - Automatic calculation of the costs associated to the maintenance tasks: cost of workforce intervention (preventive), cost of repair, cost of replacement - Automatic calculation of 'damage' index associated to the failure: People affected, restoration time, reputation, amount of data lost, etc. - Generation of an optimal intervention list prioritizing the most important assets for maintenance and protection according to the aforementioned analysis - Schedule every maintenance task and assign them to individual workers so that they travel in the most optimal way. - Keep track of the status of the maintenance tasks by using the inputs of the workers in a mobile application - Consider skills and capabilities of the workers in the task assignation - Consider stock availability in the task assignation - Presentation of the results in a GUI
Related business case(s)	BC1, BC2, BC3, BC5

1.4 Narrative of use case

Narrative of use case
Short description
<p>This UC is aiming at generating a ranking intervention of assets considering the failure criticality, probability and consequences. Based on this ranking, individual maintenance tasks for the identified asset interventions are created and scheduled for being carried out by the workforce, prioritizing the most critical ones according to the different criteria and reducing the time wasted travelling.</p>
Complete description
<p>This is aiming at generating a ranking intervention of assets considering the failure criticality, probability and consequences. The ranking will be updated periodically based on the new intervention details generated by other UC.</p> <p>For the use ranking, multi-Criteria Decision Making (MCDA) mechanism will be used, where the intervention list will be sorted according to a score, calculated using the following criteria:</p> <ul style="list-style-type: none"> - Cost of the intervention - Cost in case of failure (considering cascading effects) - Failure probability - Restoration time - Health, environmental and safety criticality level (including worker and end-user) - Amount of people affected in case of failure <p>Each criterion will be given a weight and the score for each intervention will be calculated accordingly.</p> <p>Based on this ranked list individual maintenance tasks for the identified asset interventions will be generated and scheduled for being carried out by the workforce, prioritizing the most critical ones according to the score and reducing the time wasted travelling.</p> <p>The main input data will be the ranking intervention of assets calculated in the other UC. These interventions will be decomposed in individual maintenance tasks that will be assigned to workers and scheduled so that they are carried out in the most optimal way.</p> <p>The optimal assignation and scheduling of maintenance tasks to workers involves determining the most efficient way to assign tasks to workers based on their skills, availability, and location.</p> <p>The objective of the task assignment problem is usually to minimize the overall completion time or cost of the tasks. Additionally, it is also important to consider factors such as safety, quality, and skill requirements when assigning tasks to workers.</p> <p>An important aspect of optimal routing is the use of Geographic Information System (GIS) technology, which can be used to map the locations of tasks, workforce, and equipment, and can also be used to analyse factors such as traffic patterns, terrain, and weather conditions. This can help to identify the most efficient routes and to plan for contingencies.</p>



D2.3 - Requirements and Detailed Architecture Design

Another important aspect is to integrate the routing problem with other aspects of maintenance management, such as workforce scheduling, inventory management, and maintenance planning. This can help to ensure that the workforce is properly equipped and that the necessary materials and equipment are available when and where they are needed.

In summary, this is a complex problem that requires a combination of mathematical optimization methods, heuristic methods, and GIS technology. It also requires a holistic approach by integrating it with other aspects of maintenance management to ensure that the workforce is properly equipped and that the necessary materials and equipment are available when and where they are needed.

The results will be shown in a GUI featuring a GIS map visualization. Additionally, the maintenance tasks details will be presented to the workers in their mobile applications.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
The list of interventions is available (coming from other UC).
The workforce details are known
Prerequisites

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC22, UC23
Level of depth
detailed
Prioritisation
4 (High)
Generic, regional or national relation
Local, regional
Nature of the use case
Technical (operational, management)
Further keywords for classification

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
System operator	Role	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity	only Distribution System Operators apply for this UC
Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
EMMA GIMAN	Application	A SW platform for the management and coordination of crew interventions developed by ETRA and which optimizes the available workforce to be allocated in critical parts of the network, in case of an occurring event.	EMMA GIMAN will be improved in R2D2 with a module, performing an identification of the most critical assets and calculates the optimal prioritization of actions

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Workforce activities scheduling towards optimal grid maintenance	The workforce is assigned with activities scheduled to be carried out in the most optimal way	System operator	Periodic (daily)	System operator has a list of maintenance actions to be carried out	Maintenance actions are assigned to operators and scheduled in the most optimal way

4.2 Steps – Scenarios

Scenario								
Scenario name:		Workforce activities scheduling towards optimal grid maintenance						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Maintenance action created by ETRA ARGOS	Maintenance actions details storage	ETRA ARGOS store maintenance action details in shared database	Maintenance action storage	EMMA ARGOS	EMMA GIMAN (DB)	3	
2	Maintenance action created manually	Maintenance actions details definition and storage	System operator uses the EMMA GIMAN product to add new periodic or individual maintenance action with all the details	Maintenance action definition	System operator	EMMA GIMAN (DB)	3	
3	Periodic	Maintenance actions analysis	The list of actions to be performed by the workforce (scheduled, automatically identified, etc.) are analyzed	Maintenance actions analysis	EMMA GIMAN (DB)	EMMA GIMAN (DB)	1	



D2.3 – Requirements and Detailed Architecture Design

4	Periodic (daily)	Maintenance actions are scheduled and assigned to operator	Maintenance actions are scheduled and assigned to operator. The maintenance actions are prioritised according to different criteria, and they are scheduled and assigned to operators based on the operator skills, grid operation details, travel time, etc	Maintenance scheduling	EMMA GIMAN	EMMA GIMAN	2	
---	------------------	--	--	------------------------	------------	------------	---	--

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Set of maintenance actions		
2	Maintenance actions assignation to operators and scheduling		
3	Maintenance action details		

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.



7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.6 USE CASE 6 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
6	Transmission and Distribution Systems / Substations	Substation components degradation detection by analysing images (Conventional & thermal)

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	23/01/2023	Ugo Stecchi		
0.2	21/03/2023	Lucas Pons		
0.3	15/05/2023	Theofanis Kontopoulos	Review	
0.4	30/05/2023	Ugo Stecchi	Improvements after review	

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	This UC12 is aimed at detecting anomalies or defects in transmission and distribution substation's equipment. It does not include all the infrastructure composing the substation, but only circuit breaker, SPD, power transformers, disconnector, and insulators
Objective(s)	Develop a tool combining multi-spectral images acquired through different cameras Identification of electric anomalies in substation equipment as: arcing, partial discharge, hot spot and overheating Improvement of the maintenance and security activities (faster and more effective procedure)
Related business case(s)	BC1, BC5

1.4 Narrative of use case

Narrative of use case
Short description This UC is based on the acquisition and processing of optical and thermal images at substations to detect potential anomalies, failures and security menaces. Through thermal and optical cameras properly positioned or captured by inspection robots, the automatic detection of electric defects in selected components will be verified as well as events that may affect the security of the installation.
Complete description This UC is based on the validation of optical and thermal images acquired at substations and processed by DL algorithm to detect anomalies or potentials menaces through the combined adoption of optical and thermal cameras. Both normal and thermal images will be acquired by the correspondent EMMA tool and processed through a DL algorithm to detect: <ol style="list-style-type: none"> 1. Defects on electric equipment: circuit breakers, insulators, SPD, disconnectors, power transformers. 2. Potential security breach or menace in the infrastructure: breaking and entering, possible stealing, suspicious behaviours, vandalism or terrorism attacks, etc. In both cases, the tool will be able to trigger an alarm when an event is considered beyond a certain threshold to be set. The UI will display the alarm and the event will be registered in the log event list.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Images (optical and thermal) are available
Substation assets are georeferenced
Prerequisites
Images (optical and thermal) are available



1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
26
Level of depth
Specialised
Prioritisation
5
Generic, regional or national relation
Generic, regional
Nature of the use case
Technical
Further keywords for classification
Predictive maintenance, fault detection

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	Distribution System Operator	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity	The DSO is responsible for the physical security of its infrastructure. When receiving a signal or an alert from the installed equipment in case either of a vandalism/theft attack or of any event affecting critical infrastructure, the available workforce personnel of the DSO must be sent to the incident site for power restoration.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
Inspection Robot	Device	An autonomous self-moving device that is guided autonomously, by remote control, or both and that carries sensors, cameras for surveying, monitoring and inspection purposes	Inspection Robot
inspection operator	Human	Person in charge to supervise the mission of the inspection robot, mainly in charge of starting, cancelling, finishing and supervising the mission	inspection operator
EMMA ARGOS	Application	SW platform developed under R2D2 with capabilities to acquire and analyse multi spectral images to monitor PV panels and identify possible failures.	EMMA ARGOS
Grouping		Group description	
HW/SW actors			
Actor name	Actor type	Actor description	Further information specific to this use case
Thermal camera	Electrical anomalies inspection equipment device	Thermal cameras are devices, providing thermal images from the assets and parts of infrastructure to be inspected	Thermal camera is planned to be installed in a fixed position inside the primary substation infrastructure. Thermal images, involving switches of the main feeders, are going to be forwarded continuously to EMMA tool for AI electric anomalies identification.



D2.3 - Requirements and Detailed Architecture Design

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Identification of electrical anomalies on images captured by fixed cameras	Identification of defects on electric equipment: circuit breakers, insulators, SPD, disconnectors and power transformers based on images captured by fixed cameras	DSO	disturbing-alarming images produced by thermal camera	Thermal camera is installed on HV/MV substation infrastructure	Electrical problems are identified
2	Identification of electrical anomalies on images captured by cameras equipped in inspection robots	Identification of defects on electric equipment: circuit breakers, insulators, SPD, disconnectors and power transformers based on images captured by cameras equipped in inspection robots	DSO	disturbing-alarming images produced by camera, equipped in inspection robot	Mission and area inside infrastructure defined for inspection by the robot	Electrical problems are identified



D2.3 - Requirements and Detailed Architecture Design

4.2 Steps – Scenarios

Scenario								
Scenario name:		Identification of electrical anomalies on images captured by fixed cameras						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Periodic	Image capture	Images are periodically captured and imported in EMMA ARGOS	inspection	Camera	EMMA ARGOS	1	
2	Periodic	Image IA processing	IA image-based maintenance EMMA module triggers the appropriate process to analyze the set of images and data for identifying electrical anomalies. Data is processed and details of potential problems are obtained	Data processing	EMMA ARGOS	DSO	2	

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Identification of electrical anomalies on images captured by cameras equipped in inspection robots						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Inspection robot mission starts	Inspection robot image/data capture	Inspection robot equipped with appropriate sensors performs a mission on a substation using a pre-loaded mission detail. Inspection robot captures as many images and data as possible and returns to the station. At the station, the inspection operator retrieves media with data and images captured (memory, disk.)	inspection	Inspection robot	Inspection operator	1	
2	images/data obtained by inspection operator	image/data upload to image maintenance software	inspection operator uploads media with data and images captured to IA image-based maintenance EMMA module	Data upload	Inspection operator	EMMA ARGOS	1	
3	images/data uploaded to EMMA	Image IA processing	IA image-based maintenance EMMA module triggers the appropriate process to analyze the set of images and data for identifying electrical anomalies. Data is processed and details of potential problems are obtained	Data processing	EMMA ARGOS	DSO	2	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Images and data (geo-located)		
2	Location and details of substation's assets affected with anomalies (damages, under-performance, etc)		
3	Security breach details		

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
UAV	Unmanned Aerial Vehicle

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.7 USE CASE 7 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
UC7	Distribution , DER / Enterprise, Station, Field, Process	Enhancement in DER control and management systems to participate in ancillary services procurement schemes for DSO and TSO to improve network operation security

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	07.04.2023	ELOVE, ELEK	-	Preliminary approved
2	08.05.2023	ELOVE, ELEK	Use case revision by auditor	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	DER Scenario
Objective(s)	O1. Optimal management of the flexibility capacity from DERs O2. Standard communication accesses to control DERs without additional hardware O3. secure communications to DERS for their automatic operation.
Related business case(s)	BC5

1.4 Narrative of use case

Narrative of use case
Short description
It is becoming necessary for DER to take over certain level of ancillary services including emergency actions. However, DER are limited in their ability when compare them with conventional energy sources. This UC will demonstrate, how DER and flexibility can fulfil these tasks.
Complete description
<p>Since with increasing share of DER fluctuations in the network increase and issues with power quality becoming more often, DER need to participate also in system services with fair share. Therefore, it is becoming necessary for DER to take over certain level of ancillary services (including emergency actions) However, DER are limited in their ability when compare them with conventional energy sources. This UC will demonstrate, how DER and flexibility can fulfil these tasks. Therefore, we need to set up the system to enable us to procure system services form DER and optimally control them. RES will be included in flexibility/system services procurement system and later provide services. Algorithm for activation of these resources will be developed, which takes in consideration volatile generation and limitations in their abilities of proper response.</p> <p>Adaptive control of the voltage profile from the transformer distribution station to the end of the power line with weighted DER participation, primarily of the PVs will be addressed. Further, local centralized control for stable participation of DER using standard communication accesses to control devices without additional investments in hardware will be set up in this UC demonstration.</p> <p>Practically, RES (particularly Wind and Sun) as a most problematic option of DER can be included in provision of services for any TSO (certainly with limitations of the demo and size of this project we are talking about kW and not MW). But schemes and mechanisms can be tested and demonstrated.</p> <p>Establishment of secure communication protocols using the latest protective communication measures such as data encryption, access filtering from allowed IPs, multi-level login procedures are also part of the project. All implementations are performed for automatic operation in real time.</p> <p>The data acquisition system must have automatic data checks that can detect attempts of unauthorized data read, receiving data outside the expected limits, and communication requests from unapproved addresses.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
<p>Triggering is done by so called flexibility server, which collects data from billing system (mostly LV network and partially MV) on one side, SCADA and DSO and DER on the other and User data of ancillary services, like DSO, TSO, Aggregator, Responsible in balance group sends the activation signal. Actions are triggered in case of events divided into 2 groups:</p> <ul style="list-style-type: none"> • Events related to support the power system operation with changing the power. • Events related to communication security
Prerequisites
<ul style="list-style-type: none"> • Real-time connection to information system of ancillary service market in distribution system • Real-time information from central SCADA system • Real-time connection with distributed RES participating in the service • Known Structural DER data (P installed, P min, Q diagram, voltage limits, etc.) • Secured communication connection between all systems

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
Level of depth
High level of detail.
Prioritisation
Highest priority (5). This service so far doesn't exist in the Slovenian power system or this is done manually for bigger units only.
Generic, regional or national relation
Generic and national, has potential to regional.
Nature of the use case
DEE functional requirements description.
Further keywords for classification
DER, Flexibility, Ancillary services, Traffic Light System, Emergency operation.

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Distribution System Operator (DSO)	System operator	‘Distribution system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	DSO control centre sends signal about the locations, where flexibility can’t be used due to potential congestions.
DER /RES	Producer	‘Producer’ means a natural or legal person who generates electricity as defined in point (25) of Article 2 of Regulation (EU) 2019/944 (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common	Producer receives signal sent by DSO and change generation accordingly.

D2.3 – Requirements and Detailed Architecture Design

		rules for the internal market for electricity and amending Directive 2012/27/EU)	
Grouping		Group description	
Hardware/Software components		Hardware/Software components used in UC7 business process	
Actor name	Actor type	Actor description	Further information specific to this use case
SCADA / ADMS system (DSO)	Control system	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, databases, networked data communications and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plant or machinery. Advanced Distribution Management System (ADMS) comprises control functions to automatically control the network and support operators.	SCADA / ADMS system is used to provide real-time active & reactive power measurements and network topology data.
Meters	Device	Meters are devices to measure energy consumption for billing purposes.	From meters we collect loading and voltages for estimation of the situation in the distribution MV and LV networks.
RTUs	Device	RTUs are used in the network nodes to collect data about topology and operation	RTUs are devices, where from SCADA gets information about topology.
Flexibility procurement system (Flex server)	Control system	Flex server is software on virtual server, that calculates congestions and activates or block flexibility sources in distribution network.	Flex server is used to calculate operation limits and activates flexibility from RES in case, needed for network support.

D2.3 - Requirements and Detailed Architecture Design

SCADA system (RES)	Control system	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, databases, networked data communications and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plant or machinery.	SCADA system is used to provide real-time active & reactive power measurements and availability and restrictions of PV plants and SHPPs.
--------------------	----------------	---	--

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Providing ancillary services by DER	At DSO side system will provide and send information about possible needs for ancillary services. DER will respond accordingly with changing generation of active / reactive power to support grid operation inside allowed limits.	DER	Regular repetition every 1-5 minutes.	The information below is available for further processing: <ul style="list-style-type: none">• Real-time information from the meters used for billing purposes. (P,Q, V)• Real-time information from SCADA system (P,Q,V, topology)• Results of state estimation	DER Ancillary services by changing generation settings according to the network conditions and their actual limitations

D2.3 - Requirements and Detailed Architecture Design

2	Assuring of secure communication channel between devices and system from Scenario 1 and procedures in case of attack	Establishment of secure communication protocols using the latest protective communication measures such as data encryption, access filtering from allowed IPs, multi-level login procedures between systems from Scenario 1 Actions are triggered in case of events related to communication security	DSOs, DERs	Periodic and random	System from Scenario 1 must operate. Implementation of secure communication protocols.	Procedures in case of detected security attack
---	--	--	------------	---------------------	---	--

4.2 Steps – Scenarios

Scenario								
Scenario name:		Providing ancillary services by DER						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Data acquisition Runs periodically	Collecting data	Data acquisition from DER control systems	Data collection	DER /SCADA, RTU, meter	DSO/ Flexibility system	1,2,3,4,5	
2	Data collected	Data pre-processing	DER operation optimization for ancillary services, taking into account voltage profile and loadings	Calculation	DSO/ Flexibility system	DSO/ Flexibility system	-	
3	Data preprocessed.	Limits checking	Detection of data (voltages and power) outside the expected limits	Calculation	DSO/ Flexibility system	DSO/ Flexibility system	-	

D2.3 - Requirements and Detailed Architecture Design

4	Limits checked	Alarming	Control acts for DER	Commands sending	DSO/ Flexibility system	DER, TSO, Aggregator, Balancing responsible /SCADA	5,6,7	
5	Data acquisition	Collecting data	Data acquisition from DER control systems	Data collection	DER /SCADA, RTU, meter	DSO / Flexibility system		
6	Data collected	Control action effect checking	Changes checked with received real values	Calculation	DSO / Flexibility system	DSO / Flexibility system	-	

Scenario								
Scenario name:		Assuring of secure communication channel between devices and system from Scenario 1 and procedures in case of attack						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Communication security check in each in steps 1 and 5 of previous scenario	Collecting data	Data acquisition	Data exchange	DER /SCADA, RTU, meter	TSO, Aggregator, Balancing responsible DSO / SCADA Flexibility system	1,2,3,4,5,6	
2	Communication security check in each in step 4 of previous scenario	Commands transfer	Commands sending	Data exchange	TSO, Aggregator, Balancing responsible DSO / SCADA Flexibility system	DER /SCADA, RTU, meter	7	
3	Data collected	Attack detection	Detect attempts of unauthorized data read, receiving data outside the expected limits, communication requests from unapproved addresses.	Real-time data check Real-time communication security check and data processing	DSO / Flexibility system	DSO / Flexibility system	-	

D2.3 – Requirements and Detailed Architecture Design

4	Attack detected	Alarming/ optional blocking control actions	Data processing and activation security procedures in case of attack	Real-time data processing	DSO / Flexibility system	DSO (IT security department)	8	
---	-----------------	---	---	------------------------------	-----------------------------	---------------------------------	---	--

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Active power measurements	P	
2	Reactive power measurements	Q	
3	Voltage measurements	U	
4	Generation availability	Boolean	
5	Generation Schedule	P,Q vs Time	
6	Limits violation	Boolean	
7	Activation request	Boolean	
8	Cyber security related data	Security protocols	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.8 USE CASE 8 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
8	Transmission / Enterprise, Operation	Outage planning optimization

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	04.03.2023	EMSS		Preliminary approved
2	24.04.2023	EMSS	Requirements definition	Preliminary approved
3	03.05.2023	SCC	Changes are given as comments and track changes	UC revision – approved by SCC
4	9.06.2023	EMSS	UC improvement after revision	Approved
5	6.12.2023	EMSS, IMP	Additional requirements definition	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Outage planning optimization
Objective(s)	Optimize the requested outages with the aim of minimizing the time of unavailability of the network elements and thus increasing system operation reliability.
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
<p>This use case defines an Outage Planning Optimization (OPO) on the basis of which the TSO can decide whether all requested outages in a given period can be approved, i.e. which requested outages cannot be accepted for a given time period (and must be rescheduled) from the point of view of transmission grid operation security.</p> <p>The outage planning business process is organized in three time frames: yearly, quarterly and weekly. In each time frame (interval), the TSO must coordinate and optimize outage requests and outage planning.</p>
Complete description
<p>In order to ensure the operational security of the transmission grid and the reliable supply of electricity to consumers, the Transmission System Operator (TSO) is obliged to review and approve the outage plans proposals of the transmission system elements, generation units (conventional and renewable), the distribution system elements and significant grid users facilities.</p> <p>In addition, the TSO must coordinate outages with neighboring TSOs and Regional Coordination Centres (RCCs). The name of this pan-European process is Outage Planning Coordination (OPC).</p> <p>The goal of this use case is to optimize outage planning at the national level (this means that coordinated outages at the regional level are input data with the highest priority). Outage Planning on national level is organized in three time frames: yearly, quarterly and weekly. In each time frame (interval), the TSO must coordinate and optimize outage requests of all above mentioned stakeholders with the aim of minimizing the time of unavailability of the network elements and thus increasing system operation reliability.</p> <p>Within the Horizon 2020 project called TRINITY, the development of the national outage planning tool was started by creating a communication platform for the exchange of outage planning information. However, the outage planning is still mostly done manually, because the given communication platform is not connected with a module that would optimize the proposed disconnections.</p> <p>Therefore, the main goal of this use case is to define an Outage Planning Optimization (OPO) algorithm and tool on the basis of which the TSO can decide whether all requested outages in a given period can be approved, i.e. which requested outages cannot be accepted for a given time period (and must be rescheduled) from the point of view of transmission grid operation security. In this way, this tool will increase the efficiency of the outage planning process at the TSO/national level and facilitate the coordination and decision-making process among the involved stakeholders using an appropriate platform for communication and coordination.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Regional coordination of outage planning is done in a separate business process – such coordinated outages are used as high-priority input data in the OPO process at the national level. Rescheduling of outages for the day ahead and intra- day is carried out in a separate business process. Re-dispatching costs due to outage coordination are also beyond OPO process as they are implemented in day ahead and intra-day system operation security control.
Prerequisites
All involved participants must prepare outage proposals for each network element they maintain. Relevant grid models are available for each outage planning period. Grid models are harmonized with generating units' availability plans.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
High level of details.
Prioritisation
High priority (4). The use case is of greater importance. With this use-case, EMSS wants to improve the outage planning business process, which would significantly speed up and facilitate work on outage planning, and at the same time increase system operation security, i.e. reduce the probability of an error. In addition, this could also reduce re-dispatching costs due to poor outage planning.
Generic, regional or national relation
Generic, national.
Nature of the use case
System functional requirements description.
Further keywords for classification
Optimization, Outage planning.

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO)	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	Transmission System Operator (TSO) is obliged to coordinate the outage plans proposals of the transmission system elements, generation units (conventional and renewable), the distribution system elements and significant grid users.

D2.3 - Requirements and Detailed Architecture Design

OP participant	Market participant or system operator	TSO or Distribution System Operator or Producer or any other grid users participating in outage planning process	OP participants request outages due to maintenance work or other reasons.
OP operator	Software operator	A software operator is a person who controls the execution of a software.	OP operator carries out manual operations within OP optimization process.
Grouping		Group description	
Software/Hardware component		Software/Hardware components used in OPO process	
Actor name	Actor type	Actor description	Further information specific to this use case
EMMA OP tool	Software application	An application program is a computer program designed to carry out a specific task other than one relating to the operation of the computer itself, typically to be used by end-users.	OP tool is used to optimize network elements outage periods.
eTNA	Software application	Ditto.	eTNA is a software designed for operations of validating, fixing, and merging the load flow data sets, load flow and contingency calculations, NTC calculation, PTD/Maxflow calculations, as well as short circuit analyses. eTNA will be used to check whether planned outages violate security criteria.
EMMA Communication platform	Communication software	Communication software is used to provide remote access to systems and exchange files and messages in text, audio and/or video formats between different computers or users.	Communication platform is used to exchange data on network elements outage periods proposals and optimized periods, as well as to confirm/reject optimization solution and to hold conference call in order to harmonize outage periods.

D2.3 – Requirements and Detailed Architecture Design

OP server	Server	A computer program or device that provides a service to another computer program and its user, also known as the client.	OP server is used to store data on network elements outage periods proposals, optimized periods and data on grid models which are used as input data in OPO process.
-----------	--------	--	--

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Basic scenario	TSO receives outage proposals from participants and optimizes/coordinates outage periods – all participants accept proposed outage plan	TSO	Regular repetition	Outages are not coordinated and optimised	All participants accept coordinated and optimized periods of outages
2	Exceptional scenario	TSO receives outage proposals from participants and optimizes/coordinates outage periods – some participants reject proposed outage plan	TSO	Outage coordination/optimization is rejected by a participant	Coordinated and optimized periods of outages are not accepted by all participants	All participants accept coordinated and optimized periods of outages

4.2 Steps – Scenarios

Scenario								
Scenario name:		Basic scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	According to maintenance activity schedule	Requesting outages proposals	TSO request towards maintenance entities to express their need for outages for the next year	Data requesting	TSO / EMMA communication platform	OP participant / EMMA communication platform	1	EMM_036
2	Request for outage proposal sent	Uploading outage periods proposals	Outage planning participants submit to TSO their proposals for outage periods of network elements	Data uploading	OP participant / EMMA communication platform	TSO / EMMA communication platform	2	EMM_036
3	Outage periods proposals are uploaded	Importing input data for UAP file creation	OP tool imports submitted proposals for outage periods of network elements	Data importing	TSO / EMMA communication platform	TSO / EMMA OP tool	2	EMM_038
4	Data for UAP file creation is imported	UAP file creation	OP tool creates UAP file	Data processing	TSO / EMMA OP tool	TSO / EMMA OP tool	2, 3	EMM_038, EMM_109, EMM_120
5	UAP file is created	UAP file export	OP tool exports UAP file to OP server	Data exporting	TSO / EMMA OP tool	TSO / OP server	3	EMM_038, EMM_109, EMM_119
6	UAP file is exported	UAP file import	UAP file is imported in OP tool for manual processing by OP operator	Data importing	TSO / OP server	TSO / EMMA OP tool	3	EMM_038, EMM_109, EMM_110, EMM_111, EMM_116

D2.3 - Requirements and Detailed Architecture Design

7	UAP file is imported	Manual processing by OP operator	OP operator carries out manual operations - by changing the dates of proposed outages / changing priorities of proposed outages	Manual data processing	TSO / EMMA OP tool (OP operator)	TSO / EMMA OP tool (OP operator)	2, 7	EMM_038, EMM_110, EMM_111, EMM_112, EMM_121
8	A request for the OPI (Outage Planning Incompatibility) is sent from the OP tool	OP tool sends command to eTNA	OP tool sends commands to eTNA: - to import CGM, CON and MON lists for selected hour	Command sending	TSO / EMMA OP tool	TSO / eTNA	4, 5, 6, 8	EMM_038, EMM_113
9	eTNA imported CGM, CON and MON lists for selected hour	OPC CON file creation	Based on the data for the selected hour, OPC CON file is created, containing the list of outages according to the specified file format	Data processing	TSO / EMMA OP tool	TSO / EMMA OP tool	9	EMM_038, EMM_118
10	OPC CON file is created	OPC CON file export	OPR exports OPC CON file to the OP server	Data exporting	TSO / EMMA OP tool	TSO / OP server	9	EMM_038, EMM_118
11	OPC CON file is exported	OP tool sends command to eTNA	OP tool sends command to eTNA to import OPC CON file	Command sending	TSO / EMMA OP tool	TSO / eTNA	8	EMM_113
12	eTNA received command to import OPC CON file	eTNA imports OPC CON file	eTNA imports OPC CON file from OP server	Data importing	TSO / OP server	TSO / eTNA	9	EMM_038, EMM_113

D2.3 - Requirements and Detailed Architecture Design

13	OPC CON file is imported by eTNA	OP tool sends command to eTNA to perform Scale OPC function	OP tool sends command to eTNA to perform Scale OPC function in order to apply outages from OPC CON file to the CGM	Command sending	TSO / EMMA OP tool	TSO / eTNA	8	EMM_038, EMM_113
14	eTNA received command to perform Scale OPC function	eTNA executes Scale OPC function	eTNA executes Scale OPC function	Data processing	TSO / eTNA	TSO / eTNA	9	EMM_122
15	eTNA executed Scale OPC function	eTNA exports the results of Scale OPC function	eTNA exports the results of Scale OPC – Modified CGM to OP server	Date exporting	TSO / eTNA	TSO / OP server	4	EMM_114
16	eTNA exported the results of Scale OPC function	OP tool sends command to eTNA to perform N-1 security analysis (one or more if it is necessary)	OP tool sends command to eTNA to perform N-1 security analysis on modified CGM file using already imported CON and MON lists and to store results on OP server	Command sending	TSO / EMMA OP tool	TSO / eTNA	4, 5, 6, 8	EMM_038, EMM_113, EMM_122
17	eTNA received command to perform N-1 security analysis	eTNA executes N-1 security analysis	eTNA executes N-1 security analysis	Data processing	TSO/ eTNA	TSO/ eTNA	4, 5, 6	EMM_122
18	eTNA executed N-1 security analysis	eTNA exports N-1 security analysis results	eTNA exports N-1 security analysis results to OP server	Data exporting	TSO / eTNA	TSO / OP server	10	EMM_038, EMM_114

D2.3 - Requirements and Detailed Architecture Design

19	N-1 security analysis results are exported	OP tool imports N-1 results	OP tool imports N-1 results from OP server	Data importing	TSO / OP server	TSO / EMMA OP tool	10	EMM_038, EMM_114
20	OP tool imported N-1 results	OP tool calculates OP optimization indicators	Based on imports N-1 results OP tool calculates indicators.	Data processing	TSO / EMMA OP tool	TSO / EMMA OP tool	10, 11	EMM_038, EMM_115
21	OP optimization indicators are calculated	OP tool exports OP optimization results	OP tool exports OP optimization results to OP server	Data exporting	TSO / EMMA OP tool	TSO / OP server	11	EMM_038, EMM_114
22	OP optimization results are exported	OP tool imports the OP optimization results calculated from N-1 results	OP tool imports the OP optimization results calculated from N-1 results and shows them in the OP tool user interface	Data importing	TSO / EMMA OP tool	TSO / EMMA OP tool	11	EMM_038, EMM_114
23	OP optimization results are analysed and no further changes are needed	Final UAP creation	OP tool creates final UAP file	Data processing	TSO / EMMA OP tool	TSO / EMMA OP tool	3	EMM_109, EMM_110, EMM_111
24	Final UAP file is created	OP tool exports the final UAP	OP tool exports the final UAP file to OP server	Data exporting	TSO / EMMA OP tool	TSO / OP server	3	EMM_109
25	Final UAP is exported to OP server	Uploading optimized outage periods	TSO uploads optimized outage periods to be confirmed by all OP participants	Data uploading	TSO / OP server	OP participant / EMMA communication platform	2	EMM_036
26	Optimized outage periods are uploaded	Optimized outage periods confirmation	OP participants confirm optimised outage periods	Data transfer	OP participant / EMMA communication platform	TSO / EMMA communication platform	12	EMM_036

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Exceptional scenario (first 26 steps are the same as Basic scenario)						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
27	Optimized outage periods are uploaded	Optimized outage periods confirmation	OP participants reject optimised outage periods	Data transfer	OP participant / EMMA communication platform	TSO / EMMA communication platform	12	EMM_036
28	Optimized outage periods are not confirmed by all OP participants	Coordination teleconference	TSO organizes teleconference call with affected OP participants to coordinate outage periods of critical elements	Conference call	TSO, OP participant / EMMA communication platform	TSO, OP participant / EMMA communication platform	2	EMM_036

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Network element outage period	Network element outage period (proposed or optimized by OP tool or coordinated via conference call)	
2	Grid model	Representative grid model for the outage planning optimization period	
3	Outage period confirmation	Outage period confirmation or rejection with proper comment if needed	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Grid Model	Grid model means a Union-wide data set agreed between various TSOs describing the main characteristic of the power system (generation, loads and grid topology) and rules for changing these characteristics during the capacity calculation process.
Outage planning (OP)	Outage planning consider planning the availability status of a relevant power generating module, a relevant demand facility or a relevant grid element.

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.9 USE CASE 9 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
9	Transmission / Enterprise	Automation of calculation of emission levels of electricity quality parameters

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	27.03.2023	EMSS	-	Preliminary approved
2	25.04.2023	EMSS	Requirements definition	Approved
3	04.08.2023	EMSS	Further requirements definition	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Power quality parameters emission levels calculation in the compliance simulation process and during permanent operation (in the compliance monitoring/monitoring process).
Objective(s)	Automated calculation the emission values for voltage asymmetry, flicker and higher harmonics, based on the planned values and the topology of the transmission network and checking the compliance of transmission system users.
Related business case(s)	BC1, BC4

1.4 Narrative of use case

Narrative of use case
Short description
The automated power quality parameters emission levels calculation will be used in the connection process (for the purposes of compliance simulation checks), as well as in permanent operation (in the compliance testing/monitoring process). The calculation of emission levels according to the relevant IEC standards is very complex and requires the development of a software application.
Complete description
<p>Checking the parameters of the quality of electricity takes place through two compliance-checking processes: simulation (within the study of connecting the facility to the transmission system) and measurements in real-time operation (during the operational life).</p> <p>National regulations usually define maximum permissible planned values of the level of voltage asymmetry, higher harmonics, and flicker as well as maximum permissible emission values in connection points.</p> <p>The international standards IEC 61000-3-6, IEC 61000-3-7, and IEC 61000-3-13 propose an algorithm for calculating the emission levels of the specified parameters at each connection point to the transmission system, based on the adopted planned values of the electricity quality parameters and network topology.</p> <p>In order to check the compliance of the operation of the facilities that will be connected to the transmission system with the specified connection requirements, it is necessary to create an automated process that, based on the planned values, uses the algorithm recommended by international standards, calculates the emission levels of the electricity quality parameters.</p> <p>The automated calculation will be used in the connection process (for the purposes of compliance simulation checks), as well as in real-time operation (in the compliance testing/monitoring process).</p> <p>In the process of connecting facilities to the transmission system, the calculation results for the specific point of connection of the new facility are compared with the data obtained from the equipment manufacturer of the new production module or the customer's facility that is connected to the transmission system, and in this way, it is possible to indicatively detect violations of emission value limits and define the necessary corrective measures.</p> <p>In the process of monitoring compliance in real-time operation, the results of calculations are compared with real-time measurements, and in this way, possible non-compliance is detected.</p> <p>Additionally, within this Use Case, an automated calculation of the minimum three-phase short-circuit power/current in the subtransient mode in each point of the transmission system will be performed.</p> <p>The calculation will also determine the equivalent impedance of the rest of the system in the form of the R/X ratio for each point of the transmission system.</p> <p>The goal of this use case is to create a script that will automate the calculation of emission levels of power quality parameters on all transmission system busbars, as well as the calculation of the minimum short-circuit power/current on all transmission system busbars.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
The application will not be able to automatically send alarms, nor will it be connected with the measurement or monitoring system, but will give a result on the user's computer that shows whether the request is fulfilled or not. There will be no automatic reading of the data, instead the input file with the measurements will have to be loaded manually. Acquisition and monitoring system for power quality parameters exists, and it periodically sends reports to the Power Quality server. It can generate alarm in case of a non-compliance.
Prerequisites
Adopted planned levels for voltage asymmetry, flicker and higher harmonics, measurement database, IEC 61000, code editor (exp. python code editor, Visual studio etc.). Grid simulation models used in the connection process are stored in Grid Model server.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
High level of detail.
Prioritisation
High (4). There is no such system at the national level, nor at the regional level. Major importance is at the national level.
Generic, regional or national relation
Generic, national
Nature of the use case
System functional requirements description.
Further keywords for classification
Power quality, planning level, emission level, harmonics, flicker, asymmetry

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles.	
Actor name	Actor type	Actor description	Further information specific to this use case
TSO	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSO is responsible for the calculation of emission values of flickers, higher harmonics and asymmetries in the process of connecting objects to the transmission system (compliance simulation) and during the operation of the object (compliance monitoring).

D2.3 – Requirements and Detailed Architecture Design

Grouping		Group description	
Hardware/Software components		Hardware/Software components used in Power Quality compliance simulations and monitoring	
Actor name	Actor type	Actor description	Further information specific to this use case
Grid Model Server	Server	A server is a computer program or device that provides a service to another computer program and its user, also known as the client. In a data center, the physical computer that a server program runs on is also frequently referred to as a server. That machine might be a dedicated server or it might be used for other purposes.	The Grid Model Server is used to store the grid models used to calculate the emission values of flicker, higher harmonics and asymmetry.
Power Quality Server	Server	Ditto	Power Quality Server is used to store the results of calculations or measured values of emission values of flickers, higher harmonics and asymmetries.
EMMA Power Quality Emission Levels (PQEL) Application	Software Application	A software application is a computer program designed to carry out a specific task other than one relating to the operation of the computer itself, typically to be used by end-users.	The EMMA PQEL application is used to calculate emission values of flickers, higher harmonics and asymmetries or to compare measured and calculated emission values of flickers, higher harmonics and asymmetries

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1.	Compliance simulation scenario	In case of the new Power Generating Module or demand facility connection, TSO checks compliance with the connection power quality requirements.	TSO / EMMA PQEL	Compliance simulation is requested within the connection process	Input data from the facility owner are obtained. Simulation model in Load Flows software is prepared.	Emission level limits are calculated and compared with the connection requirements. Possible non-compliance is detected.
2.	Compliance monitoring scenario	Compliance monitoring is the continuous process when TSO observes the Grid Code requirements fulfilment.	TSO / EMMA PQEL	Repetitive activity or Alarming	Power quality measurement device is installed in the connection point.	Emission level limits calculated and compared with the simulation results. Possible non-compliance is detected.
3.	Equivalent grid parameters calculation scenario	Based on the selected node, all necessary data is calculated, such as R/X, Z _d , Z _i , Z _o , Sk'' etc...	TSO / EMMA PQEL	Third-party request	Simulation model prepared.	Automatically calculated R/X ratio, Sk'', Z _d , Z _i , Z _o for the selected busbars.

4.2 Steps – Scenarios

Scenario								
Scenario name:		Compliance simulation scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Compliance simulation is requested within the connection process	Data input	Input of selected grid model from the Grid Model Server into the PQEL application	Data download	TSO / Grid Model Server	TSO / EMMA PQEL Application	1	EMM_041, EMM_045
2	Data input is finished	Calculation for the selected node	Calculation of emission levels of flickers, higher harmonics, asymmetries for the selected node (connection point to the transmission grid)	Calculations	TSO / EMMA PQEL Application	TSO / EMMA PQEL Application	-	EMM_041, EMM_045, EMM_046, EMM_047, EMM_048, EMM_051
3	Calculation for the selected node is finished	Saving the results	Saving the calculated emission levels of flickers, higher harmonics, asymmetries for the selected node (connection point to the transmission grid) on the Power Quality Server	Data upload	TSO / EMMA PQEL Application	TSO / Power Quality Server	2	EMM_041, EMM_045, EMM_048

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Compliance monitoring scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Repetitive activity or Alarming	Input of measured data	Input of measurements of the emission levels of flickers, higher harmonics and asymmetries from the Power Quality Server into the PQEL application	Data download	TSO / Power Quality Server	TSO / EMMA PQEL Application	3	EMM_041, EMM_045
2	Input of the measured data is finished	Input of the calculated data	Input of calculated emission levels of flickers, higher harmonics and asymmetries from the Power Quality Server into the PQ application	Data download	TSO / Power Quality Server	TSO / EMMA PQEL Application	2	EMM_041, EMM_045
3	Input of the calculated data is finished	Calculation and compliance check	Calculation – comparison of the measured and calculated emission levels of flickers, higher harmonics and asymmetries	Calculations	TSO / EMMA PQEL Application	TSO / EMMA PQEL Application	-	EMM_041, EMM_045, EMM_046, EMM_049, EMM_052
4	Calculation is finished	Saving the results	Upload of the calculation results to the Power Quality Server	Data upload	TSO / EMMA PQEL Application	TSO / Power Quality Server	4	EMM_041, EMM_045, EMM_049

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Equivalent grid parameters calculation scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Third-party request	Data input	Input of selected grid model from the Grid Model Server into the PQEL application	Data download	TSO / Grid Model Server	TSO / EMMA PQEL Application	1	EMM_041, EMM_045
2	Data input is finished	Calculations for the selected node	Calculation of the parameters such as R/X, Zd, Zi, Zo, Sk'' etc... for the selected node (third-party facility connection point to the transmission system)	Calculations	TSO / EMMA PQEL Application	TSO / EMMA PQEL Application	-	EMM_041, EMM_045, EMM_046, EMM_047, EMM_050, EMM_053
3	Calculation is finished	Saving the calculation results	Saving the calculations results to the Power Quality Server	Data upload	TSO / EMMA PQEL Application	TSO / Power Quality Server	5	EMM_041, EMM_045, EMM_050

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Grid model	A model of the transmission network and facilities connected to the transmission network with the necessary parameters for the calculation of emission values of flickers, higher harmonics and asymmetries	
2	Calculated emission levels	Emission values of flickers, higher harmonics and asymmetries according to the relevant international standard	

D2.3 – Requirements and Detailed Architecture Design

3	Measured emission levels	Measured values of flickers, higher harmonics and asymmetries according to the relevant international standard	
4	Comparison of measured and calculated values	Difference between calculated and measured emission levels in the same connection point to the transmission system.	
5	Specific parameters related to power quality	Specific parameters such as R/X, Zd, Zi, Zo, Sk'' etc. that a third party requests in order to find technical solution to reach compliance with calculated emission levels	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Emission level	Level of a given electromagnetic disturbance emitted from a particular device, equipment, system or disturbing installation as a whole, assessed and measured in a specified manner.
Emission limit	Maximum emission level specified for a particular device, equipment, system or disturbing installation as a whole.
Planned level	Level of a particular disturbance in a particular environment, adopted as a reference value for the limits to be set for the emissions from the installations in a particular system, in order to coordinate those limits with all the limits adopted for equipment and installations intended to be connected to the power supply system.



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.10 USE CASE 10 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
10	Transmission, Distribution, Der, Customer / Enterprise, Operation, Station, Field, Process	Improving of LV network observability based on billing metering system by means of secure interface with SCADA-ADMS system

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	20.03.2023.	ELPROS	-	Preliminary approved
2	13.04.2023	ELPROS	Based on EMS comments from review	

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Optimal operation of distribution and LV network during normal operation and disturbances
Objective(s)	To improve LV network observability and consequently system security and quality of supply based on billing metering data used in SCADA/EMS system by means of secure interface between both systems (billing and SCADA)
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
Improvement of LV network observability and consequently system security and quality of supply based on billing metering data used in SCADA/EMS system by means of secure interface between both systems (billing and SCADA).
Complete description
<p>In order, to act on an optimal way in case of events, SCADA/ADMS needs to have totally clear picture about situation in the network. An essential part of loads and in future also generation (DER) are connected to low voltage network (LV). In order to act properly in crisis event, one need to have exact information about available resources and situation in the LV network.</p> <p>With Advances Distribution Management System (ADMS) perfect digital twin of the network itself is achieved, but information about the actual operation state and possible overloads or voltage limits violations is not available. With close to real-time (1 minute) information from the meters used for billing purposes, SCADA can get information about the actual LV network situation.</p> <p>Since the number of on-line measurements is limited, state estimator provides further information. Therefore, crisis actions on the higher level can be evaluated and ranked also according to the influence on LV loads.</p> <p>In order to get LV measurements into SCADA/ADMS system, establishment of secure communication protocols using the latest protective communication measures such as data encryption, access filtering from allowed IPs, multi-level login procedures and so on is essential.</p> <p>All implementations should be performed for automatic operation in real time. The data acquisition system must have automatic data checks that can detect attempts of unauthorized data read, receiving data outside the expected limits, and communication requests from unapproved addresses.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
<ul style="list-style-type: none"> • Actions are performed by “Flexibility system”, which collects data from: <ul style="list-style-type: none"> ○ billing system (mostly LV network and partially MV) ○ SCADA/ADMS system (data from HV and MV network). • Flexibility system evaluates the overall system operation continuously. Actions are triggered in case of violation of normal operation divided into 2 groups: <ul style="list-style-type: none"> ○ Events related to power system operation in case of overload, voltage limits violations, etc. ○ Events related to communication security.
Prerequisites
<ul style="list-style-type: none"> • Real-time information from the meters used for billing purposes • Real-time information from SCADA system • Results of state estimation • Known structural data (P installed, P min, Q diagram, voltage limits, etc.) • Secured communication connection between billing system and SCADA system

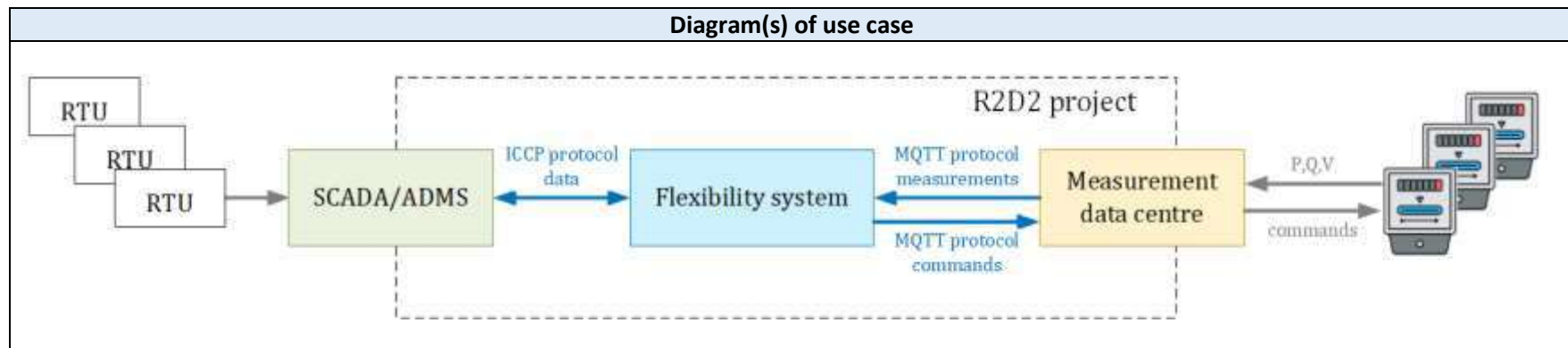
1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC5
Level of depth
High level of detail.
Prioritisation
Highest priority (5).
Generic, regional or national relation
Generic and national
Nature of the use case
System functional requirements description.
Further keywords for classification
Flexibility, emergency operation

1.8 General remarks

General remarks

2. Diagrams of use case



SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles.	
Actor name	Actor type	Actor description	Further information specific to this use case
Distribution System Operator (DSO)	System operator	‘Distribution system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	Output: Flexibility system installed at DSO will send signals to active customers and DER to decrease/increase voltage or disconnect the customer/DER from the grid. Input: <ul style="list-style-type: none"> P,Q,V from Active consumers and DER P,Q,V and topology from SCADA
Active customer	Prosumer	‘active customer’ means a final customer, or a group of jointly acting final customers, who consumes or stores electricity generated within its premises located within confined boundaries or, where permitted by a Member State, within other premises, or who sells self-generated electricity or participates in flexibility or energy efficiency schemes, provided that those activities do not constitute its primary commercial or professional activity Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	Output: information P, Q, V based on meters. Input: control signals sent from Flexibility system to perform actions like decrease/increase voltage or block/reduce the consumption.

D2.3 - Requirements and Detailed Architecture Design

Distributed energy resources (DER)	Generator	Distributed energy resources (DERs), are small-scale electricity supply or demand resources that are connected to the electric grid. They are power generation resources and are usually located close to load centres, and can be used individually or in aggregate to provide value to the grid.	Output: information P, Q, V. Input: control signals sent from Flexibility system to perform actions like generation reduction/increase
Grouping		Group description	
Software/Hardware component		Software/Hardware components used in UC16 business process	
Actor name	Actor type	Actor description	Further information specific to this use case
SCADA / ADMS system	Control system	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, databases, networked data communications and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plant or machinery. Advanced Distribution Management System (ADMS) comprises control functions to automatically control the network and support operators.	SCADA / ADMS system is used to provide real-time active & reactive power measurements, voltage measurements and network topology data.
Flexibility system	Control system	Flexibility system is software on virtual server, calculating congestions and voltage profiles and activates or block flexibility sources in distribution network.	Flexibility system is used to calculate operation limits and send actions to active sources to optimize the operation of the network.
Communication gateway	Communication system	Communication gateway is a part of Flexibility system enabling data exchange between different devices and systems by standard communication protocols: <ul style="list-style-type: none"> • TASE.2/ICCP • MQTT 	Communication gateway is a part of Flexibility system and enables data exchange between different systems and devices.
RTUs	Device	RTUs are used in the network nodes to collect data about topology and operation	SCADA receives information about network topology from RTUs.



D2.3 - Requirements and Detailed Architecture Design

Smart meters	Device	Smart metering system is an electronic system that is capable of measuring electricity fed into the grid or electricity consumed from the grid, providing more information than a conventional meter, and that is capable of transmitting and receiving data for information, monitoring and control purposes, using a form of electronic communication;	Smart meters send measurement to Flexibility system and receive commands for optimal operation of the power grid
--------------	--------	--	--

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Network optimal operation and operation during disturbances	Flexibility system is receiving in information from SCADA/ADMS system and from meters used for billing purposes in real-time (every 1 – 5 minutes). Flexibility system evaluates the overall system operation continuously. Flexibility system trigger actions in case of overloads, voltage limits violations, etc.	DSOs, Consumers (loads), DERs	Periodic (every 1 – 5 minutes)	The information below is available for further processing: <ul style="list-style-type: none"> Real-time information from the meters used for billing purposes. (P,Q, V) Real-time information from SCADA system (P,Q,V, topology) Results of state estimation 	<ul style="list-style-type: none"> Network operation state is known, Procedures for assuring stable operation of the grid in case of events are available
2	Assuring of secure communication channel between devices and system from Scenario 1 and procedures in case of attack	Establishment of secure communication protocols using the latest protective communication measures such as data encryption, access filtering from allowed IPs, multi-level login procedures between systems from Scenario 1. Actions are triggered in case of events related to communication security	DSOs, Consumers (loads), DERs	Periodic and random	System from Scenario 1 must operate. Implementation of secure communication protocols regarding to the specific of each protocol.	Procedures in case of detected security attack

4.2 Steps – Scenarios

Scenario								
Scenario name:		Network optimal operation and operation during disturbances						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Data acquisition Runs periodically (every 1 – 5 minutes)	Collecting data	Data acquisition from metering devices of different producers and from SCADA.	Data collection from remote sources	Consumer, DER, DSO / SCADA, smart meters, RTUs	DSO / Flexibility system	1, 2	
2	Data collected.	Data formats conversion	Specific data formats conversion in unified data format.	Data pre-processing	DSO / Flexibility system	DSO / Flexibility system	-	
3	Data format converted	Voltage profile and loading calculation	Service for voltage profile and loading calculation	Calculation	DSO / Flexibility system	DSO / Flexibility system	-	
4	Voltage profile and loading calculated	voltage profiles and loadings limit checking	Detection of voltages and loading outside the expected limits	Calculation	DSO / Flexibility system	DSO / Flexibility system	-	
5	Voltage profiles and loadings checked	Control action definition	Defining control actions to mitigate identified voltage and loadings outside the expected limits.	Calculation	DSO / Flexibility system	DSO / Flexibility system	-	
6	Control actions defined	Control actions sending	Actual control action on consumers/DER. Expected actions: on/off/increase/reduce	Command sending	DSO / Flexibility system	Consumer, DER / Smart meter	3	
7	Data acquisition	Collecting data	Data acquisition from metering devices of different producers and from SCADA.	Data collection from remote sources	Consumer, DER, DSO / SCADA, smart meters, RTUs	DSO / Flexibility system	1, 2	
8	Data collected	Checking of execution of control actions	Checking of received data if data values are	Back-loop control	DSO / Flexibility system	DSO / Flexibility system		

D2.3 - Requirements and Detailed Architecture Design

			changed according to the step 5					
9	Exception: Control action was not executed within expected time	Alarming	Consumer/DER is informed that it is excluded from control actions if it is confirmed that the control signal reached this consumer/DER	Alarm sending	DSO / Flexibility system	Consumer, DER	4	

Scenario								
Scenario name:		Assuring of secure communication channel between devices and system from Scenario 1 and procedures in case of attack						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Communication security check in each in steps 1, 6, 7 and 9 of previous scenario	Collecting data / Commands transfer	Data acquisition / commands sending	Data exchange	Consumer, DER, DSO / SCADA, smart meters, RTUs	DSO / Flexibility system	1,2,3,4	
2	Data collected	Attack detection	Detect attempts of unauthorized data read, receiving data outside the expected limits, communication requests from unapproved addresses.	Real-time communication security check and data processing	DSO / Flexibility system	DSO / Flexibility system	-	
3	Attack detected	Alarming/ optional blocking control actions	Activation of security procedures in case of attack	Real-time data processing	DSO / Flexibility system	DSO (IT security department)	5	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	P,Q and V data	Active power, reactive power and voltage profile measurements from smart meters, SCADA and state estimator	
2	Topology information	Topology information from SCADA and state estimator	
3	Commands	Signals which perform control action Expected actions: on/off/increase/reduce	
4	Alarm	Alarm sending in case that command was not executed	
5	Security alarms	Security alarm to IT security department	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
P	Active power
Q	Reactive power
V	Voltage
DER	Distributed energy resource



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.11 USE CASE 11 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
11	Transmission, Distribution, Der, Customer / Enterprise, Operation, Station, Field, Process	DSO - TSO congestion and power quality coordination in application of system services

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	07.04.2023	ELEK	-	Preliminary approved
2	14.04.2023	ELEK	Based on EMS comments from review	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	System Operator Scenario
Objective(s)	O1. Improve the coordination between TSO and DSO during emergency conditions O2. Improve the visibility of flexibility resources in DSO, for TSO and BRP to be activated in case of critical or emergency conditions O3. Define optimal capacity of flexibility resources according to grid constraints and limitations.
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
DSO-TSO coordination in case of congestion or power quality issues in the network and consequently imposed limitations in ancillary service availability restrictions in distribution network.
Complete description
<p>With increased share of volatile RES in the system, they will together with flexible loads participate in bigger extent in the ancillary services and balancing mechanism. The idea is, that TSO or any other actor can directly or indirectly engage ancillary service and flexibility providers also in distribution network. This network can be connected to the TSO, but according to EU regulation 2019/943, 2017/1485, 2017/2195 it could be even in another country (some frequency related services are now already open to be provided anywhere inside the interconnection). Therefore, it is important for TSO to have prompt information about availability of these resources. This is valid also for responsible actors of balancing groups, which are another potential user of these services. DSO shall not interfere with this business except in case, power supply integrity is endangered in the sense of power quality or stability (possible congestions leading to outages). Therefore, these contracts and locations of providers are not necessarily known to DSO. So, information about limitations in the network shall be distributed to all users of these services, which register for getting them. This can be TSO, aggregators or responsible for balance of balancing groups. But for sure, there are more actors, that are potentially interested in these data.</p> <p>So, in R2D2 we will develop tools to provide information about possible limitations in our network affecting availability of these resources (forecasts) and definite limitations (on-line measurements) in case of congestions and/or power quality issues in particular part of the network. Since we do not know exactly, which customers have contract to provide these services, we are giving information for all of them in the shape of location defined by measuring point.</p> <p>This information will be available in the shape of xml schemes according to OneNet project reference architecture and related IEC standards and ENTSO propositions. Broker technology will be applied for transfer. Therefore, there are no limitations if TSO and DSO are not in the same country.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions <p>Triggering is done by so called flexibility server, which collects data from billing system (mostly LV network and partially MV) on one side and SCADA/ADMS system on the other (data from HV and MV network). It evaluates the overall system operation continuously. Actions are triggered in case of violation of normal operation divided into 2 groups:</p> <ul style="list-style-type: none"> • Events related to power system operation in case of overload or voltage deviations that may lead to outage or can influence life time of equipment. • Events related to violations of power quality of supply, mostly voltage out of tolerances, sinusoidal distortion or flicker.
Prerequisites <ul style="list-style-type: none"> • Real-time information from the meters used for billing purposes. • Real-time information from SCADA system • Accessible results of state estimation • Known Structural data (P installed, P min, Q diagram, voltage limits, etc.) • Secured communication connection between billing system and SCADA system • Involved actors need to have systems able to exchange information and acting based on these information. • Weather data available from Hydro meteorological institution (desirable but not obligatory)

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
-
Level of depth
High level of detail.
Prioritisation
Highest priority (5). This service so far doesn't exist in the Slovenian power system or this is done manually.
Generic, regional or national relation
Generic and national, has potential to regional.
Nature of the use case
System functional requirements description.
Further keywords for classification
Flexibility, Traffic Light System, TSO-DSO coordination, Emergency operation.

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Distribution System Operator (DSO)	System operator	‘Distribution system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	DSO control centre sends signal about the locations, where flexibility can’t be used due to potential congestions.
TSO, Aggregator, Balance group responsible	Market participant	‘Market participant’ means market participant as defined in point (25) of Article 2 of Regulation (EU) 2019/943 (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	Market participant receives signal sent by DSO and block use of a particular flexibility source.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Hardware/Software components		Hardware/Software components used in UC11 business process	
Actor name	Actor type	Actor description	Further information specific to this use case
SCADA / ADMS system	Control system	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, databases, networked data communications and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plant or machinery. Advanced Distribution Management System (ADMS) comprises control functions to automatically control the network and support operators.	SCADA / ADMS system is used to provide real-time active & reactive power measurements and network topology data.
Flexibility procurement system (Flex server)	Control system	Flex server is software on virtual server, that calculates congestions and activates or block flexibility sources in distribution network.	Flex server is used to calculate operation limits and block flexibility activation in case, this could worsen the situation in the network.
RTUs	Device	RTUs are used in the network nodes to collect data about topology and operation	RTUs are devices, where from SCADA gets information about topology.
Meters	Device	Meters are devices to measure energy consumption for billing purposes.	From meters we collect loading and voltages for estimation of the situation in the distribution MV and LV networks.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Estimation of flexibility availability during normal operation and congestion	System will provide and send information about possible limitations in DSO network affecting availability of flexible resources (forecasts) and definite limitations (on-line measurements) in case of congestions and/or power quality issues in particular part of the network enabling both DSO and TSO to use these resources optimally.	DSO	Regular repetition every 1-5 minutes.	The information below is available for further processing: <ul style="list-style-type: none"> • Real-time information from the meters used for billing purposes. (P,Q, V) • Real-time information from SCADA system (P,Q,V, topology) • Results of state estimation thresholds and limits voltages and loadings defined by preliminary studies 	Know available flexibility of Consumers and DER during normal operation and congestion.
2	Assuring of secure communication channel between devices and system from Scenario 1 and procedures in case of attack	Establishment of secure communication protocols using the latest protective communication measures such as data encryption, access filtering from allowed IPs, multi-level login procedures between systems from Scenario 1 Actions are triggered in case of events related to communication security	DSOs, Consumers (loads), DERs	Periodic and random	System from Scenario 1 must operate. Implementation of secure communication protocols.	Procedures in case of detected security attack



D2.3 - Requirements and Detailed Architecture Design

4.2 Steps – Scenarios

Scenario								
Scenario name:		Estimation of flexibility availability during normal operation and congestion						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Data acquisition (Runs periodically)	Collecting data	Data acquisition from metering devices of different loads, producers and network elements (TS)	Data collection	Consumer, DER, DSO, / SCADA, smart meters, RTUs	DSO / Flexibility system	1,2,3	
2	Data collected	Data formats conversion	Specific data formats conversion in unified data format.	Data pre-processing	DSO / Flexibility system	DSO / Flexibility system	-	
3	Data format converted	State estimation	Calculation of network state. (Voltage profiles and loadings)	Calculation	DSO / Flexibility system	DSO / Flexibility system	-	
4	Voltage profile and loading calculated	Voltage profiles and loadings limit checking	Detection of data (voltages and power) outside the expected limits dangerous to broke contractual power quality parameters and allowed loadings	Calculation	DSO / Flexibility system	DSO / Flexibility system	-	
5	Voltage profiles and loadings checked	Restrictions activation	Defining restrictions in ancillary service control actions to prevent voltage	Calculation	DSO / Flexibility system	DSO / Flexibility system	-	

D2.3 - Requirements and Detailed Architecture Design

			and loadings outside the expected limits					
6	Restrictions activated	Aggregators notification	Actual restrictions are sent to all service providers	Data sending	DSO / Flexibility system	TSO, Aggregator, Balancing responsible, Consumer, DER / RTU, meter	4,5,6	
7	Data acquisition	Collecting data	Data acquisition from metering devices of different loads, producers and network elements (TS)	Data collection	Consumer, DER, DSO, / SCADA, smart meters, RTUs	DSO / Flexibility system	1,2,3	
8	Data collected	Control action effect checking	Status of any changes under restrictions checked with real values received from metering devices.	Calculation	DSO / Flexibility system	DSO / Flexibility system	-	

Scenario								
Scenario name:		Assuring of secure communication channel between devices and system from Scenario 1 and procedures in case of attack						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Communication security check in each in steps 1, 6 and 7 of the previous scenario	Collecting data / Commands transfer	Data acquisition / commands sending	Data exchange	Consumer, DER, DSO / SCADA, smart meters, RTUs	DSO / Flexibility system	1,2,3,4,5,6	
2	Data collected	Attack detection	Detect attempts of unauthorized data read, receiving data outside the	Real-time communication security check	DSO / Flexibility system	DSO / Flexibility system	-	



D2.3 – Requirements and Detailed Architecture Design

			expected limits, communication requests from unapproved addresses.	and data processing				
3	Attack detected	Alarming/ optional blocking control actions	Activation security procedures in case of attack	Real-time data processing	DSO / Flexibility system	DSO (IT security department)	7	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Active power measurements	P	
2	Reactive power measurements	Q	
3	Voltage measurements	U	
4	Flexibility limits power increase	Boolean	
5	Flexibility limits power decrease	Boolean	
6	Connection nodes under restrictions	Connection point IDs	
7	Cyber Attack identification message	Attack type code	
1	Active power measurements	P	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.



7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.12 USE CASE 12 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
12	Transmission / Operation	Emergency & Restoration - Over-frequency protection module

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	08.03.2023	EMSS	-	Preliminary approved
2	20.04.2023	EMSS	Requirements definition, use case improvement after revision	Approved
3	16.11.2023	EMSS	Use case redefinition, additional requirements definition	Approved
4	30.11.2023	EMSS	Use case redefinition	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Transmission system operation during emergency and restoration
Objective(s)	Create a centralized system that would simulate the lack of limited sensitive frequency mode-overfrequency (LFSM-O) on generating units in the power system
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
The Emergency & Restoration - Over-frequency protection module (OFPM) is designed as a replacement for the missing or insufficient controllers on generating units in the power system which can operate in limited frequency sensitivity mode – over-frequency (LFSM-O).
Complete description
<p>In the CROSSBOW project, two conceptual solutions for over-frequency protection system were developed, as a replacement for the missing or insufficient LFSM-O controllers (as defined in EU Regulation 2016/631 – Network Code on requirements for grid connection of generators) on generators in Serbia and in the region of Southeast Europe. According to EU Regulation 2017/2196 (Network Code on Emergency and Restoration), such a system must properly disconnect the generators.</p> <p>The first solution implied that the over-frequency protection system calculates settings for each generator in a predetermined order provided by TSOs (which takes into account local congestions), starting with 50.2 Hz (and up to 52Hz). These calculations are performed every 5 – 15 min due to changes in production in real time. In the event of a critical frequency, the Over-frequency Protection (OFP) system sends a command for generator disconnection to selected generators. In the case of application at the regional level, this system takes care not to cause unacceptable flows on the interconnecting transmission lines when the generator is disconnected by the over-frequency protection.</p> <p>The second solution implies that the generators, based on real-time measurements and calculations based on the developed algorithm, are assigned one of the predefined levels of over-frequency protection in the frequency range 50.2 - 52 Hz. Local constraints are controlled by assigning different levels of OFP to the protection devices on generators in one power plant. The OFP algorithm fills the quotas for each level of the over-frequency protection so that the effect corresponds to the virtual activation of the LFSM-O on all generators in the system. This solution was simulated for both national and regional levels.</p> <p>Based on CROSSBOW results, the modified over-frequency protection system will be implemented within R2D2 project in the transmission system of the Serbian TSO. As not all generators are equipped to carry out above given technical solution for the Emergency & Restoration - Over-frequency protection module (OFPM), they will be divided into several groups as follows:</p> <ol style="list-style-type: none"> 1. The first group of generators are generators that are equipped with LFSM-O and they do not participate in the OFPM. 2. The second group of generators will be assigned fixed over-frequency protection settings (where there are no technical possibilities for remote signal sending neither LFSM-O controllers are installed) – this is not the part of this use case 3. To the third group (where there are technical possibilities for sending signals remotely), the OFPM sends appropriate signals, which can be related to: <ol style="list-style-type: none"> a) Reduction of active power production on generators (group A) b) Disconnection of the generators from the transmission grid (group B)

D2.3 - Requirements and Detailed Architecture Design

This type of over-frequency protection system will have the role of reducing the total production in the system as closely as possible when impermissibly high frequencies occur, as if each generator is equipped with an LSFM-O controller. In addition, this system will ensure that there are no local violations of the security criteria in the network.

On the other hand, as it will be implemented at the national and not at the regional level, this OFPM will only be able to control to a lesser extent the change in active power flows on the interconnecting lines and the impacts on neighbouring systems (this can only be achieved if there is a regional implementation of the OPFM, which may be the subject of one of the future projects). Also, this system is not intended to control high frequencies in case of splitting the system into subsystems, as its main intention is to bring the Serbian TSO into compliance with the binding provisions of the EU network codes.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Generators that cannot receive command signals have fixed over-frequency protection settings harmonized with the OFPM. Protection devices operate autonomously in case of over-frequency. SCADA AGC runs autonomously after calculated set-points are received from OFPM. SCADA system transfers disconnection signal generated by OFPM to appropriate circuit breakers in the connection facility of a generator.
Prerequisites
Generating units are capable of receiving a set point to reduce their active energy production, or generating units can be remotely - disconnected from the TSO control centre, or over-frequency protection of the generating units can be reset from the TSO control centre.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
High level of detail.
Prioritisation
Highest priority (5). The centralized over-frequency protection does not currently exist in the Serbian power system, and it is necessary for the application of NC ER requirements.
Generic, regional or national relation
Generic and national.
Nature of the use case
System functional requirements description.
Further keywords for classification
Over-frequency protection, Emergency operation.

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO)	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSO control centre sends signal to decrease active power generation or reset over-frequency protection or to disconnect a generator. TSO facility to which a generator is connected receives signal to reset over-frequency protection or to disconnect a generator and execute the command.
Producer	Market participant	Producer means a natural or legal person who generates electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	Producer receives signal to decrease active power generation and execute the command sent by TSO.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Hardware/Software components		Hardware/Software components used in OFP business process	
Actor name	Actor type	Actor description	Further information specific to this use case
SCADA system	Control system	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, networked data communications and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plant or machinery.	SCADA system is used to provide real-time active power generation and frequency measurements.
OFPM	Control system	OFPM is a part of the control system designed to reduce active power production when an over-frequency threshold is reached.	OFPM is used to reduce the active power output by sending a set point signals, a generator disconnection signals and a reset of the over-frequency protection device settings.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Over-frequency identification	OFPM regularly receives SCADA measurements and calculates if OFPM should be activated and through which mechanism (Active power generation decrease or Generators disconnection) based on comparison of needed active power decrease and available downward reserve	TSO/OFPM	Regular repetition	Frequency is monitored	Over-frequency is identified and OFPM is activated
2	Active power generation decrease	Set-points are calculated and sent to the generating units of group A to decrease their active power output.	TSO/OFPM	OFPM triggered active power generation decrease	Generating units of group A follow regular generation schedule	Generating units of group A decrease their active power output according to the set-point sent by the OFPM
3	Generators disconnection	Disconnection frequencies are calculated for all generators of group B, and disconnection signals are sent to generators if measured frequency is higher than the disconnection frequency.	TSO/OFPM	OFPM triggered generators disconnection mechanism	Generating units of group B follow regular generation schedule	Some generating units of group B are disconnected

4.2 Steps – Scenarios

Scenario								
Scenario name:		Over-frequency identification						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Regular repetition	SCADA measurements download	Each 2-4 seconds SCADA systems sends to the OFPM frequency and generators active power measurements	Data download	TSO/SCADA system	TSO/OFPM	1,2	IRI_017, IRI_105, IRI_106
2	Over-frequency threshold is reached	Calculations of needed active power decrease and available downward reserve	OFPM calculates needed active power decrease and available downward reserve	Data processing	TSO/OFPM	TSO/OFPM	-	IRI_017, IRI_088, IRI_089, IRI_090, IRI_091, IRI_105, IRI_106, IRI_107, IRI_108
3	Calculations are completed	Triggering of active power generation decrease mechanism or generators disconnection mechanism	Based on comparison of needed active power decrease and available downward reserve OFPM triggers 1) active power generation decrease mechanism or 2) generators disconnection mechanism	Data processing	TSO/OFPM	TSO/OFPM	-	IRI_017, IRI_092, IRI_093, IRI_105, IRI_106, IRI_108

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Active power generation decrease (generators of group A)						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	OFPM triggered active power generation decrease	Set-points calculation	OFPM calculates generators set-points	Data processing	TSO/OFPM	TSO/OFPM	-	IRI_017, IRI_094, IRI_095, IRI_096, IRI_097, IRI_098, IRI_099, IRI_105, IRI_106, IRI_108, IRI_109
2	Set-points are calculated	Set-points transfer	OFPM sends generators set-points to SCADA/AGC	Data transmission	TSO/OFPM	TSO/SCADA system (AGC)	3	IRI_017, IRI_100, IRI_105, IRI_106, IRI_108, IRI_109

Scenario								
Scenario name:		Generators disconnection (generators of group B)						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	OFPM triggered generators disconnection mechanism	Frequency disconnection calculations	OFPM calculates generators disconnection frequency	Data processing	TSO/OFPM	TSO/OFPM	-	IRI_017, IRI_101, IRI_102, IRI_103, IRI_105, IRI_106, IRI_108, IRI_110
2	Disconnection frequency are calculated	Generators disconnection	OFPM sends disconnection signal for selected generators (according to calculated disconnection frequencies within scenario 1)	Data transmission	TSO/OFPM	TSO/SCADA system	4	IRI_017, IRI_104, IRI_105, IRI_106, IRI_108, IRI_110

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Active power measurements	Active power measurements on generating units	
2	Over-frequency protection settings	Over-frequency settings for protection devices in generator's connection point to the transmission system	
3	Protection re-set confirmation signal	Signal generated by a protection device on activated and deactivated frequency levels	
4	Frequency measurements	Measured frequency in the power system	
5	Active power set-points	Set-point for generators' active power controllers (controller leads generator's active power to the set-point value)	
6	Disconnection signals	Signal which triggers selected circuit breaker opening.	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Limited Frequency Sensitive Module – Over-frequency	Limited frequency sensitive mode — over-frequency or LFSM-O means a power-generating module or HVDC system operating mode which will result in active power output reduction in response to a change in system frequency above a certain value (Commission Regulation (EU) 2016/631 establishing a network code on requirements for grid connection of generators)



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.13 USE CASE 13 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
13	Transmission /enterprise, Operation	Cost-sharing of remedial actions with cross-border impact in West Balkan region

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	08.03.2023	EMSS	-	Preliminary approved
2	20.04.2023	EMSS	Requirements definition (regarding EMMA product)	Preliminary approved
3	12.06.2023	EMSS, SCC	Use case improvement after revision	Approved
4	29.11.2023	EMMS	Additional requirements definition	Approved

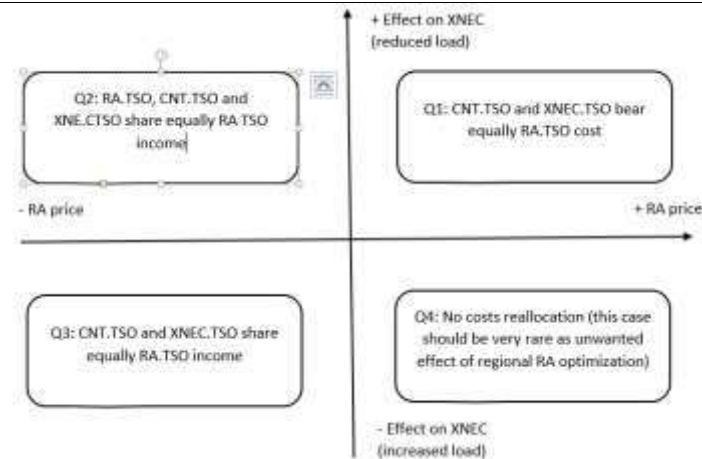
1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Cost sharing between TSOs for remedial actions with cross-border impact
Objective(s)	Define an algorithm for the cost-sharing between TSOs in West Balkan region in case of activation of remedial actions with cross-border impact
Related business case(s)	BC1, BC4

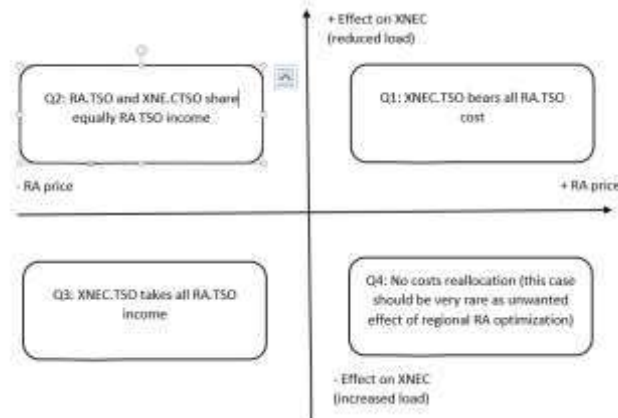
1.4 Narrative of use case

Narrative of use case
Short description
<p>Cost-sharing methodology for the remedial actions (RAs) costs with cross-border impact between transmission system operators (TSOs) is one of the most important mechanisms applied in the coordinated regional cross-border capacity calculation and regional operational security coordination.</p> <p>The cost-sharing methodology (CSm) is used in the Coordinated Regional Operational Security Assessment (CROSA) process after optimizing remedial actions (RA) at the regional level. This methodology is necessary to define the reallocation of RA costs (and revenues) after activation of RAs in national balancing mechanisms. This methodology relies on strong socialization of RA costs between involved TSOs.</p>
Complete description
<p>The RA cost-sharing mechanism is envisaged by the network codes CACM (EU regulation 2015/1222) and SO GL (EU regulation 2017/1485), as well as the methodologies derived from these codes (for example the Coordinated Security Analysis methodology).</p> <p>These network codes become mandatory for the Western Balkans TSO based on:</p> <ul style="list-style-type: none"> - Synchronous Area Framework Agreement concluded among TSOs of Continental Europe - Decision of the Ministerial Council of the Energy Community (Dec, 2022) <p>This use case proposes CSm based on 4 elements:</p> <ul style="list-style-type: none"> - Contingencies (CNTs) that requires RAs activation - Cross-border relevant network element with contingency (XNECs) due to a CNT (or in special cases, even without CNT, that is, it appears in the base case scenario without simulating the unavailability of a grid element) - RAs costs - TSOs involved (TSOs in which control areas are CNTs and/or XNECs and/or applied RAs) <p>Proposed CSm has 2 levels:</p> <ul style="list-style-type: none"> - 1st level is technical in nature and serves to decompose the costs of all implemented RAs to each XNEC – CNT pair (or only to XNEC for base case constraints) - 2nd level is social in nature and serves to redistribute the cost calculated in the first level to involved TSOs <p>Involved TSOs are:</p> <ul style="list-style-type: none"> - RA.TSO – TSO in which Control Area a RA is activated - XNEC.TSO – TSO in which Control Area is XNEC - CNT.TSO – TSO in which Control Area is CNT <p>The basic idea for cost-sharing level 2 is presented in the following figure (in case there is a contingency):</p>

D2.3 - Requirements and Detailed Architecture Design



In case when constraint exists in base case scenario, this figure is adapted as follows:



CSm is implemented for each basic market interval relevant for system operation planning (one hour at the moment) of a day. Then all results are aggregated to create invoices between TSOs, according to financial accounting and taxation rules.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
This use case does not address the determination and optimization of RAs.
Prerequisites
TSOs agree on RAs to be applied, responsible TSO activates the RA as previously agreed

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
High level of detail.
Prioritisation
Highest priority (5). This mechanism does not currently exist in the West Balkans region, and it is necessary for the application of SOGL (EU regulation 2017/1485) requirements and methodologies arising from this regulation.
Generic, regional or national relation
Regional.
Nature of the use case
System functional requirements description.
Further keywords for classification
Remedial actions, Cross-border impact, Operational security, Cost-Sharing.

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO)	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSOs provide information on the prices of remedial actions and apply the results of cost-sharing.

D2.3 - Requirements and Detailed Architecture Design

Regional coordination centre (RCC)	Regional coordination body	'Regional coordination centre' means regional coordination centre established pursuant to Article 35 of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity. Regional coordination centres shall complement the role of transmission system operators by performing the tasks of regional relevance assigned to them.	RCC collects inputs from TSOs and provides results for cost-sharing.
------------------------------------	----------------------------	--	--

Grouping		Group description	
Software/Hardware components		Software/Hardware components used in cost sharing calculation business process	
Actor name	Actor type	Actor description	Further information specific to this use case
TSO-DSO communication platform* / E-mail	Communication platform	A communication platform used for communication between TSO and DSO / A communication method that uses electronic devices to deliver messages across computer networks.	In this use case it is used to exchange RA cost-sharing calculation input and output data, as well as to launch conference call
FTP server	Sever	A computer program or device that provides a service to another computer program and its user, also known as the client	In this use case it is used to get grid models needed for PTDF calculation
Power flow software	Calculation software	A software used to calculate power flows and voltages in the base case as well as after contingencies. In addition, it can calculate the PTDF matrix.	In this use case it is used to calculate the PTDF matrix.
RA cost-sharing software	Calculation software	A software designed to calculate RA cost sharing.	This software calculates distribution of RA costs between involved TSOs.

*Optional actor

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Success (basic) scenario	All TSOs accept cost sharing results.	RCC / EMMA RA cost-sharing software (EMMA RA CSS)	Application of RAs with cross-border impact.	TSOs and RCC agree on RAs to be applied, responsible TSO activates the RA, relevant grid models are available, TSOs inform RCC on RAs costs.	RCC distributes to all affected TSOs invoices regarding RA cost-sharing.
2	Exceptional scenario	At least one TSO does not accept the results of cost sharing.	RCC / RA cost-sharing communication platform	At least one TSO does not accept the results of cost sharing.	RCC proposes the results of cost sharing.	RCC distributes to all affected TSOs invoices regarding RA cost-sharing.

4.2 Steps – Scenarios

Scenario								
Scenario name:		Success scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	RAs implemented	RA costs uploading	TSO uploads RA data on RA cost-sharing communication platform or E-mail	Data uploading	TSO / EMMA RA cost-sharing communication platform or E-mail	RCC / EMMA RA cost-sharing communication platform or E-mail	1	EMM_036
2	RA costs uploaded	Grid models selection	RCC imports relevant grid models from Grid model server	Data importing	RCC / Grid model server	RCC / power flow software	2	

D2.3 - Requirements and Detailed Architecture Design

3	Grid models downloaded	PTDF calculation	RCC calculates base case power flows and PTDF matrix for selected grid models and stores them	Calculation	RCC / power flow software	RCC / Grid model server	3, 7	
4	Base case power flows and PTDF matrices calculated	RA costs data download	RCC downloads RA costs	Data downloading	RCC / EMMA RA cost-sharing communication platform or E-mail	RCC / EMMA RA CSS	1	EMM_036, EMM_037, EMM_091
5	RA costs data downloaded	RCC downloads base case power flows and PTDF matrix	RCC downloads base case power flows and PTDF matrix	Data downloading	RCC / Grid model server	RCC / EMMA RA CSS	3,7	
6	PTDF matrix downloaded	Cost-sharing results calculation	RCC calculates cost sharing results	Calculation	RCC / EMMA RA CSS	RCC / EMMS RA CSS	-	EMM_037, EMM_077, EMM_078, EMM_079, EMM_080, EMM_081, EMM_082, EMM_083, EMM_084, EMM_085, EMM_086, EMM_087, EMM_087, EMM_092, EMM_094, EMM_095, EMM_096, EMM_097, EMM_098, EMM_099, EMM_100, EMM_101, EMM_102, EMM_103, EMM_104, EMM_105, EMM_106, EMM_107, EMM_108
7	Cost-sharing results calculated	Cost-sharing results uploading	RCC uploads cost sharing results on RA cost-sharing communication platform	Data uploading	RCC / EMMA RA CSS	TSOs / EMMA RA cost-sharing communication platform or E-mail	4	EMM_036
8	Cost-sharing results uploaded	Cost-sharing confirmation	TSOs check on cost sharing results	Confirmation/ Rejection	TSOs / EMMA RA cost-sharing communication platform or E-mail	RCC / EMMA RA cost-sharing communication platform or E-mail	5	EMM_036

D2.3 – Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Exceptional scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Cost-sharing results rejected	Cost sharing dispute resolution	All TSOs and RCC discuss the cost sharing inputs and outputs to resolve the objection	Conference call	TSOs, RCC (RA cost-sharing communication platform)	TSOs, RCC (RA cost-sharing communication platform)	6	EMM_036

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	RA costs	RA costs in euros for each full hour interval (00:00 – 01:00, 01:00 – 02:00 ... 23:00 – 24:00) in which RA was applied	
2	Common Grid Model	See the definition	
3	PTDF matrix	See the definition	
4	RA cost sharing results	Monetary transaction between two TSOs based on cost sharing methodology, for each RA applied in each full hour interval	
5	Confirmation or rejection of the of the cost sharing results	Confirmation or rejection of the cost sharing results by relevant TSOs	
6	Correction of RA costs input data or grid models used for PTDF calculation	Correction of cost-sharing calculation input data: RA costs or CGM (PTDF)	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Coordinated regional operational security assessment	An operational security analysis performed by an RCC on a common grid model, in accordance with Article 78 of the SOGL (EU regulation 2017/1485).
Contingency	Unavailability of a network element is simulated in CROSA process.
Constraint	A situation in which there is a need to prepare and activate a RA in order to respect operational security limits.
Cross-border relevant network element	A network element identified as cross-border relevant and on which operational security violations need to be managed in a coordinated way.
Cross-border relevant network element with contingency	An XNE associated with a contingency. For the purpose of the CROSA, the term XNEC also cover the case where a XNE is used in operational security analysis without a specified contingency.
Remedial Action	Any measure according to Article 22.1 of the SOGL which is applied by a TSO or several TSOs, manually or automatically, in order to maintain operational security.
PTDF matrix	Power Transfer Distribution Factors (PTDF) indicate the incremental change in real power that occurs on transmission lines due to real power transfers between two regions. These regions can be defined by areas, zones, super areas, single buses, injection groups or the system slack (in this use case PTDF refers to injections/withdrawals). These values provide a linearized approximation of how the flow on the transmission lines and interfaces change in response to a transaction between the Seller (source) and the Buyer (sink).
Common Grid Model (CGM)	Common Grid Model means a Union-wide data set agreed between various TSOs describing the main characteristic of the power system (generation, loads and grid topology) and rules for changing these characteristics during the capacity calculation process;
FTP SERVER	Operational Planning Data Environment - An ENTSO-E communication platform used for communication of data needed in operational planning processes.



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.14 USE CASE 14 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
14	Transmission / Operation	Automation of transient stability calculations

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	29.03.2023	EMSS	-	Preliminary approved
2	25.04.2023	EMSS	Requirements definition	Preliminary approved
3	03.08.2023	EMSS	Further requirements definition	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Checking the compatibility of busbar protection settings with the operation of synchronous generators, in terms of transient (rotor angle) stability.
Objective(s)	Calculation of critical fault clearing time for all selected busbars.
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
Calculating critical fault clearing time for selected busbars. The results will be used for the improvement of existing or the introduction of new protection devices.
Complete description
The critical duration of a fault on a bus is the maximum duration of a fault (usually of the 3 phase short circuit type) which still does not lead to the outage of any synchronous machine (due to loss of synchronism) in the power system. The critical fault clearing time depends, among other things, on whether the fault disappears or is switched off by the action of the protection devices. In order to check the compatibility of busbar protection settings with the operation of synchronous generators in terms of stability, for the characteristic operating regimes of the year (or even more frequent in the future), critical fault clearing time calculations are performed for specified busbars of the transmission system. Based on the results of these calculations, introduction of new protection devices is proposed, for example, introduction of differential protection of busbars. Therefore, it's useful to create a script (under the DlgSILENT Power Factory program), which would automate the described process.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Validation of the grid model against convergence of static and dynamic calculations is checked in PowerFactory before starting the TSC Script.
Checking the compliance of the protection settings with the calculated fault clearing times is performed beyond the TSC Script.
Prerequisites
Proper grid model is available.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
High.
Prioritisation
High priority (4). The use case is of high importance, due to the expected increase in the participation of RES in the total production of electricity, and the results of this analysis may show the necessity of re-dispatching power plants.
Generic, regional or national relation
Generic.
Nature of the use case
System functional requirements.
Further keywords for classification
Critical fault clearing time calculation, transient stability, rotor angle stability

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
EMS – Elektromreža Srbije (Serbian TSO).	TSO	TSO – “Transmission system operator” – natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSO is obliged to provide the stability of transmission system operation. One aspect of stability is the transient stability (stability of synchronous generator rotor angle).

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Software/Hardware components		Software/Hardware components used in automation of transient stability calculations	
Actor name	Actor type	Actor description	Further information specific to this use case
EMMA Transient Stability Calculations (TSC) Script	Script	A script is a program or sequence of instructions that is interpreted or carried out by another program rather than by the computer processor.	The TSC Script runs on DlgSILENT PowerFactory and serves to automate transient stability calculations for all synchronous generators represented in the grid model.
Server	Server	A server is a computer program or device that provides a service to another computer program and its user, also known as the client	Sever is used to store calculations results

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Basic scenario	Critical fault clearing time calculation	TSO / EMMA TSC Script	Regular repetition (grid model is validated against convergence of static and dynamic calculations in PowerFactory)	Compatibility of bus-bar protection settings with the terms of stability of synchronous generators operation is not known.	Compatibility of bus-bar protection settings with the terms of stability of synchronous generators operation is confirmed or incompatibilities are detected.

4.2 Steps – Scenarios

Scenario								
Scenario name:								
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Regular repetition (grid model is validated against convergence of static and dynamic calculations in PowerFactory)	Presetting the TSC script	Preparing all the necessary input data for the TSC script and setting up options of the script itself.	Calculation parameter settings	TSO / Operator	TSO / EMMA TSC Script	1	EMM_040, EMM_055, EMM_056, EMM_057, EMM_058, EMM_059

D2.3 - Requirements and Detailed Architecture Design

2	Presetting the TSC script is finished	Executing the TSC script	Calculation of maximum periods during which the transient stability of the synchronous generation operation after a fault is preserved (rotor angle stability)	Calculations	TSO / EMMA TSC Script	TSO / Server	2	EMM_040, EMM_060, EMM_061, EMM_062, EMM_063, EMM_064
---	---------------------------------------	--------------------------	--	--------------	-----------------------	--------------	---	---

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Setting up the initial script options	Maximum/minimum clearing time, simulation starting time, total simulation time, accuracy time step for clearing time...	
2	Calculation results	Maximum periods during which the stability of the synchronous generators stability after a fault is preserved	EMM_040

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Transient stability	Transient stability or rotor angle stability is the ability of interconnected synchronous generators of a power system to remain in synchronism after being subjected to a disturbance.
Critical fault clearing time	The Critical Fault Clearing Time (CFCT) is the most common criteria for evaluation of transient angle stability. The CFCT is the maximum time during which a disturbance can be applied without the system losing its stability.

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.15 USE CASE 15 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
15	Transmission and Distribution / Operation	TSO-DSO cooperation in Individual Grid Model creation

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	27.03.2023	EMSS		Preliminary approved
2	13.06.2023	EMSS	UC improvement after revision	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Improved quality of IGM
Objective(s)	Establish TSO-DSO coordination in IGM creation recognizing high RES integration at the distribution level.
Related business case(s)	BC1, BC4

1.4 Narrative of use case

Narrative of use case
Short description In order to create more accurate IGMs, it is necessary to appreciate the production of power plants at the distribution level. Instead of forecasting the power flow at the TSO-DSO interface, it is better to forecast and model the distribution load separately and the distributed generation separately.
Complete description In order to make the most of the possibilities of the transmission network, it is necessary to achieve the maximum accuracy of the individual grid models (IGMs). In order to achieve this under the conditions of RES integration at the distribution level, it is necessary for TSOs and DSOs to establish appropriate coordination in the preparation of the IGMs. TSO-DSO coordination should include the following: <ul style="list-style-type: none"> – DSO has a database of distributed production capacities (type of facility, location, substations whose area it belongs to) – TSO makes a forecast of distribution consumption by nodes – TSO and/or DSO prepares a forecast of distributed generation sources – TSO submits to DSO the forecast of distribution consumption and distributed generation sources – DSO proposes corrections: <ul style="list-style-type: none"> ○ in case of a change in the topology of the distribution network, which shifts the load from one node to another (e.g. due to works in the distribution network) ○ due to specific network conditions (network failures) ○ due to specific operational limitations of production units – DSO submits proposed corrections to TSO with explanation – TSO and DSO discuss the proposed changes in a teleconference (if necessary) – TSO corrects IGM based on TSO-DSO coordination – TSO monitors the improvement of the quality of IGM after the establishment of TSO-DSO coordination

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
In the process of creating the IGM model, TSO creates a lfd (load forecast data) – i.e. file that contains data on consumption and production at DSO side (110/x kV/kV nodes) on the ground of harmonized distributed generation and load forecast, subject to this use case.
Prerequisites
DSO has a database of distributed production capacities, TSO makes a forecast of distribution consumption and production by nodes.

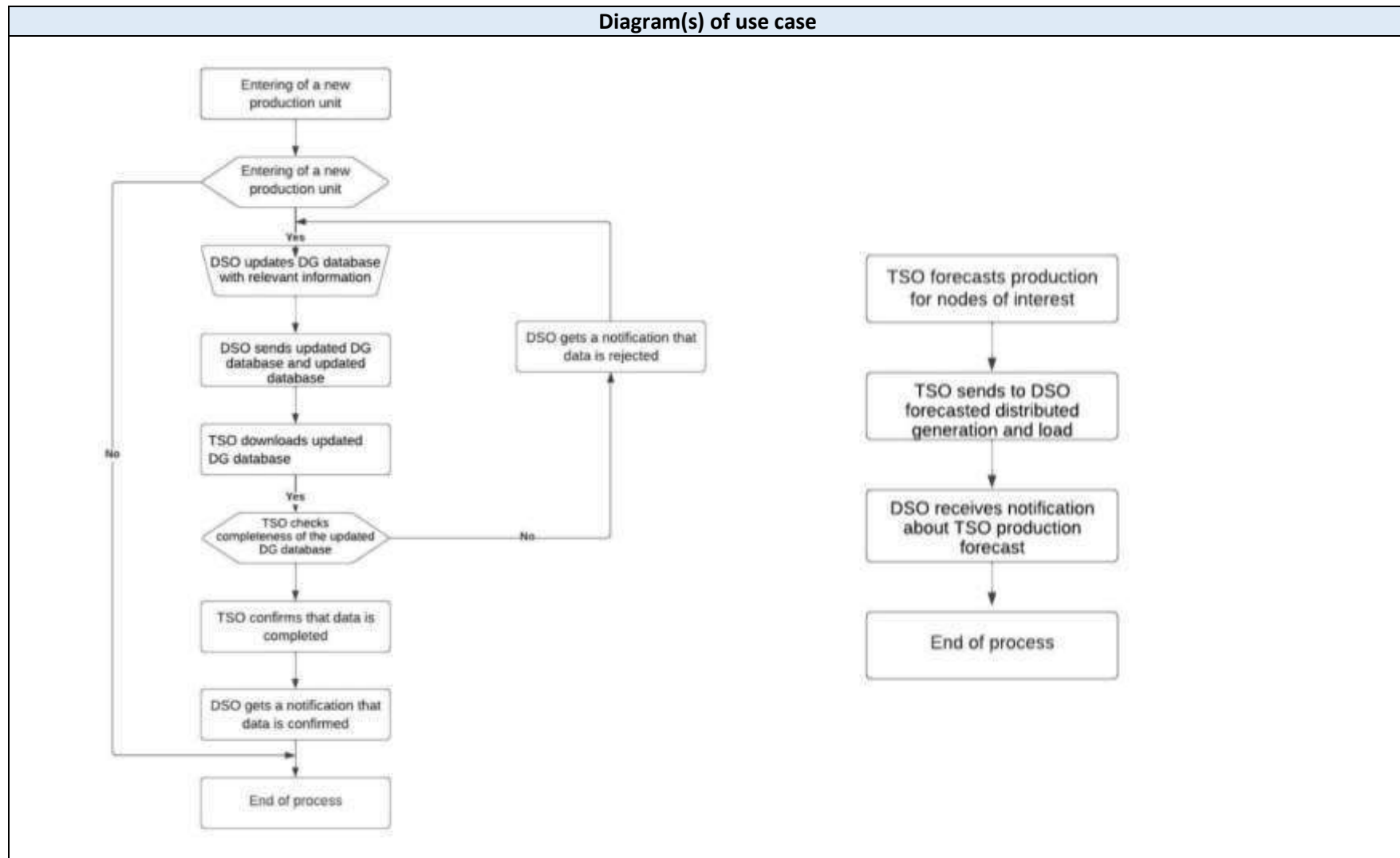
1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None
Level of depth
High level of detail
Prioritisation
The use case is of high priority, because in cases of large integration of RES at the distribution level, it is necessary to establish TSO-DSO coordination in the forecast of consumption and production in order to ensure needed quality of IGMs.
Generic, regional or national relation
Generic.
Nature of the use case
System functional requirements description
Further keywords for classification
IGM, TSO-DSO coordination, RES, distributed generation, forecasting

1.8 General remarks

General remarks
-

2. Diagrams of use case



SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO)	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSO forecasts distributed load and distributed generation forecasting (for each DSO substation connected to the transmission system).
Distribution System Operator (DSO)	System operator	‘Distribution system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	DSO keeps database on distributed generation and corrects TSO’s forecasts of distributed load and distributed generation in accordance with specific operational conditions in the distribution grid.

D2.3 – Requirements and Detailed Architecture Design

Grouping		Group description	
Software/Hardware components		Software/Hardware components used in TSO-DSO cooperation in Individual Grid Model creation	
Actor name	Actor type	Actor description	Further information specific to this use case
TSO-DSO communication platform* / E-mail	Communication platform	A communication platform used for communication between TSO and DSO / A communication method that uses electronic devices to deliver messages across computer networks.	In this use case it is used to exchange information about distributed generation structural data, as well as end load and distribution generation forecasts
Distributed Generation (DG) Database	Database	A database is an organized collection of structured information, or data, stored electronically in a computer system. A database is usually controlled by a database management system (DBMS)	DG database is used to store distributed generation structural data (type, installed power, location...)
Forecasting tool	Software application	An application program is a computer program designed to carry out a forecasting task – making predictions based on past and present data.	Forecasting tool is used to predict end load and distributed generation.

*Optional actor

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1.	Regular updating of distributed generation database	DSO updates distributed generation database with relevant information and sends updated database to TSO via communication platform	DSO	Changes in distributed generation	TSO doesn't have information regarding changes in distributed generation	TSO is informed about changes in distributed generation
2.	TSO-DSO collaboration on end load and distributed generation forecasting	TSO and DSO collaborates in day-ahead process of end load and distributed generation forecasting	TSO	Regular repetition	DSO doesn't have forecast of production units for Day Ahead in nodes of interest	DSO has forecast of production units for Day Ahead in nodes of interest

4.2 Steps – Scenarios

Scenario								
Scenario name:		Regular updating of distributed generation database						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1.	Changes in distributed generation	Distributed generation (DG) database updating	DSO updates DG database with relevant information	Data processing	DSO / operator	DSO / DG Database	1	
2.	DG database updated	DSO sends to TSO updated DG database	DSO sends updated DG database and updated database	Data uploading	DSO / DG Database	TSO / Communication platform or E-mail	1	



D2.3 - Requirements and Detailed Architecture Design

3.	Updated DG database sent by DSO to TSO	TSO receives updated DG database	TSO downloads updated DG database	Data downloading	TSO / Communication platform	TSO / operator	1	
4.	Updated DG database received by TSO	TSO checks updated DG database	TSO checks completeness of the updated DG database	Data processing	TSO / operator	TSO / operator	-	
5.	Updated DG database checked by TSO	TSO notifies DSO on updated DG database completeness	TSO sends to DSO by communication platform confirmation that updated data is complete or incomplete	Notification	TSO / operator	TSO/ Communication platform or E-mail	2	
6.	TSO notified DSO on updated DG database completeness	DSO receives information on updated DG database completeness	DSO receives by communication platform confirmation that updated data is complete or incomplete	Notification	DSO/ Communication platform	DSO/ operator	2	

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		TSO-DSO collaboration on end load and distributed generation forecasting						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1.	Regular repetition	Distributed load and distributed generation forecasting	TSO creates dataset with distributed load and distributed generation forecasting (for each DSO substation connected to the transmission system)	Data processing	TSO / Forecasting tools	TSO / Operator	3	
2.	Distributed load and distributed generation are forecasted	TSO sends to DSO forecasted distributed generation and load data	TSO sends to DSO via communication platform forecasted distributed generation and load data	Data uploading	TSO / Operator	TSO / Communication platform or E-mail	3	
3.	Forecasted distributed generation and load data sent by TSO to DSO	DSO downloads distributed generation and load data sent by TSO	DSO receives notification about TSO production forecast	Data downloading	DSO / Communication platform	DSO / Operator	3	
4.	Distributed generation and load data downloaded by DSO	DSO checks and corrects forecasted distributed generation and load data	DSO checks and corrects forecasted distributed generation and load data if this data does not comply with specific operational conditions in the distribution grid	Data processing	DSO / Operator	DSO / Operator	3	

D2.3 – Requirements and Detailed Architecture Design

5.	Forecasted distributed generation and load data checked (and corrected) by DSO	DSO uploads corrected forecasted distributed generation and load data or notifies TSO that forecast is accepted	DSO uploads corrected forecasted distributed generation and load data or notifies TSO that forecast is accepted	Notification / Data uploading	DSO / Operator	DSO / Communication platform or E-mail	3, 4	
6.	DSO notifies TSO on forecasted distributed generation and load data check	TSO receives information on forecasted distributed generation and load data check	TSO receives information on forecasted distributed generation and load data check – if DSO have corrected this data, forecasting file is attached	Notification	DSO/ Communication platform	TSO/ Operator	3, 4	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Distributed generation data	Distributed generation data consists of: generation type, installed power, geographical location, municipality, DSO substation connected to transmission grid, date of commissioning - all this data side are kept in proper database	
2	Notification on distributed generation database update completeness	TSO sends notification via communication platform to DSO that the distributed generation database update is complete or incomplete	

D2.3 - Requirements and Detailed Architecture Design

3	Forecasted distributed generation and load	Distributed generation and load are forecasted for each DSO substation connected to the transmission system	
4	Notification on forecasted distributed generation and load data check	DSO sends notification to TSO on forecasted distributed generation and load data check	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Individual Grid Model (IGM)	IGM means a data set describing power system characteristics (generation, load and grid topology) and related rules to change these characteristics during capacity calculation, prepared by the responsible TSOs, to be merged with other individual grid model components in order to create the common grid model (EU Regulation 2015/1222)
Distributed generation	Distributed generation, also distributed energy, on-site generation, or district/decentralized energy, is electrical generation and storage performed by a variety of small, grid-connected or distribution system-connected devices referred to as distributed energy resources

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.16 USE CASE 16 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
16	Transmission / Operation, Field	Phasor angles monitoring and prevention of instability

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	22.03.2023	EMSS	-	Preliminary approved
2	20.04.2023	EMSS	Requirements definition	Approved
3	04.10.2023	EMSS	Additional requirements definition	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Stability of system operation
Objective(s)	Monitor phasor angles and if a critical angle is reached apply generation re-dispatching to prevent network instability
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
<p>The possible occurrence of transient instability is monitored through two PMUs, where one is installed in the production centre and the other is installed in the consumption centre. When the critical angle difference is reached, the SCADA or WAMS system activates an alarm, after which the operators in the competent control centre should apply a re-dispatching of the active power injections into the network, which will preserve the stability.</p>
Complete description
<p>Sometimes the fulfilment of security criteria (for instance N-1 criterion) in the operation of the power system does not mean that the stability of the system is ensured. Such events are relatively rare in the European interconnection, but can lead to serious disturbances, such as local blackouts and the occurrence of oscillations between parts of the system connected by links with insufficient transmission capacity.</p> <p>By applying PMUs, it is possible to identify the risk to the stability of the system and act preventively to avoid unwanted consequences. This use-case is based on the identification of possible instability in the part of the system that connects the centre of production with the centre of consumption. The possible occurrence of transient instability is monitored through two PMUs, where one is installed in the production centre and the other is installed in the consumption centre.</p> <p>The greater the active power flow between these two observed points, the greater the angle difference measured by the PMUs which are connected to SCADA or WAMS system. When the critical angle difference is reached, the SCADA or WAMS system activates an alarm, after which the operators in the competent control centre should apply a re-dispatching of the active power injections into the network, until the angle difference falls below the critical value, which will preserve the stability of the system operation. The critical angle is calculated on an off-line application for simulating the dynamic state in the network.</p> <p>This solution can also be applied to other types of disturbances in the stability of system operation, for example when parts of the system are connected by weak interconnections, which in the case of larger flows can lead to oscillations of power flows on transmission lines between these two parts of the system.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
SCADA or WAMS system activates an alarm when the critical angle difference is reached. After alarming, the operators in the competent control centre apply a re-dispatching of the active power injections into the network, until the angle difference falls below the critical value.
Prerequisites
The critical angle is calculated on an off-line application for simulating the dynamic state in the network.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
High level of detail.
Prioritisation
High (4).
Generic, regional or national relation
Generic and national.
Nature of the use case
System functional requirements description.
Further keywords for classification
Power system stability, PMU.

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO)	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSO’s control centre operators monitor angle difference between two PMUs and implement re-dispatching if critical angle is reached.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Hardware/Software components		Hardware/Software components used in OFP business process	
Actor name	Actor type	Actor description	Further information specific to this use case
IRIS (SCADA system)	Control system	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, networked data communications and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plant or machinery.	SCADA system is used to provide real-time active power generation and frequency measurements.
PMU	Measurement device	A device used to measure the magnitude and phase angle of an electrical phasor quantity (such as voltage or current) in the electricity grid using a common time source for synchronization.	PMUs measure voltage phasors in the two observed points and send data to SCADA system via TSO telecommunication system.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Success (basic) scenario	SCADA system monitors the angle difference between the two observed points by PMUs and generates an alarm on the critical angle difference between these points	TSO / IRIS (SCADA system)	Regular repetition	Instability is detected in the power system	Control centre operators are alerted to a critical angle difference between the two observed points
2	Exceptional scenario	SCADA does not receive information from both PMUs	TSO / IRIS (SCADA system)	A lack of adequate measurements of any PMU is detected	SCADA system cannot calculate the angle difference between the two observed points by PMUs	Control centre operators are alerted to a loss of PMU measurements

4.2 Steps – Scenarios

Scenario								
Scenario name:		Success (basic) scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Regular repetition	Regular voltage phasor measurements	SCADA system receives data from PMUs	Data transmission	TSO / PMU	TSO / IRIS (SCADA system)	1	IRI_16
2	Regular repetition	Regular angle monitoring	SCADA system calculates angle difference between the two observed points	Calculation	TSO / IRIS (SCADA system)	TSO / IRIS (SCADA system)	-	IRI_16

D2.3 - Requirements and Detailed Architecture Design

3	Critical angle is calculated	Alarming	SCADA generates an alarm on the critical angle difference between two observed points	Alarming	TSO / IRIS (SCADA system)	TSO / Control Centre operator	2	IRI_16, IRI_30
---	------------------------------	----------	---	----------	---------------------------	-------------------------------	---	----------------

Scenario								
Scenario name:		Exceptional scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	A lack of adequate measurements of any PMU is detected	Unavailability alarming	SCADA detects the lack of adequate measurements of any PMU	Alarming	TSO / IRIS (SCADA system)	TSO / Control Centre operator	3	IRI_16, IRI_31

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	PMU measurements	Voltage phasor data (effective value and angle)	
2	Alarm	Alarm on critical angle difference between two observed points by PMUs	IRI_30
3	Unavailability alarm	Alarm on lack of adequate measurements of any PMU	IRI_31

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Power System stability	Power system stability is defined as the property of a power system that enables it to remain in a state of operating equilibrium under normal operating conditions and to regain an acceptable state of equilibrium after being subjected to a disturbance. Disturbances can be small or large.

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.17 USE CASE 17 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
17	Transmission / Operation	Outage coordination and automated creation of topology files for Individual Network Models

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	15.3.2023	EMSS	-	Preliminary approved
2	06.04.2023	EMSS	UC definition improvement in accordance with recommendations provided by UC auditor.	Approved by auditor
3	24.04.2023	EMSS	Requirements definition	Approved by auditor
4	10.7.2023	EMSS	Further requirement definition	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Improving the quality of IGMs
Objective(s)	When approving works on network elements (outage planning), the topology file needed for Individual Network Model building is automatically created
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
The basic idea of this use-case is to demonstrate the possibility of automating the creation of a topology file when approving works on network elements (outage planning) through the Topology Transfer Application (TTA), which is the subject of this use case. It should be noted here that the topology file is one of the 4 input files used to create the IGM in the CGMES format.
Complete description
<p>A TSO creates every day: 24 DACF models, 24 D2CF models, as well as IDCf models (three times a day at least for the next 8 hours). To create these models, a file defining the topology of the transmission system is manually created.</p> <p>In the coming years, it is planned to further increase the number of models that need to be produced, in the following processes:</p> <ul style="list-style-type: none"> - Hourly IDCf models (for all hours until the end of the day) - For operational purposes, week ahead models will be made every day for all hours seven days in advance, - Daily production of D2CF models for all hours. <p>The goal of this use-case is to devise a way to enter planned outages into the topology file, which includes the following data:</p> <ul style="list-style-type: none"> - Name of elements that are switched off (linking the name of the elements with cimId from the default model), or whose switching state is changed, including the disposition of feeders by busbars and the switching state of coupling bays - Outage period (date/time) - Type of outage (permanent, with daily switching) - Additional outage conditions (if exists, that must be entered precisely). <p>(Note: The tap position of transformers is also part of the topology file, but this use case only applies to changes due to planned works – this excludes tap positions).</p> <p>Creating a topology file from TTA application should include the following activities:</p> <ul style="list-style-type: none"> - Defining the topology when approving the outage request in a convenient format (preferred visualization) - Defining the time in which the planned topology is in effect - Conversion of data from the TTA application in the data format used by the topology file - Input of converted data into all network models (according to the time periods when the topology change is planned) - Connection with the TNA tool for model creation and delivery to OPDE <p>TTA contains a database with information about all elements in the network model with their CIMId and name. The user enters the relevant data for the outages, which are recorded in the database and used to create topological files.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Outages planning and creation of network models is not scope of this use case.
Prerequisites
Access to information of planned outages and having a default topology file.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None
Level of depth
High level of detail
Prioritisation
High. Without automation quality is not satisfactory enough
Generic, regional or national relation
Regional
Nature of the use case
System functional requirements description
Further keywords for classification
Topology, IGM

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO)	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSO operators and software/hardware assets are used in the automated creation of topology files.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Software/Hardware component		Software/Hardware components used in automated creation of topology file	
Actor name	Actor type	Actor description	Further information specific to this use case
Outage planning application	Database software	The application stores information about all planned outages for the next period	Information about changes in the network topology is obtained from this application
EMMA TTA	Application software	EMMA TTA (Topology Transfer Application) is used to automatically create topology files, which is one of the four input files for creating network models	This application was created to achieve the goal of this use case
Grid model server	Server	A software (computer program) or device that provides a service to another computer program and its user, also known as the client. In a data center, the physical computer that a server program runs on is also frequently referred to as a server	Grid model server is used to store topology files and default topology

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Basic scenario	Topology file creation	TSO / EMMA TTA	Completion of outage coordination activities	There is a topology file that is used to create the IGM in which the planned outages in the network can be entered	A topology file is created in accordance with the planned outages in the network
2	Reporting scenario	Display of planned outages for a specific date	TSO / EMMA TTA	Specific date	Information for outages import in data base	Display details of outages for specific date



D2.3 - Requirements and Detailed Architecture Design

4.2 Steps – Scenarios

Scenario								
Scenario name:		Basic scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Outage coordination activities completed	Topology changes data import	Entry of detailed data for planned switching on network elements (network element type, network element designation, period, time and type of switching (off/on), description of switching state change) in the EMMA TTA application	Data import	TSO / Outage planning application	TSO / EMMA TTA	1	EMM_039, EMM_069,
2	Topology changes data imported	Default topology import	Import of the default topology file (no planned outages included) into the EMMA TTA application	Data import	TSO / Grid model server	TSO / EMMA TTA	2	EMM_039
3	Default topology imported	Topology updating	The default topology file is imported into the application when EMMA TTA is started and then updated by the TTA application with topology changes due to scheduled outages.	Calculations	TSO / EMMA TTA	TSO / EMMA TTA		EMM_039, EMM_070

D2.3 - Requirements and Detailed Architecture Design

4	Topology is updated	Exporting of the topology file	Topology file is exported for the selected date on location where other software can import it.	Data export	TSO / EMMA TTA	TSO / Grid model server	3	EMM_039, EMM_071
---	---------------------	--------------------------------	---	-------------	----------------	-------------------------	---	------------------

Scenario								
Scenario name:		Reporting scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Regular repetition	Regular reporting	For a selected date, a report is created on all network elements which topology status differs from the default topology file	Report creation	TSO / TTA	TSO / Grid model server	4	EMM_039, EMM_072

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	List of elements subject to planned outages	The list of network elements that change status with detailed information about the topology changes - period, time and type of switching (off/on)	EMM_073
2	Default network topology file	Information about network topology excluding planned outages (normal network topology for the selected period of the year)	EMM_074

D2.3 - Requirements and Detailed Architecture Design

3	Topology file	A file containing information about the topology of all network elements, which is used in the IGM building process	EMM_075
4	Topology report	The list of all network elements which topology status differs from the default topology	EMM_076
5	Topology changes report	The list of all network elements which topology status differs from the default topology	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Individual Network Model (IGM)	A data set describing power system characteristics (generation, load and network topology) and related rules to change these characteristics during capacity calculation and coordinated regional security assessment processes, prepared by the responsible TSOs, to be merged with other individual network model components in order to create the common network model (EU regulation 2015/1222)
Common Network Model (CGM)	Common Network Model means a Union-wide data set agreed between various TSOs describing the main characteristic of the power system (generation, loads and network topology) and rules for changing these characteristics during the capacity calculation process(EU regulation 2015/1222)
CGMES	The CGMES (Common Network Model Exchange Specification) is an IEC technical specification (TS 61970-600-1, TS 61970-600-2) based on the IEC CIM (Common Information Model) family of standards. It was developed to meet necessary requirements for TSO data exchanges in the areas of system development and system operation.



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.18 USE CASE 18 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
18	Transmission / Operation	Optimization of PMU installation points

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	03.04.2023	EMSS		Preliminary approved
2	26.04.2023	EMSS	Requirement definition	Approved
3	23.10.2023	EMSS	Additional requirement definition	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Power system observability
Objective(s)	Determination of buses for optimal PMU placement for full topological observability
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
The optimization of PMU installation points means the determination of the minimum number of buses in the system (substations, power facilities etc.) where PMU devices need to be installed in order for the given power system to be fully observable.
Complete description
<p>Synchrophasor technology enables the synchronization of measurements at different geographical locations in the power system, with the usage of time tags assigned to each particular measurement. Furthermore, these measurements are collected, controlled and processed by a PDC (Phasor Data Concentrator) to form a coherent picture of the power system. Such synchronized measurements can be included to the state estimator, which serves as the main basis for the entire spectrum of applications important in operational work in control centres. State estimator based solely on PMU measurements is impractical primarily due to installation costs and historical long-term investments in the SCADA/EMS system, which has been the undisputed "ruler" of state estimation for decades. A much more realistic approach would be to use existing SCADA/EMS measurements and PMU measurements to improve the quality of the state estimation.</p> <p>The optimization of PMU installation points means the determination of the minimum number of buses in the system (substations, power facilities etc.) where PMU devices need to be installed in order for the given power system to be fully observable.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

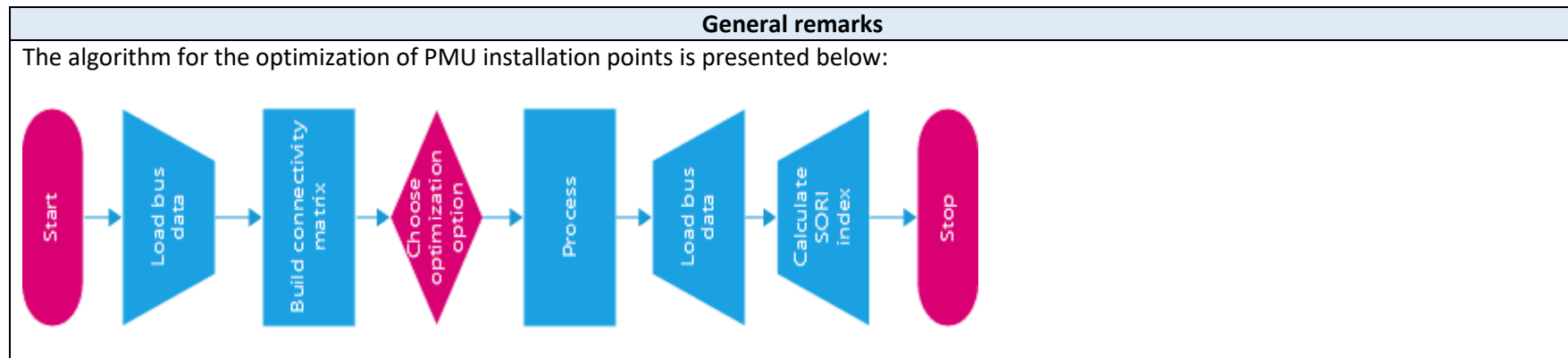
1.6 Use case conditions

Use case conditions
Assumptions
This use case does not address the full numerical observability of the power system with PMU devices.
Prerequisites
Binary connectivity matrix has to be given.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
High level of detail.
Prioritisation
High (4). This mechanism does not currently exists in the Serbian pilot site and it will improve the power system observability and estimation quality.
Generic, regional or national relation
Generic
Nature of the use case
System functional requirements description.
Further keywords for classification
PMU, observability, estimation, optimization

1.8 General remarks



2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
TSO	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	A TSO is obliged to guarantee the secure operation of the transmission system. In real-time operation, security is monitored by the SCADA/EMS application which relays on the state estimator. To obtain better state estimation quality, it is preferable to install PMUs to obtain full phasors observability.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Hardware components		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
IRIS OPP (Optimal PMU Placement) Application	Software Application	An application program is a computer program designed to carry out a specific task other than one relating to the operation of the computer itself, typically to be used by end-users.	IRIS OPP is a software application for optimization of PMU installation points in the transmission network.
Server	Server	A server is a computer program or device that provides a service to another computer program and its user, also known as the client	A server is used to store solutions and reports

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Success (basic) scenario	Determination of buses for PMU installation	TSO / IRIS OPP	Upon request	Optimal PMU installation points are not known.	Optimal PMU installation points are defined.

4.2 Steps – Scenarios

Scenario								
Scenario name:								
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Upon request	Creating connectivity matrix	Operator enters bus data in the OPP application to create connectivity matrix	Data processing	TSO / Operator	TSO / IRIS OPP Application	1	IRI_022, IRI_032
2	Connectivity matrix is built	Formulate the optimization problem	Operator chooses one of the given optimization options	Data entry	TSO / Operator	TSO / IRIS OPP Application	2	IRI_022, IRI_033
3 (optional)	Optimization option 'with already installed PMUs' is selected	Entering already installed PMUs	Operator enters buses with already installed PMUs	Data entry	TSO / Operator	TSO / IRIS OPP Application	3	IRI_022, IRI_034
4	Optimization option is selected	Apply optimization algorithm	Getting optimal installation points	Calculating	TSO / IRIS OPP Application	TSO / Server	4, 5, 6	IRI_022, IRI_035, IRI_036, IRI_037

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Binary connectivity matrix	The binary connectivity matrix represents connections (branches) between every two nodes in the grid	IRI_032
2	Optimization options	Optimization process can be: basic, N-1, with already installed PMUs	IRI_033
3	Already installed PMUs	Buses with already installed PMUs	IRI_034

D2.3 – Requirements and Detailed Architecture Design

4	Optimal solutions	Optimal solution is any solution with minimal number of PMUs according to set optimization options	IRI_035
5	SORI number	A number calculated to describe the quality of optimization (see KPIs)	IRI_036
6	Calculation report	Calculation report contains all relevant data such as: number of needed PMUs, positions for optimal PMU installation, SORI...	IRI_037

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Phasor measurement unit (PMU)	A phasor measurement unit is a device used to estimate the magnitude and phase angle of an electrical phasor quantity in the electricity grid using a common time source for synchronization.

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.19 USE CASE 19 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
19	Transmission / Enterprise, Operation, Field	Emergency & Restoration - System Split module (upgrade)

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	23.03.2023	EMSS		Preliminary Approved
2	20.04.2023	EMSS	Requirements definition	Preliminary Approved
3	28.04.2023	SCC	UC revision – combined review by IMP and SCC	Approved
4	01.08.2023	EMSS	Further requirements specification	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Emergency & Restoration system operation
Objective(s)	Create a toolset for efficient regional coordination of several TSOs by RCC in case of system split
Related business case(s)	BC1, BC4

1.4 Narrative of use case

Narrative of use case
Short description
The Emergency & Restoration - System Split module shall be used to detect system split and coordinate TSOs and RCC during system stabilization and reconnection.
Complete description
<p>ENTSO-E rules determine procedures in case of major disturbances (Continental Europe Synchronous Area Framework Agreement - Emergency & Restoration Policy rules). However, their implementation during disturbances is difficult, as there are many complex rules. ENTSO-E disturbance analysis following separation of the Continental Europe power system on 8.1.2020 shows that almost no TSO acted strictly according to these rules, although the general training of the dispatchers enabled good improvisation and effective removal of this disturbance. In addition, new European regulation 2019/943 envisages responsibility for Regional Control Centres (RCCs) in the event of major disturbances, such as:</p> <ul style="list-style-type: none"> • Supporting the coordination and optimization of regional restoration as requested by transmission system operator; • Carrying out post-operation and post-disturbances analysis and reporting; • Carrying out tasks related to the identification of regional electricity crisis scenarios. <p>Mentioned RCC tasks are in different stages of methodology development and at this point it is not fully clear what role RCCs will have in it and when these RCC services will be provided to TSOs.</p> <p>To make it easier for dispatchers to apply the Emergency & Restoration (ER) rules and to give the RCC an appropriate role in coordinating major disturbances, a use case developed in the TRINITY project provided for the following:</p> <ul style="list-style-type: none"> • Detection of major disturbances and their characteristics (system split, system blackout, frequency deviation) • Communication and coordination tool that guides TSO operators through a step-by-step ER process while allowing a RCC to oversee and steer the entire process. <p>The results of the TRINITY project have been communicated to the ENTSO-E and they have been used to create a procedure in case of system split. The purpose of this use case is to align the communication procedure in the TRINITY coordination tool with the mentioned ENTSO-E procedure and to further test and improve this coordination process. In addition, the necessary algorithms for the entire implementation of the ENTSO-E procedure will be designed.</p> <p>To facilitate implementation of ENTSO-E ER procedure in a real environment as well as to allow for its testing and further enhancements, the ER module developed in TRINITY project and deployed within SCC infrastructure will be updated and complemented with a real-time data acquisition system and a historical database. Owing to its experience and know-how from the implementation of back-up SCADA system in the Serbian TSO (EMS), IMP will deliver and deploy an instance of the SCADA system in SCC. Moreover, given that IMP developed the initial version of the ER</p>

D2.3 – Requirements and Detailed Architecture Design

module in TRINITY project, it will also establish suitable interfaces (APIs) between the ER module and future SCADA system as well as external telemetry providers (use of IEC 60870-6-505 TASE.2 is planned). In addition, IMP will perform all the necessary customizations of the ER tool and the underlying application database to store appropriately real-time data acquired by the SCADA system as well as to allow manual input and intervention in case of missing data.

The proposed ER module enhancement with SCADA system will also include modules for visual presentation of the acquired real-time data as well as the outputs from the ER module inferencing. Finally, IMP will provide the necessary technical documentation as well as operational training for the SCC personnel to ensure successful exploitation of the ER tool during and beyond the R2D2 project.

With the implementation of mentioned SCADA system, ER module will have a possibility to inform in real-time TSO dispatchers and RCC operators about ongoing power system crisis. Moreover, the ER module will be implemented and validated in real conditions (not in study mode as done in TRINITY project), by improving methodologies and algorithms for frequency leader and frequency islands determination, and by introducing more complex coordination problems thus further improving business process for emergency and restoration. The ER tool will now also have a suitable SCADA interface to visualize frequency deviation/islanding/black-out events as well as to verify the output from the decision support tool.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
All TSOs are equipped with SCADA system, EAS system and voice communication system.
Prerequisites
The working station of the Emergency & Restoration - System Split module is installed in RCC control rooms and TSOs' national control centre of West Balkan region.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
High level of detail.
Prioritisation
High (4). The Emergency & Restoration - System Split module will improve the ability of RCC and TSOs to coordinate their activities during a system split.
Generic, regional or national relation
Regional.
Nature of the use case
System functional requirements description.
Further keywords for classification
Emergency operation, System split, Regional coordination.

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO)	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSOs perform actions to remedy operating parameters after a system split and to reconnect the system.
Regional coordination centre (RCC)	Regional coordination body	‘Regional coordination centre’ means regional coordination centre established pursuant to Article 35 of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity	RCC helps with regional inter-TSO coordination during a system split.
System Area Monitor (SAM)	Transmission System Operator	TSO selected to monitor and coordinate certain activities according to the ENTSO-E Regional Group Continental Europe ‘Procedure in case of system separation and resynchronisation of separated grid areas’	

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Software/Hardware components		Software/Hardware components of the Emergency & Restoration - System Split module	
Actor name	Actor type	Actor description	Further information specific to this use case
Emergency & Restoration - System Split module (ER-SSM)	Control system	Emergency & Restoration - System Split module will be designed to detect system split and to assist Control Centre operators in system stabilisation after split and resynchronisation.	ER-SMM is used primarily as a communication tool in case of system split, but activation of ER process will be performed based on real time data provided from deployed SCADA system. Additionally, using mentioned SCADA system, it can help to identify directly affected TSOs, Frequency Leader and Resynchronisation Leader.
Conference call device	Voice communication device	A conference call device is a device through which a telephone call involving multiple participants can be arranged. These conference bridges act as virtual rooms that allow several people to host or join meetings.	The conference call device is used for steps where the SAM is involved and for extraordinary steps when discussion between the affected TSOs is required.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Success (basic) scenario	RCC coordinates TSOs in the region to reconnect the system after a system split	RCC / Emergency & Restoration - System Split module (ER-SSM)	System split is detected	There is a system split, operating parameters may be out of predefined ranges	System is reconnected, operating parameters are within predefined ranges
2	Extraordinary scenario	Conference call is launched in case any actor disagrees with identification of directly affected TSOs, Frequency Leader and Resynchronisation Leader, or any actor do not provide requested confirmation	RCC / Emergency & Restoration - System Split module (ER-SSM)	Confirmation is rejected	Confirmation in any step of basic scenario is rejected, or there is any other problem in basic scenario execution	Objections raised or problems arisen are solved

4.2 Steps – Scenarios

Scenario								
Scenario name:		Success (basic) scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	System split is detected	System split detection - WARNING	ER-SSM, on the ground of topology and frequency information provided from SCADA system, detects system split	Identification Warning	RCC / ER-SSM	TSO / ER-SSM	1	IRI_18, IRI_38, IRI_39, IRI_40, IRI_41, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_52, IRI_53

D2.3 - Requirements and Detailed Architecture Design

2	System split warning is activated	System split detection - CONFIRMATION	All TSOs in the region acknowledge system split detection (by using data of ER-SSM, SCADA system, WAMS system and EAS)	Confirmation	TSO / ER-SSM	RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_53
3	System split detection is confirmed	Directly affected TSOs – IDENTIFICATION	ER-SSM displays all directly affected TSOs in the region (bordering the system separation line)	Identification	RCC / ER-SSM	TSO / ER-SSM	3	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_54
4	Directly affected TSOs are identified	Directly affected TSOs - CONFIRMATION	All relevant TSOs in the region confirm that they are directly affected	Confirmation	TSO / ER-SSM	RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_54
5	Directly affected TSOs are confirmed	Frequency Deviation Management before Frequency Leader nomination – WARNING	RCC sends warning to all TSOs in the region to: 1) Switch Frequency Restoration Controllers to Frozen Control Mode and 2) Manually or automatically speed up the stabilization of the system by over-riding Frozen Control Mode if appropriate. 3) Adjust system state on EAS according to transmission system conditions	Warning	RCC / ER-SSM	TSO / ER-SSM	4, 10	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_55, IRI_56

D2.3 - Requirements and Detailed Architecture Design

6	Frequency Deviation Management before Frequency Leader nomination warning is activated	Frequency Deviation Management before Frequency Leader nomination – CONFIRMATION	All TSOs in the region confirm that they have 1) Switched Frequency Restoration Controllers to Frozen Control Mode and 2) Speeded up manually or automatically the stabilization of the system by over-riding Frozen Control Mode 3) Adjusted system state on EAS	Confirmation	TSO / ER-SSM	RCC / ER-SSM	2, 10	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_55, IRI_56
7	Actions regarding Frequency Deviation Management before Frequency Leader nomination are confirmed	Frequency Leader – DEFAULT DETERMINATION	EM-SSM determines for each subsystem which TSO in the region should act as Frequency Leader for each subsystem	Calculation	RCC / ER-SSM	RCC / ER-SSM	-	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_50, IRI_51, IRI_57
8	Default Frequency Leader is determined	Frequency Leader – NOMINATION	RCC sends to all TSOs in the region proposal for Frequency Leader nomination for each subsystem	Identification	RCC / ER-SSM	TSO / ER-SSM	5	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_57
9	Frequency Leader is nominated	Frequency Leader – CONFIRMATION	All TSOs in the region confirm proposal for Frequency Leader nomination for each subsystem	Confirmation	TSO / ER-SSM	RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_57

D2.3 - Requirements and Detailed Architecture Design

10	Frequency Leader is confirmed	Frequency Deviation Management after Frequency Leader nomination (aFRP) – WARNING	RCC sends warning to all TSOs in the region to: 1) Switch/keep Frequency Restoration Controller to Frozen Control Mode if TSO is not Frequency Leader 2) Switch Frequency Restoration Controller to Frequency Control Mode if TSO is Frequency Leader. 3) Additionally, to announce its status as Frequency Leader on EAS.	Warning	RCC / ER-SSM	TSO / ER-SSM	5	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_58
11	Frequency Deviation Management after Frequency Leader nomination aFRP warning is activated	Frequency Deviation Management after Frequency Leader nomination (aFRP) – CONFIRMATION	All TSOs in the region confirm that they have: 1) Switched / kept Frequency Restoration Controllers to Frozen Control Mode (if TSO is not Frequency Leader) 2) Switched Frequency Restoration Controllers to Frequency Control Mode (if TSO is Frequency Leader) 3) Announced on EAS its Frequency Leader status, if necessary	Confirmation	TSO / ER-SSM	RCC / ER-SSM	2, 10	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_58

D2.3 - Requirements and Detailed Architecture Design

12	Actions regarding Frequency Deviation Management after Frequency Leader nomination are confirmed	Frequency Deviation Management after Frequency Leader nomination (mFRP & RP) – WARNING	RCC sends warning to all TSOs in the region, with the exception of the frequency leader, to suspend the manual activation of frequency restoration reserves and replacement reserves activation (i.e manual frequency restoration process – mFRP and replacement process – RP).	Warning	RCC / ER-SSM	TSO / ER-SSM	6	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_59
13	Frequency Deviation Management after Frequency Leader nomination mFRP & RP warning is activated	Frequency Deviation Management after Frequency Leader nomination (mFRP & RP) – CONFIRMATION	All TSOs in the region, with the exception of the frequency leader, confirm that they have suspended the manual activation of frequency restoration reserves and replacement reserves activation	Confirmation	TSO / ER-SSM	RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_59
14	mFRP & RP suspension is confirmed	Resynchronization Leader determination – TELECONFERENCE WITH SYNCHRONOUS AREA MONITOR (SAM)	SAM starts a telephone conference with the directly affected TSOs, RCCs and nominated frequency leaders to determine resynchronization leader.	Identification	SAM, RCC, TSOs / Conference call device	SAM, RCC, TSOs / Conference call device	7	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_50, IRI_51, IRI_60, IRI_61
15	Resynchronization Leader is selected	Resynchronization Leader – INFORMATION	RCC informs all TSOs in the region (not directly affected) on selected Resynchronization Leader	Identification	RCC / ER-SSM	TSO / ER-SSM	7	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_60, IRI_61

D2.3 - Requirements and Detailed Architecture Design

16	Information on Resynchronization Leader is communicated to all TSOs	Resynchronization Leader – CONFIRMATION	All TSOs in the region (not directly affected) confirms that they have acknowledged information on selected Resynchronization Leader	Confirmation	TSO / ER-SSM	RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_60, IRI_61
17	Reception of information on Resynchronization Leader is confirmed	Resynchronization Leader announcement on EAS - WARNING	RCC informs the Resynchronization Leader (if this TSO is in the region) to announce its status on EAS.	Warning	RCC / ER-SSM	TSO / ER-SSM	10	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_62
18	Warning on Resynchronization Leader announcement on EAS is activated	Resynchronization Leader announcement on EAS - CONFIRMATION	Resynchronization Leader confirms that Resynchronization Leader announcement on EAS is communicated	Confirmation	TSO (Resynchronization Leader) / ER-SSM	RCC / ER-SSM	10	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_62
19	Resynchronization Leader announcement on EAS is confirmed	Upcoming resynchronisation – WARNING	Before resynchronization, the Frequency Leader of the region warns RCC and all TSOs in the region about upcoming resynchronization	Warning	TSO / ER-SSM	TSO, RCC / ER-SSM	8	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_63
20	Warning on upcoming resynchronisation is activated	Upcoming resynchronisation – CONFIRMATION	All TSOs in the region (except Frequency Leader) and RCC confirms that they have acknowledged information on upcoming resynchronization	Confirmation	TSO, RCC / ER-SSM	TSO, RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_63

D2.3 - Requirements and Detailed Architecture Design

21	Warning on upcoming resynchronisation is confirmed	Executed resynchronisation – WARNING	After resynchronization, Frequency Leader of the region warns RCC and all TSOs in the region about executed resynchronization	Warning	TSO / ER-SSM	TSO, RCC / ER-SSM	9	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_64
22	Warning on executed resynchronisation is activated	Executed resynchronisation – CONFIRMATION	All TSOs in the region and RCC confirms that they have acknowledged information on executed resynchronization	Confirmation	TSO, RCC / ER-SSM	TSO, RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_64
23	Warning on executed resynchronisation is confirmed	Resynchronization Leader status on EAS – WARNING	RCC warns the Resynchronization Leader (if this TSO is in the region) to deactivate its status as Resynchronization Leader on EAS	Warning	RCC / ER-SSM	TSO (Resynchronization Leader) / ER-SSM	10	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_65
24	Warning on Resynchronization Leader status on EAS is activated	Resynchronization Leader status on EAS – CONFIRMATION	Resynchronization Leader confirms that he has deactivated Resynchronization Leader status on EAS	Confirmation	TSO (Resynchronization Leader) / ER-SSM	RCC, TSO / ER-SSM	10	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_65
25	Resynchronization Leader confirmed that he has deactivated Resynchronization Leader status on EAS	Frequency leader after resynchronisation – NOMINATION	Frequency Leaders of reconnected areas decide who should be the Frequency Leader after resynchronisation	Identification	TSO / Conference call device	TSO / Conference call device	5	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_50, IRI_51, IRI_66, IRI_67
26	Frequency leader after resynchronisation is nominated	Frequency leader after resynchronisation – INFORMATION	Frequency leader of the region informs RCC and all other TSOs in the region about selected Frequency Leader after resynchronisation	Identification	TSO / ER-SSM	TSO, RCC / ER-SSM	5	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_66, IRI_67

D2.3 - Requirements and Detailed Architecture Design

27	Information on selected Frequency leader after resynchronisation is distributed to RCC and TSOs	Frequency leader after resynchronisation – CONFIRMATION	All TSOs in the region and RCC confirms that they have acknowledged information on selected Frequency leader after resynchronisation	Confirmation	TSO, RCC / ER-SSM	TSO, RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_66, IRI_67
28	Frequency leader after resynchronisation is confirmed	Frequency Leader deactivation status on EAS – WARNING	RCC warns Frequency Leader to confirm or to deactivate its Frequency Leader status on EAS	Warning	RCC / ER-SSM	TSO (Frequency Leader) / ER-SSM	10	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_68, IRI_69
29	Frequency Leader deactivation status on EAS warning is activated	Frequency Leader deactivation status on EAS – CONFIRMATION	Frequency Leader confirms or deactivates its Frequency Leader status on EAS	Confirmation	TSO (Frequency Leader) / ER-SSM	RCC, TSO / ER-SSM	10	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_68, IRI_69
30	Frequency Leader confirmed or deactivated its Frequency Leader status on EAS	Frequency Deviation Management after Resynchronisation – WARNING	RCC sends warning to all TSOs in the region to switch Frequency Restoration Controller to: 1) Frozen Control Mode (for those TSOs which are not Frequency Leader) 2) Frequency Control Mode (if TSO is Frequency Leader after resynchronization)	Warning	RCC / ER-SSM	TSO / ER-SSM	4	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_70

D2.3 - Requirements and Detailed Architecture Design

31	Warning on Frequency Deviation Management after Resynchronisation is activated	Frequency Deviation Management after Resynchronisation – CONFIRMATION	TSOs confirm that they have switched Frequency Restoration Controller to: 1) Frozen Control Mode (for those TSOs which are not Frequency Leaders anymore) 2) Frequency Control Mode (if TSO is Frequency Leader after resynchronization)	Confirmation	TSO / ER-SSM	RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_70
32	Warning on Frequency Deviation Management after Resynchronisation is confirmed	Return of the Frequency Restoration Controller to Normal Operation Mode – WARNING	Frequency Leader (after resynchronisation and system stabilization) informs RCC that other TSOs should switch Frequency Restoration Controllers to Normal Operation Mode	Warning	TSO / ER-SSM or Conference call device (if Frequency Leader does not belong to the region coordinated by the RCC)	RCC / ER-SSM or Conference call device (if Frequency Leader does not belong to the region coordinated by the RCC)	4	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_71
33	Warning on return of the Frequency Restoration Controller to Normal Operation Mode is passed to RCC	Return of the Frequency Restoration Controller to Normal Operation Mode – CONFIRMATION (this step is executed if the Frequency Leader does not belong to the region coordinated by the RCC)	RCC confirms that Frequency Restoration Controllers should be switch to Normal Operation Mode by all others TSOs	Confirmation	RCC / Conference call device	TSO / Conference call device	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_71

D2.3 – Requirements and Detailed Architecture Design

34	Warning on return of the Frequency Restoration Controller to Normal Operation Mode is confirmed by RCC	Return of the Frequency Restoration Controller to Normal Operation Mode – WARNING (this step is executed if the Frequency Leader does not belong to the region coordinated by the RCC)	RCC warns all TSOs in the region (except Frequency Leader) to switch Frequency Restoration Controllers to Normal Operation Mode and to change their status on EAS, if appropriate.	Warning	RCC / ER-SSM	TSO / ER-SSM	4	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_72, IRI_73
35	Warning on return of the Frequency Restoration Controller to Normal Operation Mode is passed to TSOs	Return of the Frequency Restoration Controller to Normal Operation Mode – CONFIRMATION	All TSOs in the region (except Frequency Leader) confirm that they have switched Frequency Restoration Controllers to Normal Operation Mode	Confirmation	TSO/ ER-SSM	RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_50, IRI_51, IRI_72, IRI_73

D2.3 – Requirements and Detailed Architecture Design

36	All TSOs (except Frequency Leader) have switched Frequency Restoration Controllers to Normal Operation Mode	Return of the Frequency Restoration Controller to Normal Operation Mode by the Frequency Leader – WARNING (this step is executed if the Frequency Leader belongs to the region coordinated by the RCC)	RCC sends warning to the Frequency Leader to switch Frequency Restoration Controllers to Normal Operation Mode, to deactivate the Frequency leader status on EAS and return the system state to Normal (green).	Warning	RCC / ER-SSM	TSO/ ER-SSM	4	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_48, IRI_50, IRI_51, IRI_74, IRI_75
37	RCC warned the Frequency Leader to switch Frequency Restoration Controllers to Normal Operation Mode	Return of the Frequency Restoration Controller to Normal Operation Mode – Frequency Leader CONFIRMATION (this step is executed if the Frequency Leader belongs to the region coordinated by the RCC)	Frequency Leader confirms that Frequency Restoration Controller is switched to Normal Operation Mode and Frequency leader status on EAS has been deactivated.	Confirmation	TSO/ ER-SSM	RCC / ER-SSM	2	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45, IRI_46, IRI_47, IRI_51, IRI_74, IRI_75

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Extraordinary scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Any confirmation is rejected by any actor, any problem prevents basic scenario to be executed	Dispute or problem solving – CONFERENCE CALL	RCC opens teleconference with all TSOs to resolve dispute or problem	Conference call	RCC, TSO/ ER-SSM	RCC, TSO/ ER-SSM	24 (solution of a raised objection or arisen problem)	IRI_18, IRI_38, IRI_39, IRI_40, IRI_42, IRI_43, IRI_44, IRI_45

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	System split warning	Warning to TSOs and RCC that system split has been detected	IRI_41
2	Confirmation	Confirmation that the actor has accepted (and performed) the current step of the System Split procedure	IRI_46, IRI_47
3	Directly affected TSOs identification	List of TSOs considered directly affected	
4	Warning on required Frequency Restoration Controllers Mode	Warning to all TSOs to reset Frequency Restoration Controllers to the required operating mode	
5	Frequency Leader nomination	Name of the TSO nominated to act as Frequency Leader	
6	Warning on suspension of mFRP & RP	Warning to all TSOs to suspend mFRP & RP	
7	Resynchronization Leader nomination	Name of the TSO nominated to act as Resynchronization Leader	

D2.3 - Requirements and Detailed Architecture Design

8	Information on upcoming resynchronization	Information on upcoming resynchronization to all TSOs	
9	Information on executed resynchronization	Information on executed resynchronization to all TSOs	
10	Warnings related to EAS communication		

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Frequency leader	TSO appointed and responsible for managing the system frequency within a synchronised region or a synchronous area in order to restore system frequency back to the nominal frequency (Commission regulation (EU) 2017/2196 establishing a network code on electricity emergency and restoration).
Resynchronisation leader	TSO appointed and responsible for the resynchronisation of two synchronised regions (Commission regulation (EU) 2017/2196 establishing a network code on electricity emergency and restoration).
Resynchronisation	Synchronising and connecting again two synchronised regions (Commission regulation (EU) 2017/2196 establishing a network code on electricity emergency and restoration).
Frequency restoration process (FRP)	Process that aims at restoring frequency to the nominal frequency and, for synchronous areas consisting of more than one LFC area, a process that aims at restoring the power balance to the scheduled value (Commission regulation (EU) 2017/1485 establishing a guideline on electricity transmission system operation). This process can be automatic (aFRP) and manual (mFRP).
System split	Splitting of a single interconnection (synchronous area) into two or more separate synchronised regions due to a disturbance.



D2.3 - Requirements and Detailed Architecture Design

Directly affected TSOs	TSOs whose parts of the Control Area are located in different synchronized regions after the system split, or whose interconnecting line to another control area of the same synchronous area, is out of service and separates the two synchronized regions.
Frequency Restoration Controller	Device installed on the generator module that performs FRP.

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.20 USE CASE 20 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
20	Transmission, Distribution / Enterprise, Operation, Station, Field, Process	Physical security enhancement in core network components (Primary HV/MV Substations and Secondary MV/LV substations)

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	11/03/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos		
0.2	28/03/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis	Minor corrections/improvements in scenario descriptions	
0.3	30/03/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis	Updates/corrections in scenarios description	
0.4	24/04/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis	Minor corrections	
0.5	03/05/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis	Correcctions after 1 st revision by EMSS	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	<p>The purpose of this Use Case is the enhancement of physical substation security through the installation of visual surveillance and metering equipment, in order to prevent possible damage to substation infrastructure. On the one hand, this UC aims at the instant notification of the network operator through image signals or alerts, in case of a possible vandalism/theft attack. Furthermore, through this UC, a quicker notification and faster response measures by the DSO can be achieved, in the event of a physical phenomenon, which may affect one or multiple substations' infrastructure. The scope of the UC is linked with both primary and secondary substations physical security:</p> <ul style="list-style-type: none"> • Primary substations (HV/MV transformers): Through the installation of equipment, such as surveillance cameras, protection against vandalism attacks can be achieved, as the operator has visual surveillance over the HV/MV substation. Furthermore, in the case of a possible physical event (e.g. fire or flood) in the area inside or near the HV/MV substation, the surveillance equipment can contribute to faster restoration actions by the DSO. In that way, the mitigation of possible damage to the substation infrastructure or even outages can be achieved. • Secondary substations (MV/LV transformers): In this UC, the installation of sensor devices (e.g. metering equipment) to MV/LV substations could lead to alarms and notifications to the network operator in case of possible vandalism and theft attacks in the transformers. Moreover, a natural event could affect several MV/LV transformers in a specific location of the network, while an outage to many consumers may occur. In case of alarms to the DSO through the proposed devices of this UC, the exact location of the damage in the infrastructure can be instantly known and the necessary actions can follow for a faster power restoration.
Objective(s)	Prevention or mitigation of potential infrastructure loss, equipment damage, outage or even a cascading effect
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
<p>This Use Case focuses on physical substation security enhancement through the installation of equipment on either HV/MV or MV/LV substations. In case of a vandalism/theft attack to primary or secondary substation infrastructure, the DSO could be instantly notified by surveillance or metering equipment and proceed to the necessary actions. Moreover, in the event of a physical phenomenon or a natural disaster, which may affect the primary or secondary substation infrastructure, the installation of the aforementioned equipment could lead to the faster mitigation of possible damage to critical substation components, as well as to quicker power restoration.</p>
Complete description
<p>Physical substations security is a critical aspect for the distribution network with expanding impact on the end-users, the power system and the market, considering the increased RES penetration on distribution network and their participation to the market. Thus, a physical event or a vandalism attack on a HV/MV substation especially when there is significant amount of RES power installed could affect numerous consumers, affect the electricity transmission system and even cause market deregulation up to an extent.</p> <p>This UC focuses firstly on physical HV/MV substation security enhancement, through the installation of equipment, such as surveillance cameras. On the one hand, protection against physical phenomena, that could cause a serious damage to a HV/MV substation, is considered of major importance. Lack of instant notification to the operator, in case of an incident, such as a fire inside or in the area near the HV/MV substation, could lead to a serious impact on the network. Serious damage to equipment inside the substation could occur, leading to loss of power supply to the main MV feeders. Thus, through surveillance cameras installation, the transmission of instant alarms to the network operator would lead to the mitigation or even the avoidance of the aforementioned consequences.</p> <p>On the other hand, surveillance equipment could also lead to the prevention and mitigation of possible vandalism/theft attacks to a HV/MV substation, as the operator could proceed faster to all the necessary actions, in order to avoid any possible consequences.</p> <p>MV/LV overhead substations are vulnerable to vandalism and theft due to the illegal trade of copper, which is included in the transformer's coils and is of value. This UC aims at the mitigation and prevention of such events through the installation of sensors on MV/LV substations, like metering devices or accelerometers. In case of a vandalism or theft attack to one MV/LV substation, the sensor device would provide an alert signal to the DSO, so that the latter can be notified for the incident and proceed to the necessary actions. As a result, a possible power loss problem to a group of loads fed by the specific substation could be restored in a faster way.</p> <p>Furthermore, through the installation of sensors to MV/LV substations, a faster restoration to possible damages by a local physical event could be achieved. The loss of a MV/LV substation due to a natural event would lead either to zero value voltage indications from a metering device, or to an alert signal from a sensor device.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Local authorities (police, or other national mechanisms) may need to intervene for actions beyond the context of this UC (e.g. after a vandalism/attack the local authorities must be notified by the DSO personnel to intervene to the incident area).
Prerequisites
Surveillance cameras installed in the perimeter of the HV/MV substation
Sensor devices installed to MV/LV substations

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
12
Level of depth
High
Prioritisation
5
Generic, regional or national relation
Regionally, nationally – will be applied to the GR demo site and HEDNO is also interested in replicability – scalability of physical substation enhancement solutions in several regions of the country
Nature of the use case
Description of a process for the enhancement of physical substation security (in case of vandalism/theft attack, or physical incidents)
Further keywords for classification
Visual surveillance equipment, sensors, HV/MV substations physical security, MV/LV substations physical security

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	System operator	‘Distribution system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU).	The DSO is responsible for the physical security of its infrastructure. When receiving a signal or an alert from the installed equipment in case either of a vandalism/theft attack or of physical event (e.g. fire), the responsible local authorities must be notified. Then the available workforce personnel of the DSO must be sent to the incident site for power restoration.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
R2D2 actors		Tools to be developed as part of R2D2 products	
Actor name	Actor type	Actor description	Further information specific to this use case
EMMA ARGOS	AI image-based maintenance EMMA module	EMMA module, to be utilized for Image AI processing	AI image-based maintenance EMMA module triggers the appropriate process to analyze the set of images and data for identifying electrical anomalies. Data is processed and details of potential problems are obtained.

Grouping		Group description	
HW/SW actors		Hardware/Software components, either existent, or to be procured through R2D2 Project, used for surveillance/monitoring	
Actor name	Actor type	Actor description	Further information specific to this use case
Surveillance cameras	Surveillance equipment device	Surveillance cameras installed on primary substation	Surveillance cameras will provide the network operator with the ability to be instantly notified about possible infrastructure damages, in cases of vandalism/theft attack or physical phenomenon.
Sensor devices	Secondary substation sensor devices	Devices installed on MV/LV substations, to enhance monitoring of the DSO in several parts of the network.	Sensor devices provide various measurements and data to the network operator. In case of an event, in which damage in the infrastructure has taken place, the DSO can instantly be notified and apply the necessary actions.
SCADA - DMS	System	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, networked data	SCADA systems provides several real-time measurements of the MV



D2.3 - Requirements and Detailed Architecture Design

		communications and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plant or machinery.	line feeders to the network operator, as well as alarms, related either to high values of currents and reactive power in the MV lines, or change of status of main feeders' telecontrollable (remotely control) switches in case of faults. Furthermore, the operator can take several remote control actions, involving telecontrollable switches in the network.
--	--	---	--

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	HV/MV substation: Vandalism/theft attack to primary substation components	Vandalism/theft attack to primary substation components	DSO	Alarming-disturbing images produced by the cameras installed at HV/MV substation due to a vandalism/theft attack.	DSO personnel have remote visual supervision of HV/MV distribution transformer substations.	Prevention or mitigation of potential infrastructure loss or equipment damage
2	HV/MV substation: Physical incident inside or near the substation infrastructure	A natural event (eg fire, flood, etc) has occurred, affecting the HV/MV substation infrastructure, in which part of the primary substation infrastructure has possibly been damaged, and a power loss may have occurred	DSO	Alarming-disturbing images produced by the cameras installed at HV/MV substation	DSO personnel have remote visual supervision of HV/MV distribution transformer substations.	Prevention of potential infrastructure loss, equipment damage, faster restoration from outage
3	Vandalism or theft attack to MV/LV substation	Vandalism or theft attack to MV/LV substation for the theft of copper	DSO	Alert produced by the sensor device installed at MV/LV substation	DSO personnel has observability over certain MV/LV distribution transformer substations.	Prevention or mitigation of vandalism attacks
4	MV/LV substation: physical/natural disaster affecting locally one or multiple substations	Physical phenomenon, causing damage to one or multiple MV/LV transformers in the network, leading to a power loss of a group of customers	DSO	Alert produced by the sensor device installed at MV/LV substation	DSO personnel has observability over certain MV/LV distribution transformer substations.	Faster restoration in case of physical events

D2.3 - Requirements and Detailed Architecture Design

4a	MV/LV substation: physical/natural disaster affecting the substation	Exceptional scenario: false alarm to the DSO, due to communications issues between sensors and network operator	DSO	Alarm by sensors installed in MV/LV substation	DSO personnel has observability over certain MV/LV distribution transformer substations.	Check by the DSO why false alarm was occurred (Wrong Parametrization of the device, etc)
----	--	---	-----	--	--	--

4.2 Steps - Scenarios

Scenario								
Scenario name:		1- HV/MV substation: Vandalism/theft attack to primary substation components						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Alarming-disturbing images produced by the cameras installed at HV/MV substation due to vandalism/theft attack	Notification to the DSO	Visual signal sent to the network operator, due to an occurring vandalism/theft attack, via the security cameras	24h live image	Surveillance equipment	DSO (security control room with monitor)	ID1	
2	Notification to the DSO received	Image capture - Streaming of image to EMMA	Images are periodically captured and imported in EMMA ARGOS via live streaming	Inspection	Camera	EMMA ARGOS	ID1	

D2.3 - Requirements and Detailed Architecture Design

3	Image captured	Periodic image AI processing	AI image-based maintenance EMMA module triggers the appropriate process to analyze the set of images and data for identifying potential security breaches	Data processing	EMMA ARGOS	EMMA ARGOS	ID1	
4	AI image processing completed	Image analysis results forwarding to DSO	Image analysis by EMMA, has identified a vandalism/theft attack, and sends notification to the DSO	DSO notification	EMMA ARGOS	DSO	ID6	
5	Image analysis results forwarded to DSO	Local authorities notification to intervene	DSO is notified on vandalism/theft attack and informs local authorities to intervene	Notification to local authorities	DSO	Local authorities		

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		2-HV/MV substation: Physical incident inside or near the substation infrastructure						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Alarming-disturbing images produced by the cameras installed at HV/MV substation	Notification to the DSO	Visual signal sent to the network operator, due to an occurring physical incident	24h live image - inspection	Surveillance equipment	DSO	ID1	
2	SCADA detects some damage in the HV/MV substation infrastructure	Signals/Alarms sending to DSO	In case some damage in the HV/MV substation infrastructure has already occurred, SCADA system will trigger alerts and MV feeders will be cut off	Periodic data - measurements to DSO	SCADA	DSO	ID2	
3	Image from cameras sent to EMMA	Image from cameras sending to EMMA	24h live image sent to EMMA via streaming link, so that an analysis by the tool can be executed on a 24h basis	24h image streaming	DSO	EMMA ARGOS	ID1	

D2.3 - Requirements and Detailed Architecture Design

4	Image from cameras sent to EMMA	EMMA analyses image received	AI image-based maintenance EMMA module triggers the appropriate process to analyze the set of images and data for identifying electrical anomalies. Data is processed and details of potential problems are obtained.	AI image analysis	EMMA ARGOS	EMMA ARGOS	ID1	
5	EMMA image analyses completed	The output of the image analysis sending back to DSO	Image analysis output is forwarded to DSO for further actions (e.g. electrical anomalies or problems detected to infrastructure due to the physical event)	AI image analysis results messaged	EMMA ARGOS	DSO	ID6	
6	The output of the image analysis sent back to DSO	Execution of remote control commands	DSO must proceed to control commands, such as primary substation isolation, network reconfiguration, in order to supply power to customers through another HV/MV substation, in case of power outage due to the physical event	Power restoration	DSO	SCADA	ID3	
7	Execution of remote control commands completed	Workforce intervention	Human resources sent to HV/MV substation for restoration	Power restoration	DSO	Available workforce		

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		3-Vandalism or theft attack to MV/LV substation						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Alert produced by the sensor device installed at MV/LV substation	Alert signal sending to the network operator	Signal sent to the network operator, due to an occurring physical incident or a vandalism attack	Notification of transformer status	Sensor device	DSO	ID4	
2	Measurements from metering devices, that require attention	Measurements sending to the DSO	In case some damage in the MV/LV substation has occurred (vandalism or physical event), zero voltage and current indications will be received by the metering devices.	Periodic measurements of the transformer	Metering devices	DSO	ID5	
3	DSO notified	Personnel intervention	DSO sends the available workforce to the incident site, in order to replace transformer	Power restoration	DSO	Available workforce		

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		4- MV/LV substation: physical/natural disaster affecting locally one or multiple substations						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Alert produced by the sensor device installed at MV/LV substation	Alarm from device	Signal sent to the network operator, due to an occurring physical incident or a vandalism attack	Notification of transformer status	Sensor device	DSO	ID4	
2	Measurements from metering devices, that require attention	Measurements sending to the DSO	In case some damage in the MV/LV substation has occurred (vandalism or physical event), zero voltage and current indications will be received by the metering devices.	Periodic measurements of the transformer	Metering devices	DSO	ID5	
3	DSO notified by either sensor devices or metering devices	Execution of remote control commands	DSO must proceed to control commands, such as network reconfiguration, in order to supply power to customers through another MV line.	Power restoration	DSO	SCADA	ID3	
4	execution of remote control commands completed	Workforce intervention	Human resources sent to MV/LV substations for restoration	Power restoration	DSO	Available workforce		

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		4a- MV/LV substation: physical/natural disaster affecting one or multiple substations						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Alarm by sensors installed in MV/LV substation	Measurements sent to the DSO	Zero values received to the DSO, because of communication issue between metering device and telemetry centre	Periodic measurements of the transformer	Metering devices	DSO	ID5	
2	DSO notified	Evaluation of metering devices communication process	DSO evaluates that some problematic measurements have been identified due to a communication issue with the metering device, and no actual disaster has occurred in the infrastructure	Metering values assessment	DSO	DSO	ID5	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Image from HV/MV substation cameras	Visual image provided by the cameras on 24h basis	
2	SCADA periodic measurements and SCADA alarms	Periodic SCADA measurements of the main feeders of MV lines. SCADA measurements involve V, I, S of MV line feeders and a set of alarms, in case of certain events in the MV lines	
3	remote control commands sent through SCADA system and other decentralised systems	Remote control commands, involving telecontrollable switches status operation for network reconfiguration, load curtailment commands to flexible assets, etc.	

D2.3 - Requirements and Detailed Architecture Design

4	Alert signal from sensor device	When a damage happens in the MV/LV substation infrastructure, the sensor device installed (e.g. accelerometer) sends signal to the network operator, informing that damage has undergone in the secondary substation	
5	measurements from metering devices	Sensors (metering devices) provide periodically measurements of the node, where the secondary substation is installed (V, I, P, Q, etc.)	
6	Output messages/results of AI image analysis		

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.21 USE CASE 21 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
21	Transmission / Operation	Remedial Actions Automation

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	22.05.2023	EMSS	-	Approved
2	12.08.2023	EMSS	Introducing priority index for RA and adding appropriate requirement. Expansion of the diagrams of use case.	Approved
3	08.12.2023	EMSS	Additional requirement definition	Approved
4	10.1.2024	EMSS	Power Flow tool integrated in SCADA	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Remedial Action Automation
Objective(s)	Define applicable remedial actions in an automated manner in case of unforeseen situations in the power system.
Related business case(s)	BC1, BC4

1.4 Narrative of use case

Narrative of use case
<p>Short description</p> <p>Transmission element overload is detected in real-time contingency analysis or when a disturbance has already occurred. In this case, the RA automation tool matches the element overload with predefined lists of RAs and defines a possible solution. After confirmation by the Control Centre operator, the appropriate signals are sent to the SCADA system to perform selected RAs.</p>
<p>Complete description</p> <p>Currently, in ROSC methodology RAs are based on analysis calculated prior to the real time, on a model prepared in day ahead or intraday time frame. This implies that RAs that are agreed in day ahead or even intraday may not be applicable to the real time operation, due to unexpected changes in the system. In such cases, the agreed RAs must be reconsidered or even new RAs must be defined in a very short period of time. This is only possible if RAs selection is automated. This mechanism can also be used when defining so-called fast RAs according to the ROSC methodology (presently, qualitative, based on personal experience, criterion is used instead of numerical when defining fast RAs). With automated RAs, the resilience of the system could be greatly increased in the most demanding situations.</p> <p>RAs can be:</p> <ol style="list-style-type: none"> 1. Preventive (PRA) which is by the definition from ROSC methodology "a RA that is the result of an operational planning process and needs to be activated prior to the investigated timeframe for compliance with the (N-1) criterion" 2. Curative (CRA) which is by the definition from ROSC methodology "a RA that is the result of an operational planning process and is activated straight subsequent to the occurrence of the respective contingency for compliance with the (N-1) criterion, taking into account transitory admissible overloads and their accepted duration" <p>For preventive RAs the change of flows or voltage shall be assessed on the N situation and on each of the N-1 situations resulting of the contingency list simulation. For curative RAs the change of flows or voltage shall be assessed by simulating of the post-contingency situation for which this curative RA has been designed.</p> <p>Automation part of this use case doesn't only apply to the RA selection but also to RA execution. The set of the signals that contain switching commands or set-points from a certain RA can be sent to SCADA system to be executed on primary equipment level. This will help reduce the time needed for manual operations and RA would be applied almost instantly.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
SCADA/EMS system executes switching commands and forwards set-points signals to generating units.
Prerequisites
Network components are able to receive remote commands.
Database of Remedial Actions created by each TSO.
Power flow tool capable of importing chosen format of grid model.
SCADA system used for remote control is able to interface with software tool for RA automation.
Database of power plants re-dispatch prices is defined.

1.7 Further information to the use case for classification/mapping

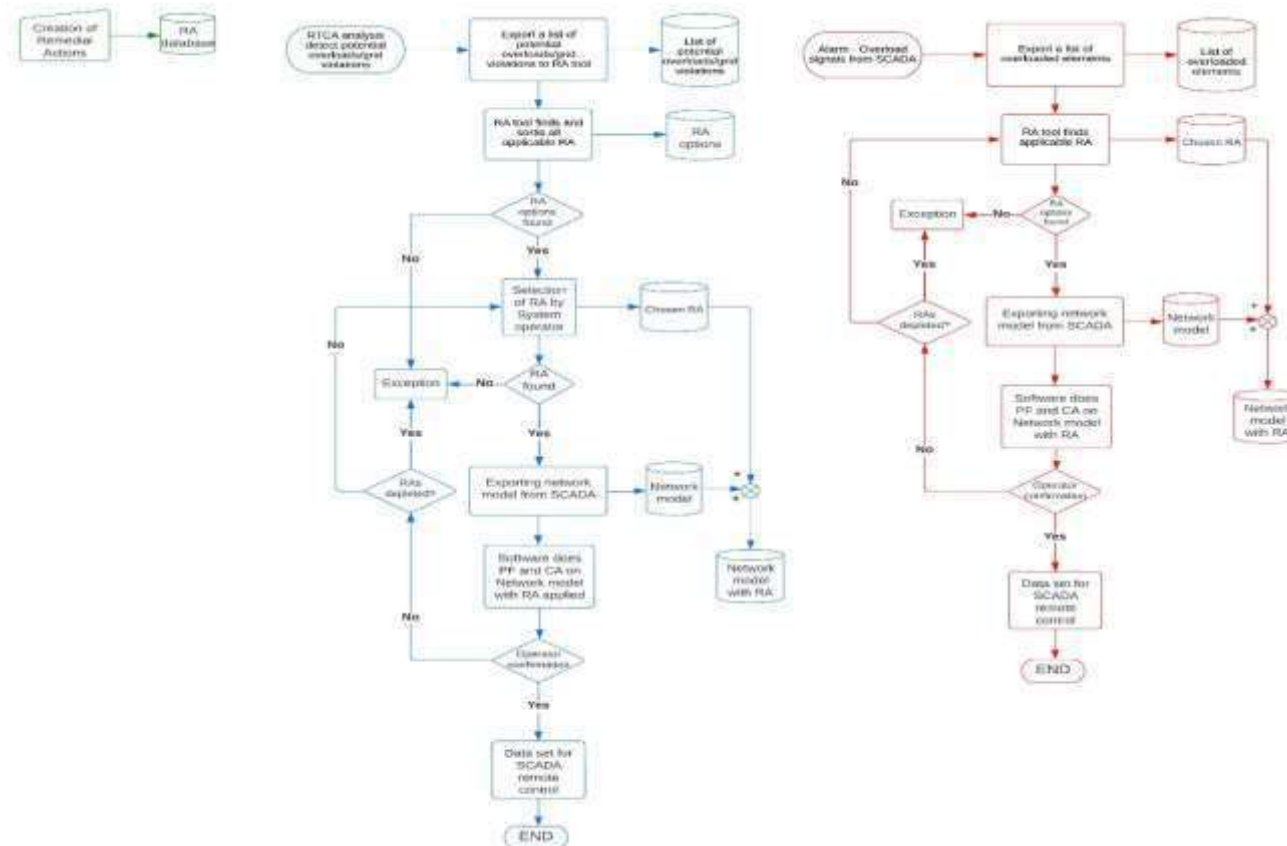
Classification information
Relation to other use cases
None
Level of depth
High level of detail
Prioritisation
5 (High). There is no tool for fast remedial action automation.
Generic, regional or national relation
National
Nature of the use case
System functional requirements description
Further keywords for classification
Remedial action, automation, remote control, power flow, contingencies, resiliency, system operation.

1.8 General remarks

General remarks

2. Diagrams of use case

Diagram(s) of use case



SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO)	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSO operator manually selects RAs from RA database and confirms RAs that should be applied according to power flow and contingency analysis calculations results.
Grouping		Group description	
Software components		Software components used in OFP business process	
Actor name	Actor type	Actor description	Further information specific to this use case
SCADA system	Control system	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, networked data communications and graphical user interfaces for high-level supervision and control of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with generation units.	SCADA/EMS system is used to: <ul style="list-style-type: none"> - run security violations (SCADA/Study CA) - create information on security violation (SCADA/Estimator) - transfer alarm to European Awareness System (EAS)

D2.3 - Requirements and Detailed Architecture Design

			<ul style="list-style-type: none">- provide interface between RA tool and network equipment that is remotely controlled.- perform base case and contingency analyses(SCADA/PF tool)
IRIS Remedial Action tool	Software application	Software solution that will be developed for this use case, and will be able to interface with SCADA/EMS system and power flow tools.	RA tool will be able to communicate with relevant systems and have graphical interface that will enable TSO operators to approve actions or manually enter new ones.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Preventive RA automation	Success scenario. Execution of accepted RAs based on N-1 violations	IRIS RA tool/SCADA	RTCA analysis detects potential overloads/security violations	Potential overloads/security violations are detected	Improved grid state
2	Fast RA automation	Success scenario. Execution of accepted RA based on real time grid violation	IRIS RA tool/SCADA	Alarm - Overload signals from SCADA	Potential overloads/security violations are detected	Improved grid state
3	Re-evaluation of RAs for preventive RA automation	Exceptional scenario. Used RAs don't give desired results.	IRIS RA tool/SCADA	Operator rejection of suggested RAs	Potential overloads/security violations are detected	Improved grid state
4	Re-evaluation of RAs for fast RA automation	Exceptional scenario. Used RAs with highest remaining priority don't give desired results.	IRIS RA tool/SCADA	Operator rejection of suggested RAs	Potential overloads/security violations are detected	Improved grid state
5	Lack of preventive RA	Exceptional scenario. All RA recommendations rejected	IRIS RA tool	No applicable RAs for potential overloads/security violations	Potential overloads/security violations are detected	Unchanged grid state Active alarm on EAS platform
6	Lack of fast RA	Exceptional scenario. All RA recommendations rejected	IRIS RA tool	No applicable RAs for potential overloads/security violations	Active security violations	Unchanged grid state Active alarm on EAS platform

4.2 Steps – Scenarios

Scenario								
Scenario name:		Preventive RA automation						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	RTCA analysis detects potential overloads/security violations	Exporting a list of potential overloads/security violations	SCADA system/Estimator sends a list of potential overloads/security violations to IRIS RA tool	Data transmission	SCADA / Estimator	IRIS RA tool	1	IRI_021, IRI_076, IRI_087
2	RA tool received a list of potential overloads/security violations	Finding and sorting all applicable RAs	IRIS RA tool finds applicable RAs and sort them for each violation	Calculation	IRIS RA tool	IRIS RA tool	-	IRI_021, IRI_077
3	Sorted database of applicable RAs is created	Manual selection of RA	Manual selection of RAs from sorted RA database	Manual data entry	TSO operator	IRIS RA tool	3	IRI_021, IRI_078, IRI_079
4	Selection of RA is completed	Transfer of chosen RAs	IRIS RA tool sends chosen RA actions to PF tool	Data transmission	IRIS RA tool	SCADA / PF tool	4	IRI_021, IRI_080
5	PF tool received chosen RA actions	Power flow calculation	PF tool runs power flow calculation with applied RAs	Calculation	PF tool	PF tool	-	
6	Power flow calculation is valid	Study CA calculation	Study CA runs contingency analysis with applied RAs	Calculation	SCADA / Study CA	SCADA / Study CA	-	

D2.3 - Requirements and Detailed Architecture Design

7	Contingency analysis is completed	Operator confirmation	System operator confirms RAs that should be applied according to power flow and contingency analysis calculation results	Manual data entry	TSO operator	IRIS RA tool	6	IRI_021, IRI_081
8	Operator confirmed RAs	Sending control signal	IRIS RA tool sends set of control signals to SCADA/EMS system	Data transmission	IRIS RA tool	SCADA	2	IRI_021, IRI_082

Scenario								
Scenario name:		Fast RA automation						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Alarm - Overload signals from SCADA	Choosing one or more overloads with intention to be solved	Operator manually choses one or more overloads with intention to be solved using applicable RAs	Manual data entry	TSO operator	IRIS RA tool	5	IRI_021, IRI_083, IRI_084
2	System operator has chosen relevant overloads	Using applicable RA with the highest priority	IRIS RA tool finds applicable RAs and chooses RAs with the highest priority	Calculation	IRIS RA tool	IRIS RA tool	-	IRI_021, IRI_077, IRI_086
3	Database of applicable RAs with the highest priority is created	Transfer of chosen RAs	IRIS RA tool sends database of chosen RAs to PF tool	Data transmission	IRIS RA tool	SCADA / PF tool	4	IRI_021, IRI_080

D2.3 – Requirements and Detailed Architecture Design

4	PF tool received chosen RA actions	Power flow calculation	PF tool runs power flow calculations with applied RAs	Calculation	SCADA / PF tool	SCADA / PF tool	-	
5	Power flow calculation is completed	Operator confirmation	Operator confirms RAs according to power flow calculation results	Manual data entry	TSO operator	IRIS RA tool	6	IRI_021, IRI_081
6	Operator confirmed RAs	Sending control signal	IRIS RA tool sends set of control signals to SCADA system	Data transmission	IRIS RA tool	SCADA	2	IRI_021, IRI_082

Scenario								
Scenario name:		Re-evaluation of RAs for preventive RA automation						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Operator rejection of suggested RAs	Manual selection of RAs	Manual selection of RAs from sorted RA database	Manual data entry	TSO operator	IRIS RA tool	3	IRI_021, IRI_078, IRI_079
2	Selection of RAs is completed	Transfer of chosen RAs	IRIS RA tool sends chosen RA actions to PF tool	Data transmission	IRIS RA tool	SCADA / PF tool	4	IRI_021, IRI_080
3	PF received chosen RAs	Power flow calculation	PF tool runs power flow calculation with applied RAs	Calculation	SCADA / PF tool	SCADA / PF tool	-	

D2.3 - Requirements and Detailed Architecture Design

4	Power flow calculation is valid	Study CA calculation	Study CA runs contingency analysis with applied RAs	Calculation	SCADA / Study CA	SCADA / Study CA	-	
5	Contingency analysis is completed	Operator confirmation	Operator confirms RAs that should be applied according to power flow calculation results	Manual data entry	TSO operator	IRIS RA tool	6	IRI_021, IRI_081
6	Operator confirmed RAs	Sending control signal	IRIS RA tool sends set of control signals to SCADA/EMS system	Data transmission	IRIS RA tool	SCADA	2	IRI_021, IRI_082

Scenario								
Scenario name:		Re-evaluation of RAs for fast RA automation						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Operator rejection of suggested RAs	Using applicable RAs with the next highest priority	IRIS RA tool finds next applicable RAs according to priority index	Calculation	IRIS RA tool	IRIS RA tool	-	IRI_021, IRI_077, IRI_086
2	Database of applicable RAs is created	Transfer of chosen RA actions	IRIS RA tool sends database of chosen RAs to PF tool	Data transmission	IRIS RA tool	SCADA / PF tool	4	IRI_021, IRI_080
3	PF received chosen RA actions	Power flow calculation	PF tool runs power flow calculation with applied RAs	Calculation	SCADA / PF tool	SCADA / PF tool	-	

D2.3 - Requirements and Detailed Architecture Design

4	Power flow calculation is completed	Operator confirmation	Operator confirms RAs that should be applied according to power flow calculation results	Manual data entry	TSO operator	IRIS RA tool	6	IRI_021, IRI_081
5	Operator confirmed RAs	Sending control signal	IRIS RA tool sends set of control signals to SCADA system	Data transmission	IRIS RA tool	SCADA	2	IRI_021, IRI_082

Scenario								
Scenario name:		Lack of preventive RA						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	No applicable RAs for potential overloads/ security violations	Alarm sending to EAS	Alarm is sent to EAS platform through SCADA system – N-1 violation (yellow colour)	Data transmission	IRIS RA tool	SCADA	2	IRI_021, IRI_085

Scenario								
Scenario name:		Lack of fast RA						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	No applicable RAs for potential overloads/ security violations	Alarm sending to EAS	Alarm is sent to EAS platform through SCADA system – N violation (red colour)	Data transmission	IRIS RA tool	SCADA	2	IRI_021, IRI_085

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	CA results	List of CA results	IRI_076
2	Control signals	Set of signals sent from SCADA system	
3	Check list of RA	List of RAs that could be selected by end user	
4	Chosen RAs	List of RAs actions chosen by system operator	
5	Check list of overloaded elements	List of overloaded elements in real time that could be selected by end user	
6	Yes/No	Confirmation type of information	IRI_081

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Remedial action (RA)	Any measure according to Article 22.1 of the SO GL (EU Regulation No. 2017/1485) which is applied by a TSO or several TSOs, manually or automatically, in order to maintain operational security.
Preventive remedial action	A remedial action that is the result of an operational planning process and needs to be activated prior to the investigated timeframe for compliance with the (N-1) criterion.
Curative remedial action	A remedial action that is the result of an operational planning process and is activated straight subsequent to the occurrence of the respective contingency for compliance with the (N-1) criterion, taking into account transitory admissible overloads and their accepted duration.



D2.3 - Requirements and Detailed Architecture Design

ROSC (Regional Operational Security Coordination) methodology	Common provisions for regional operational security coordination, to be applied by the regional security coordinators and the TSOs of the capacity calculation region, based on the methodology for coordinating operational security analysis, as defined in SO GL.
---	--

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.22 USE CASE 22 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
22	Distribution, DER / Operation, Station, Field, Process	Prevention and mitigation of cascading effects in case of extreme weather events

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	11/03/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos		
0.2	28/03/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis	Minor changes in scenario descriptions	
0.3	30/03/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis	Split UC into two scenarios (occurring event, forecasted event)	
0.4	15/05/2023	Ugo Stecchi	UC 1 st Revision	Approved
0.5	25/05/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis	Corrections after 1 st Revision	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	The objective of this use case is the enhancement of the grid's resilience against potential cascading effects, which stem from an extreme weather event. Initially, an assessment of the current state of grid resilience is performed, followed by an analysis of a potential cascading effect's impact, which is triggered by an extreme weather event. By exploiting R2D2 both C3PO and EMMA tool, the optimal mitigation measures can be proposed to the network operator and then be executed, in order to achieve a faster restoration of the network and minimize load shedding and power loss to customers. The intervention of available workforce shall be done in an optimal way to the most critical locations of the damaged assets, so that a faster repair of infrastructure can be achieved.
Objective(s)	<ol style="list-style-type: none">1. The impact of extreme weather on the grid is minimized thanks to the implemented mechanisms described in this use case.2. The grid operator prepares a report with all details of the actions taken and the rationale behind them. The lessons learned from the event are incorporated to the knowledge of the mechanism, so its performance can be improved for future situations.
Related business case(s)	BC1, BC2

1.4 Narrative of use case

Narrative of use case
<p>Short description</p> <p>This Use Case focuses on the enhancement of the grid's resilience under extreme weather events. The analysis of the network's current state, along with potential cascading effect indicators calculation that derive from a possible extreme weather event, are necessary for the R2D2 tools to propose the optimal corrective actions for the minimization of potential major outages. A series of actions, like network flexibility capability and reconfiguration actions are utilised for the grid's resilience enhancement. Finally, a faster restoration of outages can be achieved, through the optimal workforce allocation in the critical parts of the network.</p>
<p>Complete description</p> <p>The target of this use case is to both assess and enhance the resilience of the grid against potential cascading effects from extreme weather events. Such an event can cause severe damages in the network infrastructure (eg several MV lines fed by a HV/MV substation, primary and secondary substations) and as a consequence, a major outage to several customers may occur.</p> <p>Initially, the module of '<i>spatial and temporal event and fragility modelling</i>' (T3.3.1) will be used, in order to assess the system resilience, taking into account the existing network infrastructure and thus calculating fragility curves. Furthermore, the '<i>cascading modelling and quantification</i>' module (T3.3.2) will be used to provide some crucial indications, related to the impact of the event. Based on this assessment, resilience enhancement measures to mitigate the impact in case of an imminent extreme weather event will be examined. Finally, the EMMA module developed in the '<i>resource management</i>' Task (T6.3), will be the one to determine and allocate the available workforce and human resources in an optimal way, in order to achieve the fastest possible power restoration. The aforementioned mechanisms will include:</p> <ul style="list-style-type: none"> • Forecast of weather events that could potentially threaten the grid. • Modelling of extreme weather impact on the network. • Optimal schedule of demand response and energy storage systems to minimize load shedding. • The application of further mitigation actions (isolation of faulted sections of a feeder, etc.) • Automatic generation, assignment, and tracking of the necessary works to mitigate the identified problem.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
This UC will be simulated, by assuming that a part of the network infrastructure is affected by an extreme weather event – scenario 1
The forecast of weather events is triggered periodically (e.g. hourly) – scenario 2
Prerequisites
The topology of the network is well known and modelled.
An accurate weather forecast for the area of the grid is available and periodically updated.
In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the distributed generators

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
23
Level of depth
5
Prioritisation
High
Generic, regional or national relation
Regionally, nationally – will be applied to the GR demo site and HEDNO is also interested in replicability – scalability of resilience enhancement solutions in several regions of the country. Worldwide - Also, the modules used in this UC could be utilised to resolve grid problems from extreme weather events, on an international basis.
Nature of the use case
This UC indicates a sequence of certain functionalities of C3PO and EMMA modules, aiming at the mitigation of an either occurring or forecasted extreme weather event
Further keywords for classification
Cascading effect, extreme weather event, resilience assessment, power loss mitigation, grid restoration

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	Network operator	Distribution System Operator	The DSO is responsible for the physical security of its infrastructure, as well as for the continuous supply of power to its customers. In case of an imminent extreme weather event, the DSO must assess the potential effects to the network and proceed to the necessary optimal corrective actions.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
C3PO Cascading simulators, operational network planning modules	Application	R2D2 Product for the assessment of the event and proposal of optimal mitigation measures.	R2D2 Product, which assesses the impact of the physical event on network infrastructure and finds the optimal mitigation measures to be performed by the network operator
EMMA GIMAN	Application	<ul style="list-style-type: none"> R2D2 module, which optimizes the available workforce to be allocated in critical parts of the network, in case of an occurring event R2D2 module, performing an identification of the most critical assets and calculates the optimal prioritization of actions, in case of a forecasted event. 	<p>If a natural event has caused damage in infrastructure or even a power loss to a group of customers, the available personnel can be sent in an optimal way to the critical parts of the network, for a faster power restoration.</p> <p>Furthermore, in case of a forecasted extreme weather event, an identification of critical assets along with the optimal prioritization of actions to be done by the workforce is calculated, in order to act first on the locations where the cascading effect can occur.</p>

Grouping		Group description	
Other actors			
Actor name	Actor type	Actor description	Further information specific to this use case
Weather service provider	Weather service provider		A weather service provider is responsible for the periodic notification to the network operator

D2.3 - Requirements and Detailed Architecture Design

			about several parameters of an occurring extreme weather event.
SCADA - DMS	System	System providing periodic data to the DSO, along with certain kind of alarms.	SCADA systems provides several periodic measurements of the MV line feeders to the network operator, as well as alarms, related either to high values of currents and reactive power in the MV lines, or change of status of main feeders' telecontrollable switches in case of faults. Furthermore, the operator can take several remote control actions, involving telecontrollable switches in the network.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Assessment and mitigation of effects when occurring extreme weather event	In case of an extreme weather event, an assessment of its effect in network infrastructure is performed, followed by the optimal mitigation measures calculated from C3PO and EMMA tool.	DSO	An extreme weather event has already occurred, affecting the network infrastructure.	<ul style="list-style-type: none"> • The topology of the network is well known and modelled. • In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the distributed generators 	The impact of extreme weather event on the grid is minimized thanks to the implemented mechanisms described in this use case. The grid operator prepares a report with all details of the actions taken and the rationale behind them.
1a	Insufficient data for modelling of extreme weather event impact	Exceptional scenario: In case some critical network data is missing, C3PO tool can't perform initial assessment of the occurring event impact to the grid	Ditto	Ditto	Ditto	Ditto
1b	Measures proposed by C3PO non-executable by the DSO	Exceptional scenario: In case the DSO judges that the optimal mitigation measures cannot be executed, an alternative solution must be proposed by the tool	Ditto	Ditto	Ditto	Ditto

D2.3 - Requirements and Detailed Architecture Design

2	Assessment and proactive actions in case of forecasted extreme weather event	In case of a forecast of an extreme weather event, an assessment of its effect in network infrastructure is performed, followed by the optimal mitigation measures calculated from C3PO and EMMA tool.	DSO	The forecast of weather events is triggered periodically (e.g. hourly). The impact of weather event on system is assessed and if necessary, the appropriate proactive operational actions are applied.	<ul style="list-style-type: none"> • The topology of the network is well known and modelled. • An accurate weather forecast for the area of the grid is available and periodically updated. • In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the distributed generators 	<ul style="list-style-type: none"> • The impact of the imminent extreme weather event on the grid is minimized thanks to the implemented mechanisms described in this use case. • The grid operator prepares a report with all details of the actions taken and the rationale behind them. • The lessons learned from the event are incorporated to the knowledge of the mechanism, so its performance can be improved for future situations.
---	--	--	-----	--	---	--

4.2 Steps – Scenarios

Scenario								
Scenario name:		1 - Insufficient data for modelling of extreme weather event impact						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Extreme weather event has happened		An extreme weather event has already occurred, affecting part of the grid infrastructure.					

D2.3 - Requirements and Detailed Architecture Design

2	Alarms triggered by the SCADA	Signals/Alarms sent to DSO	In case of a damage to the network infrastructure due to an occurring extreme weather event, SCADA triggers alarms to the DSO	Periodic measurements to DSO	SCADA	DSO	ID1 - V, I of MV line feeders, Alarms from SCADA	
3	Modelling of extreme weather impact on distribution system	Current network resilience assessment	In the event of extreme weather, its spatiotemporal impact on distribution system components is modelled. This can be achieved using fragility curves or a N-k criterion for different weather regions.	Resilience assessment	C3PO - spatial and temporal event and fragility modelling tool	C3PO - cascading modelling and quantification module	ID2 - Probability of component failures, vulnerable components identified	
4	Assessment of potential power loss or cascading effect by C3PO cascading simulators	R2D2 C3PO calculates the effect of the occurring event	Use of C3PO Cascading simulators, in order to assess the damage occurred and calculate cascading effect indicators	Calculation of several metrics	C3PO - cascading modelling and quantification module	C3PO-Operational planning tool	ID3 - Cascading effect indicators calculation	
5	Use of C3PO-Operational planning tool, in order to take all necessary actions to mitigate the event	C3PO suggests the optimal mitigation plan	C3PO-Operational planning tool finds the optimal necessary actions for the DSO (flexibility sources, network reconfiguration etc.) in order to mitigate the event.	Optimization of mitigation measures	C3PO-Operational planning tool	DSO	ID4 - Optimal Actions suggested: use of available flexibility, storage for black start for certain parts of the network, network reconfiguration options	

D2.3 - Requirements and Detailed Architecture Design

6	Outputs of C3PO forwarded to EMMA	C3PO results provided to EMMA	Critical network infrastructure affected components, as well as proposed mitigation measures forwarded to EMMA		C3PO	EMMA-GIMAN	ID5 – Affected network infrastructure and optimal measures	
7	Workforce availability and allocation calculated by EMMA	Optimal allocation of personnel to critical parts	The tool calculates the available human resources to intervene in an optimal way to critical nodes of the network. Optimal Human resources sent to incident sites for restoration	Optimization of personnel allocation	EMMA-GIMAN	Workforce	ID6 - Optimal Allocation of workforce, human resources	
8	Implementation of proposed operational measures to mitigate the event	Execution of optimal commands	DSO executes the optimal measures proposed by step 5, activating available flexibility, DSM, changing the status of telecontrollable switches, etc.		DSO	SCADA	ID7 – remote control commands sent through SCADA system	
9	Results monitoring		The results of the actions are monitored in order to assess the adequacy of the decisions adopted. Further actions can be taken in order to correct deviations from the expected behaviour.		Grid monitoring devices, SCADA, grid operator	C3PO	Grid operator feedback	

D2.3 - Requirements and Detailed Architecture Design

10	Lessons learned		After the end of extreme weather, the grid operator (together with the appropriate personnel) analyses the result of the mitigation actions in order to extract lessons learned and improve future operations. The necessary changes to the process are performed using C3PO		Grid operator	C3PO	Grid operator feedback	
----	-----------------	--	--	--	---------------	------	------------------------	--

Scenario								
Scenario name:		1a - Insufficient data for modelling of extreme weather event impact						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Extreme weather event has happened		An extreme weather event has already occurred, affecting part of the grid infrastructure.					
2	Alarms triggered by the SCADA	Signals/Alarms sent to DSO	In case of a damage to the network infrastructure due to an occurring extreme weather event, SCADA triggers alarms to the DSO	Periodic measurements to DSO	SCADA	DSO	ID1 - V, I of MV line feeders, Alarms from SCADA	

D2.3 - Requirements and Detailed Architecture Design

3	Data missing		If no data (e.g. insufficient network topology) is received from any of the different sources, C3PO will issue an alert to the grid operator.		C3PO	DSO	Alert	
---	--------------	--	---	--	------	-----	-------	--

Scenario								
Scenario name:		1b - Measures proposed by C3PO non-executable by the DSO						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Extreme weather event has happened		An extreme weather event has already occurred, affecting part of the grid infrastructure.					1
2	Alarms triggered by the SCADA	Signals/Alarms sent to DSO	In case of a damage to the network infrastructure due to an occurring extreme weather event, SCADA triggers alarms to the DSO	Periodic measurements to DSO	SCADA	DSO	ID1 - V, I of MV line feeders, Alarms from SCADA	2

D2.3 - Requirements and Detailed Architecture Design

3	Modelling of extreme weather impact on distribution system	Current network resilience assessment	In the event of extreme weather, its spatiotemporal impact on distribution system components is modelled. This can be achieved using fragility curves or a N-k criterion for different weather regions.	Resilience assessment	C3PO - spatial and temporal event and fragility modelling tool	C3PO - cascading modelling and quantification module	ID2 - Probability of component failures, vulnerable components identified	3
4	Assessment of potential power loss or cascading effect by C3PO	R2D2 C3PO calculates the effect of the occurring event	Use of C3PO- Cascading simulators, in order to assess the damage occurred and calculate power loss duration and potential cascading effect.	Calculation of several metrics	C3PO - cascading modelling and quantification module	C3PO-Operational planning tool	ID3 - Cascading effect indicators calculation	4
5	Use of C3PO- Operational planning tool, in order to take all necessary actions to mitigate the event	C3PO suggests the optimal mitigation plan	C3PO-Operational planning tool finds the optimal necessary actions for the DSO (flexibility sources, network reconfiguration etc.) in order to mitigate the event.	Optimization of event mitigation measures	C3PO- Operational planning tool	DSO	ID4 - Optimal Actions suggested: use of available flexibility, storage for black start for certain parts of the network, network reconfiguration options	5



D2.3 - Requirements and Detailed Architecture Design

6	Proposed measures cancellation		If the grid operator considers that the determined measures are not the proper solution, they are cancelled and new restrictions are added in order a new solution to be found by C3PO tool. Lessons learned from this experience will be integrated into the system as explained in Step 11		DSO	C3PO	Cancellation command	6
7	C3PO- Operational planning module proposes an alternative actions to mitigate the event	C3PO suggests the optimal alternative mitigation plan	C3PO-Operational planning tool finds an alternative proposal of actions for DSO (flexibility sources, network reconfiguration etc.)	Repeat of optimization process, based on the new restrictions set by the DSO	C3PO- Operational planning tool	DSO	ID4 - Optimal Actions suggested: use of available flexibility, storage for black start for certain parts of the network, network reconfiguration options	7

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		2- Assessment and proactive actions in case of forecasted extreme weather event						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Weather forecasting	Periodic weather forecasts	Weather forecasting is performed in a regular basis.	Weather forecasting	Weather service provider	C3PO - spatial and temporal event and fragility modelling tool	ID8 - Weather forecast parameters	
2	Modelling of extreme weather impact on distribution system	Current network resilience assessment	In the event of a forecasted extreme weather event, its spatiotemporal impact on distribution system components is modelled. This can be achieved using fragility curves or a N-k criterion for different weather regions.	Resilience assessment	C3PO - spatial and temporal event and fragility modelling tool	C3PO - cascading modelling and quantification module	ID2 - Probability of component failures, vulnerable components identified	
3	Assessment of potential power loss or cascading effect by C3PO cascading simulators	R2D2 C3PO calculates the effect of the forecasted event	Use of C3PO Cascading simulators, in order to calculate potential power loss duration and indicators of the incoming event.	Calculation of several metrics	C3PO - cascading modelling and quantification module	C3PO- Operational planning tool	ID3 - Cascading effect indicators calculation	

D2.3 - Requirements and Detailed Architecture Design

4	Use of C3PO-Operational planning tool, in order to calculate all necessary proactive actions.	C3PO suggests the optimal proactive plan	C3PO-Operational planning tool finds the optimal necessary actions for the DSO (flexibility sources, network reconfiguration etc.) in order to be proactive for the event.	Optimization of pre-disaster measures	C3PO-Operational planning tool	DSO	ID4 - Optimal Actions suggested: use of available flexibility, storage for black start for certain parts of the network, network reconfiguration options	
5	Outputs of C3PO forwarded to EMMA	C3PO results provided to EMMA	Critical infrastructure to be most likely affected and proactive measures calculated forwarded to EMMA		C3PO	EMMA-GIMAN	ID9 – Network critical infrastructure and optimal proactive measures	
6	Prioritization of actions to be performed and identification of most critical parts before the event happens	Optimal calculation of pre-disaster actions	The tool calculates in advance the available human resources and emergency shifts that must be in alert, as well as the actions that must take high priority	Pre-disaster plan formulation	EMMA-GIMAN	Workforce	ID10 – pre-disaster plan and prioritization of actions to be executed by the workforce	
7	Application of proposed proactiveoperational measures before the event	Execution of optimal commands	DSO executes the optimal proactive measures proposed by step 4, activating available flexibility, DSM, changing the status of telecontrollable switches, etc.		DSO	SCADA	ID7 – remote control commands sent through SCADA system	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	V, I of MV line feeders, Alarms from SCADA	Periodic SCADA measurements of the main feeders of MV lines. SCADA measurements involve V, I, S of MV line feeders and a set of alarms, in case of certain events in the MV lines	
2	Probability of component failures, vulnerable components identified	depending on the methodology followed to model the impact	
3	Cascading effect indicators calculation	Indicators provided as output of the C3PO - cascading modelling and quantification module (energy not supplied, loss of load probability, loss of load duration, resilience trapezoid, etc.)	
4	Optimal Actions suggested by C3PO-Operational planning tool	use of available flexibility solutions, decentralised control of DER, network reconfiguration, generation redispatch, islanding, DR, etc.	
5	Affected network critical infrastructure and optimal measures	Results from C3PO spatial and temporal event and fragility modelling tool and C3PO cascading modelling and quantification module, regarding the critical network assets affected by the extreme weather event, as well as the optimal measures proposed to be executed by the DSO	
6	Optimal Allocation of workforce, human resources	EMMA GIMAN module calculates the optimal allocation of the available workforce of the DSO, in order to give priority to the power restoration in the most critical parts of the network, and thus achieve faster power restoration	

D2.3 – Requirements and Detailed Architecture Design

7	remote control commands sent through SCADA system and other decentralized systems	Remote control commands, involving telecontrollable switches status operation for network reconfiguration, load curtailment commands to flexible assets, etc.	
8	Weather forecast parameters	Weather forecast parameters (e.g. hourly wind speed)	
9	Network critical infrastructure and optimal proactive measures	Results from C3PO spatial and temporal event and fragility modelling tool and C3PO cascading modelling and quantification module, regarding the critical network assets most likely to be affected by the forecasted extreme weather event, as well as the optimal proactive measures proposed to be executed by the DSO	
10	pre-disaster plan and prioritization of actions to be executed by the workforce	EMMA GIMAN calculates the optimal pre-disaster plan to follow after the extreme weather event. Furthermore, the available workforce that will be needed for possible intervene to the most critical assets will be also calculated.	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.23 USE CASE 23 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
23	Transmission, Distribution / Operation, Station , Field, Process	Cooperative crisis handling in case of cascading event

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	11/03/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos, Theofanis Kontopoulos	Minor corrections in scenario descriptions	
0.2	28/03/2023	Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis, Theofanis Kontopoulos	Minor corrections in scenario descriptions	
0.3	30/03/2023	Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis	Minor corrections in scenario descriptions	
0.4	15/05/2023	Ugo Stecchi	Revision	Approved
0.5	26/05/2023	Theofanis Kontopoulos, Viktoras Papadimas, Greg Kanellos, Dimitrios Selimis	Minor corrections after 1 st Revision	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	<p>The scope of this UC is to indicate the signal that must be exchanged between the system and the network operator, in case of a failure in the interconnection point between system and network. An event, which may affect the HV/MV substations due to either an extreme weather event or even a cyber-attack event, could cause a potential cascading effect. An alert signal must be exchanged between the system and network operators, so that a cooperative crisis handling can follow. The main scenarios under examination in this Use Case are the following ones:</p> <ul style="list-style-type: none"> • In case of a major failure to a large part of the distribution network, several MV lines or even a HV/MV substation may need to be cut off, in order not to affect the upper system. In that scenario, an upward alert/signal needs to be provided by the DSO to the system operator, so that the latter can proceed with all necessary actions. Then, UC36 can also be initiated by the DSO, in order to mitigate the event and all proposed remedial actions may follow. • In case of an event in part of the system, a downward signal must be received by the DSO, in order to proceed to actions, such as the isolation of a HV/MV substation to mitigate a potential cascading effect.
Objective(s)	Proactive mitigation of cascading events
Related business case(s)	BC1, BC2, BC4

1.4 Narrative of use case

Narrative of use case
Short description
This Use Case focuses on the upward or downward signal/alert that must be exchanged between the system and the network operator, in order to prevent a potential cascading effect caused by a failure in the interconnection point between system and network.
Complete description
The objective of this use case is to examine the necessary signal that can be sent in case of a failure in the interconnection point between system and network, which may lead to a potential cascading effect. The cause of such an event could either be an extreme weather event or a cyber-attack. An extreme weather event as described in UC36, can cause severe damage to the grid infrastructure, and may lead to a possible outage. Furthermore, in case of a cyber-attack, which may come from a possible malicious attack to the databases of the HV/MV substation control systems (eg SCADA) or from software/firmware distortion of the controllers of protection relays of MV lines, major parts of the network can be cut off. Considering that according to the HEDNO Manual the loss of more than 50 MVA for more than half an hour is considered as



D2.3 - Requirements and Detailed Architecture Design

emergency and IPTO (Greek TSO) should be notified, this UC focuses on the signals and alerts that must be exchanged between the system and network either upstream or downstream, so that a cooperative crisis handling between the operators can follow.

In case either of an incident in the HV/MV substation (interconnection point between system-network) or an event, which may affect large part of the MV distribution network, a cascading event may occur. A possible result could be the HV/MV substation isolation and the grid operator must inform the TSO by sending a signal-alert, so that the latter can proceed to its necessary proactive actions. Furthermore, R2D2 C3PO tools could also be utilized from the DSO, in order to mitigate such an event, as described in UC36 (for physical events).

If an incident (physical or cyber) has occurred in the system, which may affect the distribution network by leading to a loss of multiple MV lines, a signal must be sent to the grid operator, in order for the latter to take proactive measures for the mitigation of the event.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Simulation of the alert signal only, that has to be exchanged between TSO and DSO
Assumption of an event simulation in the interconnection point between system and network
Prerequisites
Existence of communication channels between TSO-DSO
The topology of the network is well known and modelled

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC22 (in case of physical events)
Level of depth
low
Prioritisation
high
Generic, regional or national relation
Regionally, nationally – will be applied to the GR demo site and HEDNO is also interested in replicability – scalability. Worldwide - Also, the modules used in this UC could be replicated in an international level.
Nature of the use case
Focuses on signal exchange between system and network operator
Further keywords for classification
Cascading effect, signal/alert exchange between transmission and distribution operator

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	System operator	Distribution System Operator	In case of a cascading effect, due to an event in the interconnection point between system and network, or in the distribution network, the DSO sends an upward signal to the TSO.
TSO	System operator	Transmission system operator	In case of a cascading effect, due to an event in the system, the TSO sends a downward signal to the DSO
Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
C3PO Cascading simulators, operational network planning modules	Application	R2D2 Product for the assessment of the event and proposal of optimal mitigation measures.	R2D2 Product, which assesses the impact of the physical event on network infrastructure and finds the optimal mitigation measures to be performed by the network operator

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Incident in the interconnection point between system – network (HV/MV substation) or in the distribution network	Incident in the interconnection point between system – network (HV/MV substation) or in the distribution network	DSO	Physical event or cyber-attack incident in the interconnection point between system-network	Existence of communication channels between TSO-DSO The topology of the network is well known and modelled	Proactive mitigation of cascading events
2	Failure to the system	failure to the transmission system, that may cause a cascading effect by affecting HV/MV substations	TSO	incident in the transmission system	Existence of communication channels between TSO-DSO • The topology of the network is well known and modelled	Proactive mitigation of cascading events

4.2 Steps – Scenarios

Scenario								
Scenario name:		Incident in the interconnection point between system – network						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Incident identification in the interconnection point between system – network (HV/MV substation) or in the distribution network	Signal from the SCADA	Physical phenomenon incident or cyber-attack that leads to the loss of multiple MV lines of the network	Notification to the DSO	SCADA	DSO	ID1 –Alert from SCADA	
2	Assessment of potential power loss or cascading effect by C3PO	R2D2 C3PO calculates the effect of the occurring event	Use of C3PO-Cascading simulators, in order to assess the damage occurred and calculate power loss duration and potential cascading effect.	Calculation of several metrics	C3PO-cascading simulators	C3PO-Operational planning tool	ID2 - Cascading effect indicators calculation	
3	Grid operator informs the TSO of the potential cascading effect	Upward signal to TSO	DSO sends an alert to the TSO, in case of a cascading effect, where the largest part of the network under the HV/MV substation will lose power	TSO notification	DSO	TSO	ID3 – Signal/Alert	



D2.3 - Requirements and Detailed Architecture Design

4	TSO evaluates the situation and proceeds to the necessary proactive measures (eg islanding the failed HV/MV substation)				TSO			
5	DSO proceeds to the measures proposed by C3PO (operational planning tool) (physical events), as described in UC36		UC 22 initiation. See UC22 on how DSO tackles a potential cascading effect from a physical phenomenon		DSO			

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Failure to the system						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	TSO informs the DSO of the potential cascading effect, which stems from a failure to the system	Downward signal to DSO	TSO sends a signal to the grid operator in case of a potential cascading effect, where for example a HV/MV substation will be needed to be cut off	DSO notification	TSO	DSO	ID3 –Signal/Alert	
2	Use of C3PO-operational planning tool (T.3.4) to suggest necessary proactive measures	R2D2 C3PO calculates the necessary reconfiguration actions to be taken.	Use of C3PO-Operational planning tool, in order to proceed to proactive measures of network reconfiguration, after the DSO has received the signal from TSO.	Necessary proactive actions to be taken by the DSO	C3PO-operational planning	DSO	ID5 - Optimal Actions suggested: use of available flexibility, storage for black start for certain parts of the network, network reconfiguration options	
3	DSO proceeds to the necessary proactive measures		DSO takes a series of actions, in order to secure the maximum possible security of supply to customers. (e.g. network reconfigurations to supply power from other primary substations)		DSO	SCADA	ID4 – Remote control commands for necessary network remedial actions.	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Alert from SCADA	V, I of MV line feeders, Alarms from SCADA. Periodic SCADA measurements of the main feeders of MV lines. SCADA measurements involve V, I, S of MV line feeders and a set of alarms, in case of certain events in the MV lines	
2	Cascading effect indicators calculation	Indicators provided as output of the C3PO module (energy not supplied, loss of load probability, loss of load duration, resilience trapezoid, etc.)	
3	Signal/Alert	Upward or downward alert/signal that must be exchanged between system and network operator.	
4	Remote control commands for necessary network remedial actions	Change of status of remote controllable switches, network reconfiguration to supply power from other MV lines or different primary substations etc.	
5	Optimal Actions suggested by C3PO-Operational planning tool	use of available flexibility solutions, decentralised control of DER, network reconfiguration, generation redispatch, islanding, DR, etc.	



6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.24 USE CASE 24 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
24	Transmission, Distribution / Operation, Station	Cyber Security Risk assessment on EPES infrastructure

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	31.5.2023	Cyber Noesis (CYBER)		Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Conduct Cyber Security Risk Assessment using the C3PO Cyber Risk Assessment Tool to assist TSOs/DSOs assess the cyber security posture of their organization.
Objective(s)	<ul style="list-style-type: none"> Evaluate an EPES system operator security posture. Evaluate EPES system operators' operational technology (OT) and information technology (IT) cyber security practices. Identify high risk areas and propose mitigation measures.
Related business case(s)	BC3

1.4 Narrative of use case

Narrative of use case
Short description <p>The aim of this use case is to demonstrate the use of the developed C3PO Cyber Risk Assessment Tool (T3.1), and its capability to identify and assess risks, measure risks levels and assess the security posture of the target environment, propose risk mitigation measures, including the developed R2D2 components.</p>
Complete description <p>This UC will deploy the Cyber Risk Assessment Tool to the Pilot Site environment to assess the target environment's cyber security posture. This process entails the following steps:</p> <ol style="list-style-type: none"> 1. <u>Context Establishment</u>: Define the scope of the target environment, legal requirements, restrictions and priorities in line with the context of the organization's activities and objectives. Acceptable risk levels will be also defined during this step. 2. <u>Context Modeling</u>: This step involves the modelling of objects (assets), and the establishment of their relation to one another, as well as the establishment of the potential impacts. 3. <u>Assessment, Evaluation and Treatment of Risks</u>: Having established the context, including the assets and their values with respect to the impact for the organization in case of a cybersecurity incident, and having identified the threats, the risk assessment tool will be used to calculate the risks. The results will be evaluated against acceptable risk levels and/or specific attack scenarios. For those risk scenarios that exceed these levels, mitigation measures will be proposed, among which are the solutions proposed by R2D2, to demonstrate their contribution towards risk reduction. <p>These steps will be performed with the close cooperation of the involved partners and the Pilot Sites. The Risk Assessment experts will utilize the domain knowledge of the Pilot Sites in the establishment of the context for the target environment, in order to allow for the best possible modeling of the various assets and threats. Each Pilot Site will provide information on the assets and threats relevant specifically to their environment, and perform the risk analysis using the developed tool, with the help of the experts. The Pilot Sites will then receive the Risk Assessment results and suggested mitigation measures for future implementation.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Pilot Sites availability: Xanthi
Prerequisites
Information about the target environment (assets, impact, infrastructure, measures) is available.
Pilot site resources (personnel) are engaged to provide information during the process

1.7 Further information to the use case for classification/mapping

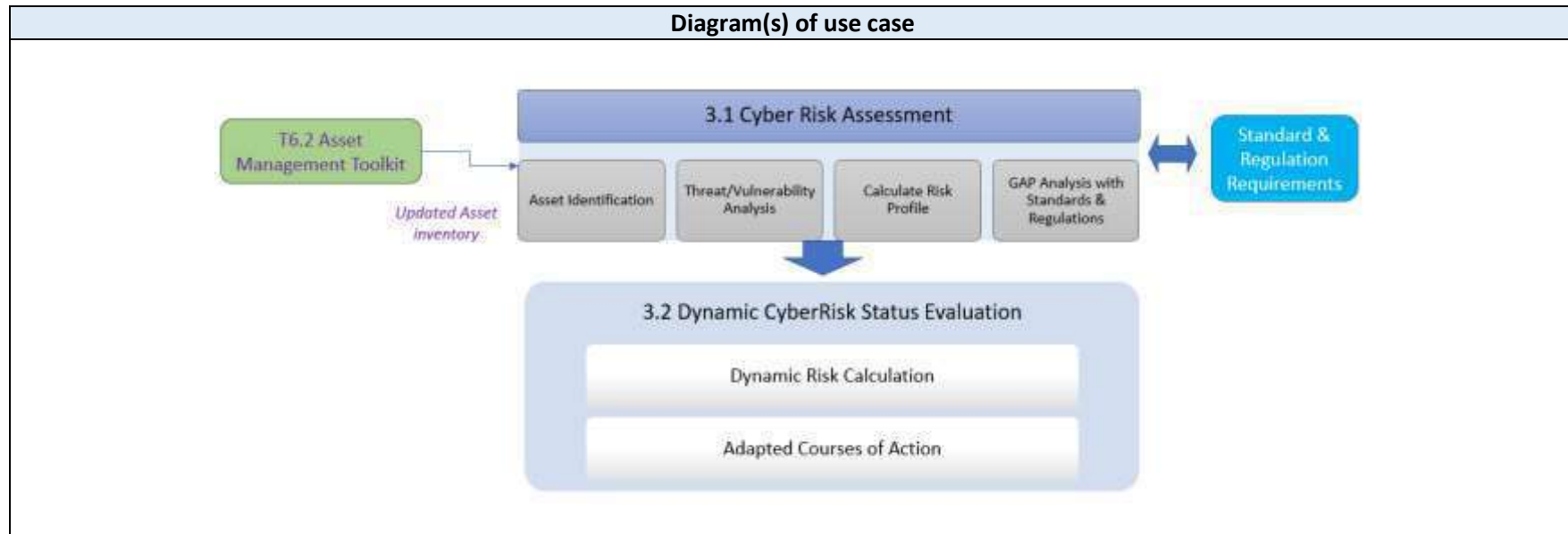
Classification information
Relation to other use cases
<ol style="list-style-type: none"> 1) Provide cyber risk information (assets and corresponding values) to the Dynamic Cyber Risk Evaluation Tool - Use Case 25 2) Receive information on the asset inventory of the pilot site from the Asset Management Toolkit – T6.2 - Alternatively the list of assets for the selected target environment shall be obtained by the Pilot Site.
Level of depth
High.
Prioritization
Generic, regional or national relation
Nature of the use case
The use case aims to verify the functional requirements of the cyber security risk assessment tool.
Further keywords for classification

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.



3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	System Operator	A party that is responsible for a stable power system operation (including the organisation of physical balance) through a transmission grid in a geographical area. The System Operator will also determine and be responsible for cross border capacity and exchanges. If necessary, he may reduce allocated capacity to ensure operational stability. Transmission as mentioned above means “the transport of electricity on the extra high or high voltage network with a view to its delivery to final customers or to distributors. Operation of transmission includes the tasks of system operation as well concerning its management of energy flows, reliability of the system and availability of all necessary system services”. (Definition taken from the ENTSO-E RGCE Operation handbook Glossary).	Pilot site to provide information regarding the target environment. This includes: <ul style="list-style-type: none"> • List of assets of the selected target environment • Value of assets for the organization • Threats related to the target environment Deployed security measures
Grouping		Group description	
R2D2 actor			
Actor name	Actor type	Actor description	Further information specific to this use case
Task 3.1 partners (CYBER, ICCS etc.)	Cyber Security Experts	The parties responsible for conducting the risk assessment using the C3PO Cyber Security Risk Assessment Tool.	Utilize information provided by pilot site personnel to conduct the risk assessment for the target environment using the Cyber Risk Assessment Tool and propose mitigation measures.

D2.3 - Requirements and Detailed Architecture Design

C3PO Cyber Risk Assessment Tool	Application	The tool designed to perform Cyber Risk Assessment on EPES organizations	The System will be used by the Pilot Sites to assess their risk levels and receive mitigation measures
---------------------------------	-------------	--	--

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link
1	Publication relevant to RA best practices	NIST Risk Management Framework		It can be used as a source for established Risk Management methodologies.	NIST	NIST Risk Management Framework CSRC
2	Compliance Requirements	Minimum Security Measures for Operators of Essentials Services		It can be used to establish relevant compliance requirements applicable to the EPES environment.	ENISA	Minimum Security Measures for Operators of Essentials Services — ENISA (europa.eu)
3	Compliance Requirements	COMMISSION RECOMMENDATION of 3.4.2019 on cybersecurity in the energy sector		It can be used to establish relevant cybersecurity compliance requirements of the EU toward energy providers.	EUROPEAN COMMISSION	COMMISSION RECOMMENDATION of 3.4.2019 on cybersecurity in the energy sector
4	Publication relevant to RA best practices	Interoperable EU Risk Management Framework		It can be used to provide comparable results calculated in Use Case 38 with other Pilot Site assessments and previous attempts.	ENISA	Interoperable EU Risk Management Framework — ENISA (europa.eu)
5	Publication relevant to RA best practices	Cybersecurity Capability Maturity Model (C2M2)		It can be used as a resource for the assessment of the cybersecurity posture of the pilot sites	Office of Cybersecurity, Energy Security, and Emergency Response	Cybersecurity Capability Maturity Model (C2M2) Department of Energy

D2.3 - Requirements and Detailed Architecture Design

6	Directive	Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)		The Risk Assessment tool will be in line with the requirements set by the NIS2 Directive with respect to the risk management strategies adopted by operators of essential services. It will also contribute to setting or assessing the cybersecurity baseline for organizations	EU	https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0122
---	-----------	--	--	--	----	---

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Conduct overall risk assessment on target EPES environment	The Cyber Risk Assessment Tool will be used to identify, assess and evaluate risks on the selected target environment(s), and propose appropriate mitigation measures.	C3PO Cyber Risk Assessment Tool	Default Scenario	Pilot site(s) provides essential information: 1. IT and OT Assets inventory 2. Possible Threats 3. Deployed measures	
2	Conduct attack-specific risk assessment on target EPES environment	The Cyber Risk Assessment Tool will be used to identify, assess risk levels on the selected target environment(s) against specific security incidents/attacks, and propose appropriate mitigation measures.	C3PO Cyber Risk Assessment Tool	Default Scenario	Pilot site(s) provides essential information: 1. IT and OT Assets inventory 2. Possible Threats 3. Deployed measures	

4.2 Steps – Scenarios

Scenario								
Scenario name:		Conduct overall risk assessment on target EPES environment						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Use case initiation	Context establishment	The actors have to frame the target environment and identify involved assets	Identify the target environment	Task 3.1 partners, Pilot site	C3PO Cyber Risk Assessment Tool	1, 2, 7	1
2	Context Established	Asset Valuation and System Modelling	The Pilot Site will provide information regarding the value of the identified assets with respect to the associated impacts, and the relations between the assets.	Asset Valuation and System Modelling	Pilot Site	C3PO Cyber Risk Assessment Tool	3, 4	2
3	Assets Modelled	Risk scenarios development.	Associated threats and vulnerabilities of the target environment are identified, and risk scenarios are developed.	Risk scenarios development.	Task 3.1 partners, Pilot site	C3PO Cyber Risk Assessment Tool	5	3
4	Risk Scenarios Developed	Risk Assessment	Having Identified the risk scenarios, the C3PO Cyber Risk Assessment Tool will be used to assess risks for the target environment.	Provide risk assessment results and mitigation measures	C3PO Cyber Risk Assessment Tool	Pilot Site	5, 6	4

D2.3 - Requirements and Detailed Architecture Design

5	Risk Assessment Performed	Risk evaluation and treatment	The Pilot Site evaluates the assessment results and mitigation measures are proposed for risk treatment.	Risk treatment	C3PO Cyber Risk Assessment Tool	Pilot Site	8	5
---	---------------------------	-------------------------------	--	----------------	---------------------------------	------------	---	---

Scenario								
Scenario name:		Conduct attack-specific risk assessment on target EPES environment						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Use case initiation	Context establishment	Identify assets related to the attack scenarios in the organization's target environment	Identify the target environment	Task 3.1 partners, Pilot site	C3PO Cyber Risk Assessment Tool	1, 2, 7	
2	Context Established	Asset Valuation and System Modeling	The Pilot Site will provide information regarding the value of the identified assets with respect to the associated impacts, and the relations between the assets.	Asset Valuation and System Modeling	Pilot Site	C3PO Cyber Risk Assessment Tool	3, 4	
3	Assets Modeled	Risk scenarios development.	Associated threats and vulnerabilities of the target environment are identified, and risk scenarios are developed for the specific attack scenarios.	Risk scenarios development.	Task 3.1 partners, Pilot site	C3PO Cyber Risk Assessment Tool	5	

D2.3 - Requirements and Detailed Architecture Design

4	Risk Scenarios Developed	Risk Assessment	Having Identified the risk scenarios, the C3PO Cyber Risk Assessment Tool will be used to assess risks for the target environment.	Provide risk assessment results and mitigation measures	C3PO Cyber Risk Assessment Tool	Pilot Site	5, 6	
5	Risk Assessment Performed	Risk evaluation and treatment	The Pilot Site evaluates the assessment results and mitigation measures are proposed for risk treatment.	Risk treatment	C3PO Cyber Risk Assessment Tool	Pilot Site	8	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Applicable standards, legislation, regulations and industry best practices	The Pilot site shall communicate all applicable legislation, regulations and industry best practices that should be considered during the risk assessment process for the selected target environment.	
2	Asset	The Pilot Site shall provide a complete list of assets of the selected target environment	
3	Impacts	The Pilot Site shall provide information about the impact on the organization if an asset is subject to a security incident.	
4	Asset Modelling	Information describing the layout and interconnection of the various Assets of the Pilot Site (Target environment architecture)	
5	Risk scenarios	A complete list of risk scenarios for the target environment, considering assets, potential threats and vulnerabilities	

D2.3 - Requirements and Detailed Architecture Design

6	Risk Assessment Results	The results of the conducted risk assessment for the risk scenarios	
7	Existing measures	The list of security measures deployed in the target environment	
8	Mitigation Measures	The results of the RA calculation performed by the system and the mitigation measures provided by the system to manage the risks that exceed the acceptable levels. If the lack of existing security measures is unknown, the tool will provide mitigation measures for the inherent risks.	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.25 USE CASE 25 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
25	Transmission, Distribution / Enterprise, Station	Dynamic Cyber-Risk Status Evaluation considering existing technical vulnerabilities

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	28/2/2023	Cyber Noesis (CYBER)		
0.2	21/4/2023	Cyber Noesis (CYBER)		Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Conduct Dynamic Risk Assessment to improve the cyber security posture of the organization
Objective(s)	The aim is to deploy the Dynamic Cyber-Risk Evaluation Tool developed in T3.2 to <ul style="list-style-type: none"> dynamically assess cybersecurity risks by considering collected and analyzed cyber threats and technical vulnerabilities reported about the environment suggest mitigation measures
Related business case(s)	BC3

1.4 Narrative of use case

Narrative of use case	
Short description	
The C3PO Dynamic Cyber Risk Evaluation Tool will facilitate the dynamic and close to real-time threat detection and mitigation as well as vulnerability management in the targeted IT/OT environment, by (proactively) assessing associated risks for the organization's target environment.	
Complete description	
<p>The C3PO Dynamic Cyber Risk Evaluation Tool will combine the asset inventory and their corresponding values, that will be provided by the Asset Management Toolkit (T6.2) and/or the C3PO Cyber Risk Assessment Tool (UC 24), the technical Vulnerability Assessment tool, and the Deep learning data analytics for security tool (UC 24, 35), to generate risk scoring for critical assets along with mitigation suggestions.</p> <p>The Dynamic Risk Analysis will assist the organisation to confront existing and emerging threats aiming to exploit vulnerabilities identified in the target environment and propose the appropriate mitigation measures to maintain the security posture of the organisation to an acceptable level.</p> <p>The developed tool will address the requirements of the converged IT-OT environment, and therefore, the threats and vulnerabilities that are also associated with the OT environment.</p> <p>In contrast to the static risk assessment that will be demonstrated by UC24 (C3PO Cyber Risk Assessment Tool), the dynamic risk assessment does not consider generic threats, like unauthorized access and user errors, that are usually addressed by a typical risk assessment method, but more technical existing and emerging threats and (newly) identified technical vulnerabilities, to assess the criticality of a technical vulnerability and the likelihood of a threat actor attacking an organisation's asset and conducting a malicious activity. Based on the assessed parameters and on the potential impact to the organization should such an attack materialize, the dynamic risk assessment toll will calculate associated risk levels and be able to provide close to real-time visibility about the organisation's security posture.</p>	

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Pilot Sites availability: Xanthi
Prerequisites
Information about the target environment (assets, impact, infrastructure).
Deployment of a Vulnerability Assessment tool in the target environment.
R2D2 components that provide input to the Dynamic Risk Assessment tool (Deep learning data analytics, Asset management toolkit) should be deployed to the same environment.
Interfaces with the Asset Management Toolkit (T6.2) and the “Deep learning data analytics for security” tool (T5.4)

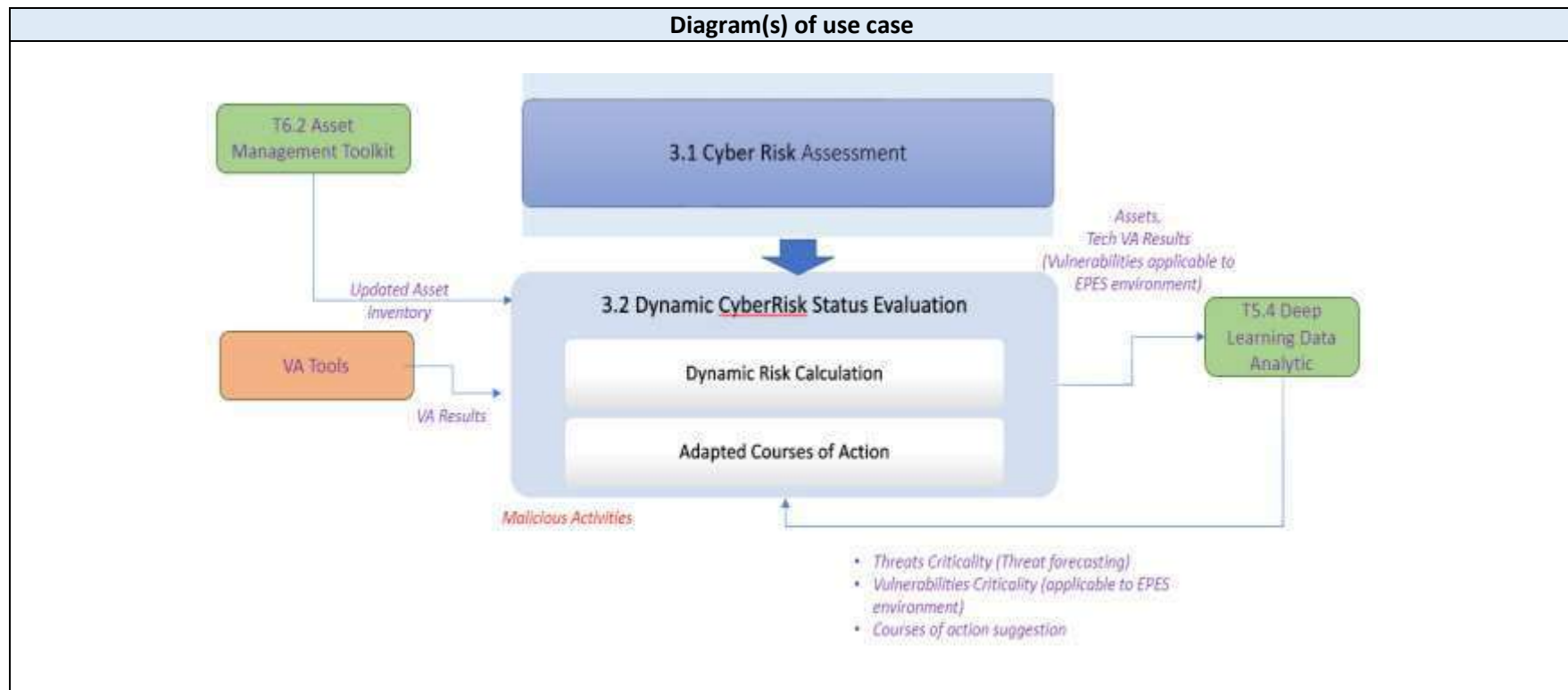
1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
Cyber Threat Intelligence knowledge collection/sharing with external sources (UC 26)
Level of depth
High
Prioritization
4
Generic, regional or national relation
Nature of the use case
The use case aims to utilize the C3PO Dynamic Cyber Risk Evaluation Tool to support EPES in assessing risks in their IT/OT environment in a dynamic manner, and close to real time
Further keywords for classification

1.8 General remarks

General remarks

2. Diagrams of use case



SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Pilot Site	System Operator	A party that is responsible for a stable power system operation (including the organisation of physical balance) through a transmission grid in a geographical area. The System Operator will also determine and be responsible for cross border capacity and exchanges. If necessary, he may reduce allocated capacity to ensure operational stability. Transmission as mentioned above means “the transport of electricity on the extra high or high voltage network with a view to its delivery to final customers or to distributors. Operation of transmission includes the tasks of system operation as well concerning its management of energy flows, reliability of the system and availability of all necessary system services”. (Definition taken from the ENTSO-E RGCE Operation handbook Glossary).	<p>Pilot site to provide information regarding the target environment. This includes:</p> <ul style="list-style-type: none"> List of assets of the selected target environment Value of assets for the organization Threats related to the target environment <p>Deployed security measures</p>

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
Deep Learning Data Analytics	Software	The deep learning analytics system is an intelligent actor that is designed to process large amounts of data and identify patterns and trends that are not easily observable by humans. As an actor, the system has the ability to learn and adapt over time, using advanced algorithms and neural networks to continually improve its performance. The system is proactive in its approach, continuously processing data in real-time and providing insights that can be used	The deep learning system supports risk management by analyzing data, identifying patterns and trends, providing predictive insights, and enabling real-time monitoring and alerts. It improves the accuracy and

D2.3 - Requirements and Detailed Architecture Design

		to make better decisions. It has the ability to interact with other systems, exchanging information and providing feedback to enhance the accuracy and effectiveness of the overall system. The deep learning analytics system is a valuable actor in a variety of applications, providing accurate and timely information to support a wide range of decision-making processes.	efficiency of risk assessments and helps make informed decisions to manage risks effectively.
Cyber Threat Intelligence Collection/Sharing System	Software	A piece of software designed to collect, analyse, organize, and share CTI information relevant to the EPES environment.	The system is responsible for receiving CTI information from external sources and forwarding it to the Pilot Site defence systems and the Deep Learning tool. The system is also responsible for collecting information generated by the Pilot Site protection mechanisms, analysing it, and sharing it with other partners, or with the public, as open-source intelligence.
Vulnerability Assessment Tool	Software	A software tool to scan a collection of systems to identify, quantify, and prioritize any technical vulnerabilities	A vulnerability assessment tool will be used in the Pilot's site network or part of the network to review the cyber security weaknesses. It will evaluate the systems against known vulnerabilities, assign severity levels, and propose remediation actions
Task 3.2 partners	Cyber Security Experts	The parties responsible for managing the C3PO Cyber Security Risk Assessment Tool.	Utilize information provided by pilot site personnel to initialize and customize the system for the target environment.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link
1	Publication relevant to RA best practices	NIST Risk Management Framework		The document can be used as a source for established Risk Management methodologies.	NIST	NIST Risk Management Framework CSRC
2	Compliance Requirements	Minimum Security Measures for Operators of Essentials Services		The document can be used to establish relevant compliance requirements applicable to the EPES environment.	ENISA	Minimum Security Measures for Operators of Essentials Services — ENISA (europa.eu)
3	Compliance Requirements	COMMISSION RECOMMENDATION of 3.4.2019 on cybersecurity in the energy sector		The document can be used to establish relevant cybersecurity compliance requirements of the EU toward energy providers.	EUROPEAN COMMISSION	COMMISSION RECOMMENDATION of 3.4.2019 on cybersecurity in the energy sector

D2.3 - Requirements and Detailed Architecture Design

4	Publication relevant to RA best practices	Interoperable EU Risk Management Framework		The document can be used to establish the best way to network the system described in Use Case 38 with other R2D2 systems and any existing Pilot Site systems.	ENISA	Interoperable EU Risk Management Framework — ENISA (europa.eu)
5	Publication relevant to RA best practices	Cybersecurity Capability Maturity Model (C2M2)		The document can be used as a resource when creating the dynamic risk assessment toolkit	Office of Cybersecurity, Energy Security, and Emergency Response	Cybersecurity Capability Maturity Model (C2M2) Department of Energy
6	Publication relevant to Dynamic Risk Management	Leveraging cyber threat intelligence for a dynamic risk framework		The document can be used as a resource when creating the dynamic risk assessment toolkit	Universidad Politécnica de Madrid	https://oa.upm.es/63893/1/INVE MEM 2019 321228.pdf

D2.3 - Requirements and Detailed Architecture Design

7	Publication relevant to Dynamic Risk Management	Synthesis of the System of Iterative Dynamic Risk Assessment of Information Security		The document can be used as a resource to design the dynamic risk assessment toolkit	CEUR Workshop Proceedings (CEUR-WS.org)	https://ceur-ws.org/Vol-3188/paper13.pdf
8	Publication relevant to Dynamic Risk Management	Dynamic risk management		The document can be used as a resource to design the dynamic risk assessment toolkit	https://patents.google.com/	https://patents.google.com/patent/US7908660B2/en
10	Publication relevant to Dynamic Risk Management	Dynamic Risk Assessment and Analysis Framework for Large-Scale Cyber-Physical Systems		The document can be used as a resource to design the dynamic risk assessment toolkit	The University of Texas at El Paso European Union Digital Library	https://eudl.eu/doi/10.4108/eai.25-1-2022.172997

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Conduct dynamic risk assessment on target EPES environment	Provide Dynamic Risk Assessment capabilities on the targeted environment to assess and mitigate risks related to new existing and emerging threats aiming to exploit vulnerabilities identified at the target environment.	C3PO Cyber Security Risk Assessment Tool	Default Scenario	1. IT and OT Assets inventory of the target environment 2. Cyber Threat Intelligence Tool 3. Deep Learning Analytics 4. Vulnerability Assessment results	

4.2 Steps – Scenarios

Scenario								
Scenario name:		Conduct dynamic risk assessment on target EPES environment						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Use case initiation	Context establishment	Frame the target environment and identify involved assets and existing measures	Identify the target environment	Task 3.2 partners, DSO	C3PO Dynamic Cyber Risk Evaluation Tool	1	
2	Established target	Source systems integration	Source systems are integrated with the Dynamic Risk Evaluation tool to provide the required information to conduct the assessments and deployed to the	Dynamic Risk Evaluation data feed provision	DSO T6.2 Asset Management Toolkit T3.1 Cyber Risk Assessment T5.4 Deep Learning Data Analytic	C3PO Dynamic Cyber Risk Evaluation Tool	1,2,3,4	

D2.3 - Requirements and Detailed Architecture Design

			target environment		Vulnerabilities Assessment tools			
3	System Integrated	System initialization	The system instance is provided with the target environment's information i.e., assets, criticality, security measures.	System initialization	Task 3.2 partners, DSO	Task 3.2 partners, DSO	1, 4	
4	System Initialized	Vulnerabilities Identification	Vulnerability assessment tool will be used to identify pilot site's target network to evaluate existing technical vulnerabilities and feed	Vulnerabilities Identification	VA Tool	C3PO Dynamic Cyber Risk Evaluation Tool	2	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	IT & OT assets inventory input	Information regarding the currently deployed assets, IT and networking equipment as well as other applicable information of the Pilot Site, including deployed measures.	
2	VA results	Results from the technical vulnerability assessments	
3	Deep learning data analytics	Analytics from the T5.4 Deep Learning component – Threats likelihood, Vulnerabilities criticalities, Courses of action suggestion	
4	Assets Value	Asset Value is available from the Cybersecurity Risk Assessment Tool and/or via manual input	
5	Risk Scoring	Risks are being calculated for cyber threats that aim to exploit identified vulnerabilities.	
6	Adapted courses of action	Based on the scoring and the data provided, courses of action are suggested	



6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.26 USE CASE 26 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
26	Transmission, Distribution / Enterprise	Cyber Threat Intelligence knowledge collection/sharing with external sources

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	21/4/2023	Cyber Noesis (CYBER)		Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Establish a Cyber Threat Intelligence (CTI) Collection and Sharing system, to collect CTI from external sources but also share any relevant events observed internally.
Objective(s)	<ul style="list-style-type: none"> • Provide a user-friendly, sustainable, and reliable way to receive relevant threat intelligence data from external sources, to be used with other R2D2 components to improve the security of EPES' OT and IT systems. • Establish communication channels for sharing with the community information about security events observed on EPES infrastructure, to expand collective knowledge.
Related business case(s)	BC4

1.4 Narrative of use case

Narrative of use case
Short description
Demonstrate the capabilities of the CTI Tool (T3.6) in collecting, correlating, producing added-value data ready to be ingested by security appliances and further disseminating CTI.
Complete description
<p>This UC will deploy the Cyber Threat Intelligence Collection and Sharing System to the Pilot Site environment, to both gather and provide CTI. This process entails the following steps:</p> <ol style="list-style-type: none"> 1. CTI Source Establishment: Identify CTI sources relevant to the EPES context. 2. Information Recipients Establishment: Identify external partners/channels that will receive information collected by the R2D2 system. 3. Establish Interfaces: Establish connections between the CTI Collection & Gathering system and the Pilot Site defense mechanisms. This will allow the CTI tool to receive Cyber-Security event information from the Pilot Site, and to inform the existing defense mechanisms of received information. <p>After successful deployment, the system will:</p> <ol style="list-style-type: none"> 1. Begin monitoring the information received by outside sources. Any information received will be analyzed and forwarded to other R2D2 modules to assist the creation of added value data. 2. Begin monitoring the information generated by the Pilot Site (chosen) defense mechanisms. The information provided by other R2D2 modules will be further processed to render it secure, for example, sanitize it, and then shared, either with pre-selected partners or as open-source intelligence.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Pilot Sites availability: Xanthi (HEDNO)
Prerequisites
Cyber-threat information sharing policy by participating pilot sites

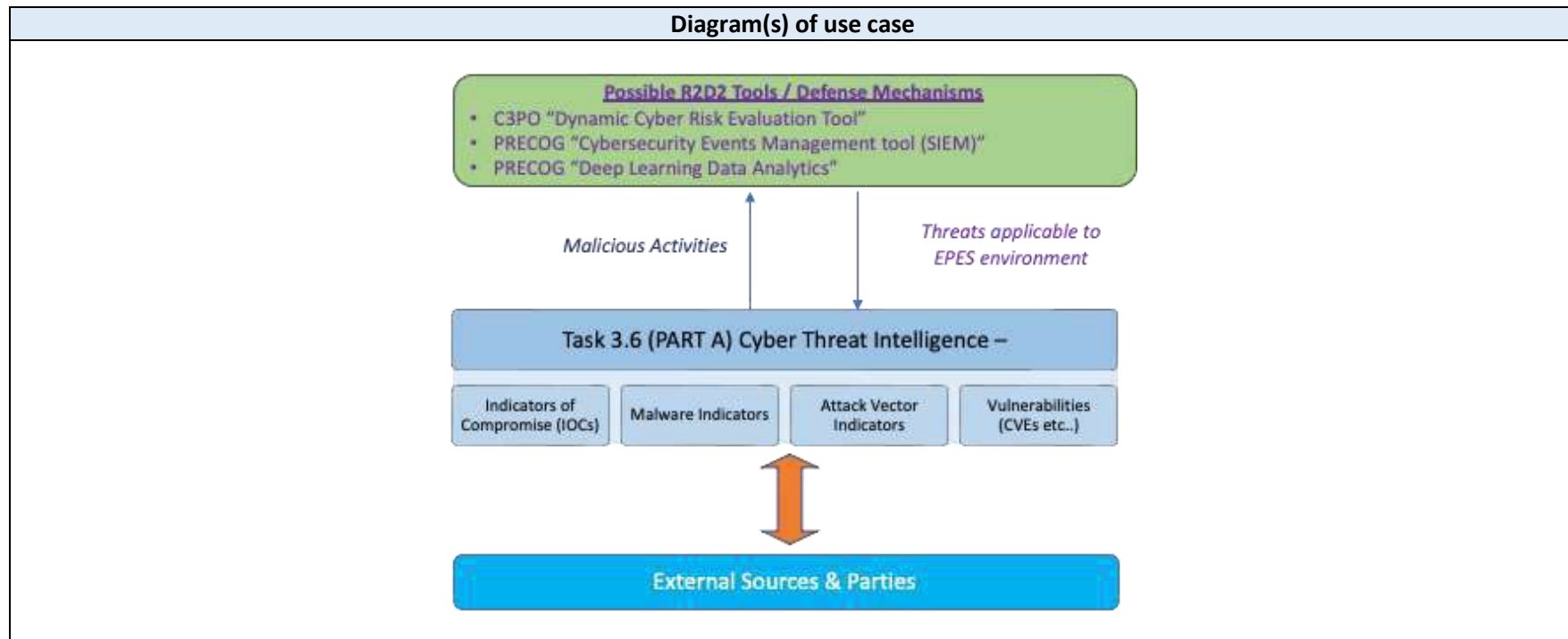
1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
<ol style="list-style-type: none"> 1. Provide threat intelligence information to C3PO “Dynamic Cyber Risk Evaluation Tool” (UC 25) and/or PRECOG “Cybersecurity Events Management tool (SIEM)” (UCs 33, 34) 2. Receive threat intelligence on Cyber Attacks detected using PRECOG Tools (e.g. Deep Learning Data Analytic – UC 35) and disseminate to the community. <p>Optionally, receive information on the asset inventory of the pilot site from Asset Management Toolkit – (use cases 2,4,6)</p>
Level of depth
High
Prioritization
High
Generic, regional, or national relation
Generic Relation
Nature of the use case
The use case aims to describe the functional requirements of the threat intelligence sharing and management system to be developed
Further keywords for classification

1.8 General remarks

General remarks

2. Diagrams of use case



SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Pilot Site	System Operator	A party that is responsible for a stable power system operation (including the organization of physical balance) through a transmission grid in a geographical area. The System Operator will also determine and be responsible for cross-border capacity and exchanges. If necessary, he may reduce allocated capacity to ensure operational stability. Transmission as mentioned above means “the transport of electricity on the extra high or high voltage network with a view to its delivery to final customers or to distributors. Operation of transmission includes as well the tasks of system operation concerning its management of energy flows, reliability of the system and availability of all necessary system services.” (Definition taken from the ENTSO-E RGCE Operation handbook Glossary).	Establish interface between existing security systems and the threat intelligence sharing system.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
C3PO CTI Tool (Cyber Threat Intelligence Collection/Sharing System)	Software Solution	A software solution designed to collect, correlate, analyze, organize, and disseminate CTI information relevant to the EPES environment.	The system is responsible for receiving CTI information from external sources and forwarding it to the Pilot Site defense systems and the Deep Learning tool. Additionally, it will collect information generated by the Pilot Site protection mechanisms, analyze it, and share it with other partners, or with the public, as open-source intelligence.
R2D2 Defence Mechanisms	Software Solution	R2D2 Tools like	
	C3PO "Dynamic Cyber Risk Evaluation Tool"		
	PRECOG "Cybersecurity Events Management tool (SIEM)"		

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link
1	Regulatory Framework	DIRECTIVE (EU) 2022/2555		The document can be used to establish relevant cybersecurity compliance requirements and regulations regarding Cyber Security	European Parliament and European Council	https://eur-lex.europa.eu/eli/dir/2022/2555/oj
2	Regulatory Framework	Network Code on sector-specific rules for cybersecurity aspects of cross border electricity flows (NCCS)		The document can be used to establish relevant cybersecurity compliance requirements and regulations regarding Cyber Security, aimed specifically toward Electricity Providers	ACER	Network Code on sector-specific rules for cybersecurity aspects of cross border electricity flows (NCCS)
3	Methodology	ENISA CYBERSECURITY THREAT LANDSCAPE METHODOLOGY		Methodology, by ENISA aiming to set a baseline for the transparent and systematic delivery of horizontal, thematic, and sectorial cybersecurity threat landscapes.	ENISA	https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology



4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Receive CTI from external sources for the needs of R2D2	The Intelligence Gathering and Sharing system will receive CTI information, related to Pilot's Assets and share CTI with the Pilot Site defense systems.	C3PO Cyber Threat Intelligence Collection/Sharing System	Default Scenario	Establish CTI communication with external sources.	
2	Share CTI with external sources	Disseminate CTI detected from the Pilot Site defense mechanisms to the selected external partners and/or to the public.	C3PO Cyber Threat Intelligence Collection/Sharing System	Default Scenario	Establish CTI communication with external sources.	

4.2 Steps – Scenarios

Scenario								
Scenario name:		Share CTI with external sources						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Use Case Initiation	CTI Sources Connections Establishment	<p>C3PO CTI Tool, in cooperation with the Pilot Site will create and maintain a curated list of CTI sources, to be used in the system.</p> <p>The system is deployed, and interfaces are established between the system, and R2D2 defense mechanisms and the selected external CTI sources and optionally with the asset management tool (T6.2).</p>	CTI sources identification and connections with other components	CTI Sources	C3PO CTI Tool	1	
2	CTI Sources Connections Establishment	CTI Collection	The system collects pertinent CTI data from external sources.	CTI collection	CTI Sources	C3PO CTI Tool	2	



D2.3 - Requirements and Detailed Architecture Design

3	CTI Collection	CTI Analysis & Internal Dissemination	The system filters CTI data collected from external sources and correlates them to the relevant assets, and forwarded to other R2D2 Defense Mechanisms.	Relevant CTI information provided to R2D2 components.	C3PO CTI Tool	R2D2 Defense Mechanisms	2	3
---	----------------	---------------------------------------	---	---	---------------	-------------------------	---	---

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Share CTI with external sources						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Use Case Initiation	CTI Sources Connections Establishment	C3PO CTI Tool, in cooperation with the Pilot Site will create and maintain a curated list of CTI sources, to be used in the system. The system is deployed, and interfaces are established between the system, and R2D2 defense mechanisms and the selected external CTI sources and optionally with the asset management tool (T6.2).	CTI sources identification and connections with other components	CTI Sources	C3PO CTI Tool	1	
2	CTI Sources Connections Establishment	CTI Collection	The system collects pertinent CTI data from R2D2 defense mechanisms.	CTI collection	R2D2 defense mechanisms	C3PO CTI Tool	3	



D2.3 – Requirements and Detailed Architecture Design

3	CTI Collection	CTI Analysis & External Dissemination	The system filters CTI data collected from R2D2 Defense Mechanisms, sanitize them, prepares, and disseminates them to CTI Sources.	Relevant CTI information provided to external CTI Sources.	C3PO CTI Tool	CTI Sources	3	3
---	----------------	---------------------------------------	--	--	---------------	-------------	---	---

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	List of relevant CTI sources and external partners	CYBER will establish a list of CTI sources that provide information relevant to the EPES environment, and a list of external partners to receive information regarding observed security events.	
2	CTI information	Cyber Threat Intelligence data from various external or internal sources.	
3	Produced CTI information	Information regarding threats on the Pilot Site ecosystem is analyzed, filtered, sanitized (to protect sensitive information) and shared to other CTI sources.	



6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.27 USE CASE 27 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
27		Monitor communications behavior of newly deployed components

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	7/4/2023	Cyber Noesis (CYBER)		
0.2	21/4/2023	Cyber Noesis (CYBER)		
0.3	18/5/2023	GUARD	Final phase of UC review, new comments and changes added	Approved
0.4	22/05/2023	GUARD	Revision done	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Monitoring communications of newly deployed components to detect and prevent abnormal or malicious behavior of newly deployed components.
Objective(s)	<ul style="list-style-type: none"> - Identify and track potential cyber threats posed by new components. - Detect misconfigurations or vulnerabilities on newly deployed components before they can be exploited. - Take measures to mitigate detected threats.
Related business case(s)	BC3

1.4 Narrative of use case

Narrative of use case
<p>Short description</p> <p>The aim of this use case is to demonstrate the capabilities of the “Sandbox Tool” of the PRECOG Supply Chain Assessment Toolkit (T5.5 - Device Origin and Supply Chain Toolkit), and its ability to monitor the communication of newly deployed components, and to use them to classify them as safe or unsafe prior to deployment in a production environment.</p>
<p>Complete description</p> <p>This UC will deploy the Communications Monitoring System to the Pilot Site environment to assess the safety of new components, by monitoring their communications. This process entails:</p> <ol style="list-style-type: none"> 1. <u>Sandbox Tool Deployment</u>: A new component is deployed in the staging or test environment provided by the Pilot Site. This environment should allow the component to emulate normal operations, without interacting with the production environment. 2. <u>Communications Monitoring</u>: During Sandbox Tool operation, the communications of the component are monitored by the R2D2 SIEM (T5.3). 3. <u>Communications Analysis</u>: The captured communications are analyzed, with the help of the Deep Learning module (T5.4), to detect abnormalities and use them to classify the component as safe or unsafe. 4. <u>Blockchain</u>: Assessment results of the deployed components will be signed with the utilization of the blockchain technology. Having assessed the component, the signatures will be safely stored in a registry database, available to the Pilots community, as additional proof of the component’s integrity. <p>These steps will be performed in close cooperation with the involved partners and the Pilot Sites. Each Pilot Site will provide information of new assets deployment method into their environment, as well as new components provision process in a sandbox environment, assisted by the technical experts. After the testing process, the Pilot Sites will receive the results and the assessment results for the new components.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Pilot Sites: Xanthi
Pilot site able to offer/set-up a staging environment (e.g., a test bed)
Prerequisites
Information on pre-existing assets (and connectivity between them)
Information on the procedures followed by the pilot when deploying new components

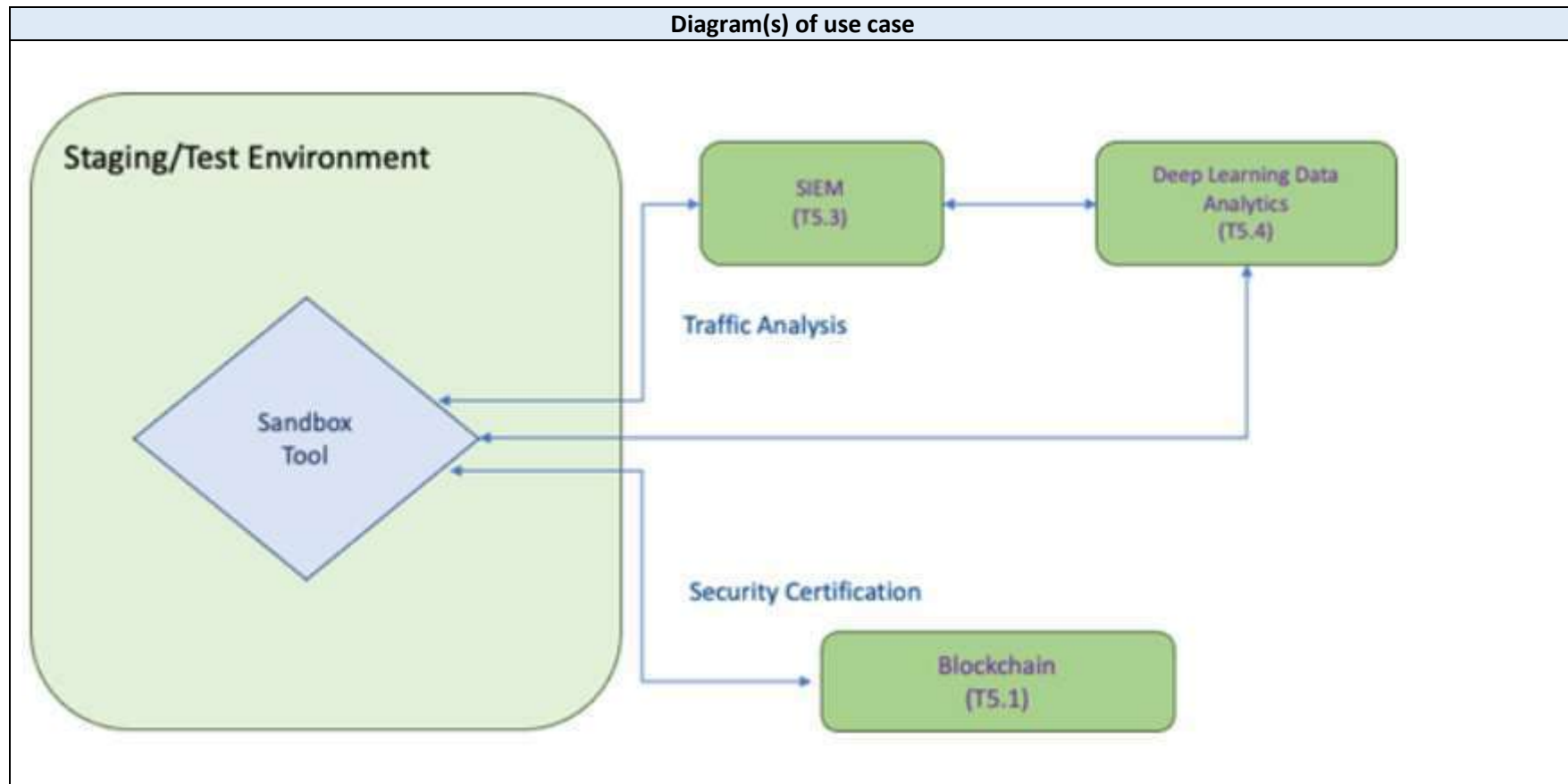
1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC33, UC34
Level of depth
Medium
Prioritization
Generic Relation
Nature of the use case
The use case aims to describe the functional requirements of the communication monitoring system for new components.
Further keywords for classification

1.8 General remarks

General remarks

2. Diagrams of use case



SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	System operator	A party that is responsible for a stable power system operation (including the organisation of physical balance) through a transmission grid in a geographical area. The System Operator will also determine and be responsible for cross border capacity and exchanges. If necessary, he may reduce allocated capacity to ensure operational stability. Transmission as mentioned above means “the transport of electricity on the extra high or high voltage network with a view to its delivery to final customers or to distributors. Operation of transmission includes the tasks of system operation as well concerning its management of energy flows, reliability of the system and availability of all necessary system services”. (Definition taken from the ENTSO-E RGCE Operation handbook Glossary).	The pilot site (DSO) will provide a test/staging environment to test the newly deployed components. The Pilot Site will use the Sandbox Tool to test the communications of all newly deployed components.

Grouping		Group description	
R2D2 Actors			
Actor name	Actor type	Actor description	Further information specific to this use case
Sandbox Tool	Software	The tool is responsible for monitoring, analyzing, and assessing the integrity of newly deployed components.	Monitor the communications in the given staging environment, analyze

D2.3 - Requirements and Detailed Architecture Design

		Furthermore the tool stores the signatures of the classified software.	the traffic using T5.4 tool, assess the security of the component, register the results in T5.1 blockchain
Communications Monitoring System (SIEM)	Software	A piece of software responsible for monitoring the communications of newly deployed components in the sandbox environment (T5.3).	The system will monitor the communications of the newly deployed components while they are deployed in the sandbox environment and pass them to the Deep Learning System for evaluation.
Deep Learning System	Software	The Deep Learning System will be developed in Task 5.4. It will be used to analyze the monitored communications of the newly deployed components.	In this use case, the Deep Learning System will analyze the information collected by the Communications Monitoring System and use it to classify the component as safe or unsafe.
Blockchain	Software	The Blockchain technology described in T5.1	The blockchain will be used to sign the results regarding the classification of the newly deployed components as safe or unsafe.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link
1	Cyber-Security best practices publication	ISA/IEC 62443 Series of Standards		The ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). These standards set best practices for security and provide a way to assess the level of security performance. Thus, they can be utilized when monitoring the communication of newly deployed components.	International Society of Automation	ISA/IEC 62443 Series of Standards - ISA
2	Directive	DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL		The document can be used to establish relevant cybersecurity compliance requirements and regulations regarding Cyber Security.	European Parliament and European Council	Publications Office (europa.eu)

D2.3 - Requirements and Detailed Architecture Design

3	Cyber-Security best practices publication	SP 800-82 Rev. 2 -Guide to Industrial Control Systems (ICS) Security		The document describes the currently established best practices regarding the cyber security of ICS.	NIST	SP 800-82 Rev. 2, Guide to Industrial Control Systems (ICS) Security CSRC (nist.gov)
4	Cyber-Security best practices publication	Supply Chain Assurance		A set of guidelines regarding how organizations can verify that the internal components and system firmware of the computing devices they acquire are genuine and have not been unexpectedly altered during manufacturing, distribution, or operational use	NIST	https://www.nccoe.nist.gov/supply-chain-assurance
5	Framework for supply chain security	System of Trust Framework		A comprehensive, consistent, and repeatable supply chain security risk assessment process	MITRE	https://sot.mitre.org/

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Communications Monitoring and Classification	The Communications Monitoring System is implemented and deployed in the Pilot Site environment.	Pilot Site	Default Scenario	The Pilot Site shall provide a test environment, to safely test the newly deployed components. Other modules (T5.4, T5.1) able to be used in conjunction with the Communications Monitoring System must be deployed on the same site.	The component in question is assessed and results about its integrity (VALID, SUSPICIOUS, COMPROMISE) are produced.



D2.3 - Requirements and Detailed Architecture Design

4.2 Steps – Scenarios

Scenario								
Scenario name:		Communications Monitoring and Classification						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	New Component Deployed	Communications monitoring of newly deployed component	When deploying a new component, it will be first deployed in the test environment i.e., a staging or test environment of the pilot site, where the System will monitor its communications and provide them to the Deep Learning System for evaluation	Communications monitor	Communications Monitoring System (SIEM)	Deep Learning System	1	

D2.3 - Requirements and Detailed Architecture Design

2	New component behavior analysis results	Deep Learning Analysis	After the new component's communications have been collected it will be sent to the Deep Learning System to classify it as safe or unsafe.	Deep Learning	Deep Learning System	Sandbox Tool	1, 2	
3	Classification results	Blockchain registration	. Assessment results are hashed and registered in blockchain that returns an unique signature as cryptographic proof for further integrity validation.	Blockchain	Sandbox Tool	Blockchain	2	
4	Creation of classification results and proof	Storage	Store classification with associated proof to make them available to Pilots' community	Data storage	Blockchain, Deep Learning	Sandbox Tool	3	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Newly deployed component communications	Once a component is deployed on the staging or test environment, its communications are monitored and analyzed. This allows determining whether the new component is safe, before it is integrated in the Pilot Site infrastructure.	
2	Component assessment results	The assessment results of the newly deployed component.	
3	Blockchain proof	Cryptographic proof that contains information for data integrity validation. .	



6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.28 USE CASE 28 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
28		Adapt/Develop EPES specific vendor management & suppliers' audit practices

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	7/4/2023	CYBER NOESIS (CYBER)		
0.2	23/4/2023	CYBER NOESIS (CYBER)		
0.3	19/05/2023	GUARD	Final phase of UC review, new comments and changes added	
0.4	22/05/2023	GUARD	Revision done and UC accepted. Added some comments CYBER needs to work with.	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Use the EPES-specific vendor management & suppliers' audit practices guidelines to evaluate Pilot Site suppliers/vendors.
Objective(s)	Develop and/or adapt a set of EPES specific vendor management and supplier auditing practices and use them to evaluate the current practices to: O1. Prevent supply chain attacks. O2. Enhance trustworthiness in supplier practices. O3. Identify weaknesses in vendors' development and production practices and minimize exploitability
Related business case(s)	BC3

1.4 Narrative of use case

Narrative of use case
Short description
Demonstrate the use of the EPES specific vendor management & suppliers' audit practices to evaluate current practices and propose necessary enhancements.
Complete description
<p>This UC will deliver two sets of guidelines and assess the stakeholders best practices, based on the "Self-assessment Tool" of the PRECOG Supply Chain Assessment Toolkit (T5.5 - Device Origin and Supply Chain Toolkit).</p> <p>This UC will develop two sets of guidelines. One set for EPES specific to vendor management guidelines and one for suppliers to enhance the existing supply chain practices. This set of best practices and guidelines will be provided to relevant vendors, who will compare their current policies and practices against them assisted by a self-assessment tool. Additionally, a self-assessment tool will be available to EPES to compare their status against the available guidelines. The guidelines will be shared to the Pilot Site(s), helping them evaluate their vendors.</p> <p>Completing the steps described this use case will demonstrate the use of a self-assessment tool which aims to:</p> <ul style="list-style-type: none"> • Prevent supply chain attacks. • Enhance trustworthiness in supplier practices. • Identify weaknesses in vendor's development and production practices and minimize exploitability.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Pilot Sites: Xanthi (staging environment supported by ICCS)
Pilot Site and Vendors can perform self-assessment and share the results
Prerequisites

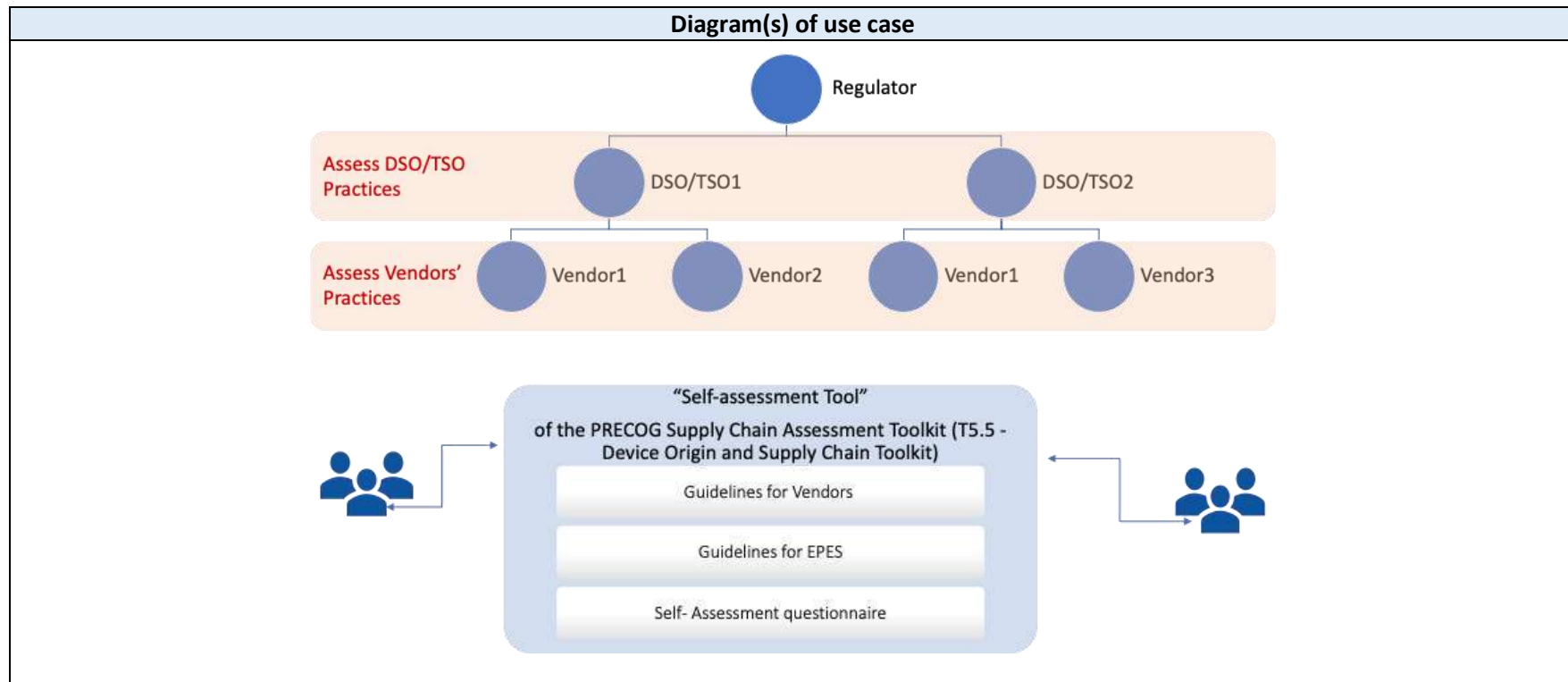
1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
Level of depth
High
Prioritization
Generic, regional or national relation
Generic Relation
Nature of the use case
Business/industrial use case
Further keywords for classification

1.8 General remarks

General remarks

2. Diagrams of use case



SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	System Operator	A party that is responsible for a stable power system operation (including the organisation of physical balance) through a transmission grid in a geographical area. The System Operator will also determine and be responsible for cross border capacity and exchanges. If necessary, he may reduce allocated capacity to ensure operational stability. Transmission as mentioned above means “the transport of electricity on the extra high or high voltage network with a view to its delivery to final customers or to distributors. Operation of transmission includes as well the tasks of system operation concerning its management of energy flows, reliability of the system and availability of all necessary system services”. (Definition taken from the ENTSO-E RGCE Operation handbook Glossary).	The pilot site will provide a sandbox system (e.g., test bed) to test the newly deployed components. The Pilot Site will use the final system, created by CYBER, to test the communications of all newly deployed components.
Grouping		Group description	
Others actors			
Actor name	Actor type	Actor description	Further information specific to this use case
EPES representative	Human	The entity responsible for operating the self-assessment tool.	This entity will conduct the self-assessment and get the results on behalf of the EPES operator.

D2.3 - Requirements and Detailed Architecture Design

Vendors' / Suppliers' representatives	Human	Entities that manage EPES-related solutions.	In this context, the vendors are actors that provide the Pilot Site with infrastructure components.
Self-Assessment tool	Software	The tool that will be develop by T5.5 partners and used for the assessment of the supply chain practices used by vendors but also by Pilot Sites	

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link
1	Industry Best Practices	Best Practices in Cyber Supply Chain Risk Management		A set of best practices for cyber supply chain risk management. It includes a long list of potential questions to ask suppliers, vendors, and third parties about their cyber supply chain risk management system.	National Institute of Standards and Technology	Best Practices in Cyber Supply Chain Risk Management
2	Relevant Standard	ISO/IEC 27036		The document offers guidance on the management of information risks involved in the acquisition of ICT goods and services from suppliers	International Standards Organization	ISO/IEC 27036
3	Security Recommendations	SECURING THE SOFTWARE SUPPLY CHAIN : Recommendations for Developers		Provide guidance in line with industry best practices and principles, including topics like security requirements planning, designing software architecture from a security perspective, adding security features, and maintaining the security of software and the underlying infrastructure.	Cybersecurity and Infrastructure Security Agency	SECURING THE SOFTWARE SUPPLY CHAIN

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	EPES Evaluation against EPES-specific guidelines	The EPES specific vendors and suppliers' management and audit practices accompanied with a self-assessment tool to evaluate themselves against the guidelines.	EPES representative /Pilots	Default Scenario	Both the Pilot Site and the vendors perform self-assessment of their current practices	Best practices guidelines developed and implemented for the Pilot Site and evaluated through an assessment tool improving their security posture.
2	Vendor Evaluation against EPES-specific guidelines	EPES vendors guide-lines with industry best practices and principles regarding security requirements planning, designing, developing and maintaining software from a security perspective. The guidelines will be evaluated through a self-assessment tool.	EPES representative / Vendors-Suppliers	Default Scenario	Both the Pilot Site and the vendors perform self-assessment of their current practices	Best practices guidelines developed and implemented for the EPES vendors and evaluated through an assessment tool improving their security posture.
4	Security Recommendations	Supply chain security guidance		The document proposes a list of 12 principles, designed to help establish control and oversight of organizations supply chain.	National Cyber Security Centre	Supply chain security guidance

D2.3 – Requirements and Detailed Architecture Design

5	Cyber-Security best practices publication	Supply Chain Assurance		A set of guidelines regarding how organizations can verify that the internal components and system firmware of the computing devices they acquire are genuine and have not been unexpectedly altered during manufacturing, distribution, or operational use	NIST	https://www.nccoe.nist.gov/supply-chain-assurance
6	Framework for supply chain security	System of Trust Framework		A comprehensive, consistent, and repeatable supply chain security risk assessment process	MITRE	https://sot.mitre.org/

4.2 Steps – Scenarios

Scenario 1								
Scenario name:		EPES Evaluation against EPES-specific guidelines						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Scenario Initiation	Conduct self-assessment based on the provided guidelines to EPES	The EPES pilot will use the self-assessment tool to assess its own supply chain practices.	Provide input to the tool	Pilot Site (EPES representative)	Assessment tool	1	
2	Input provided	Input assessment	The provided input will be assessed against best practices and guidelines	Assess the input	Assessment tool	Assessment tool	2, 3	
3	Self-assessment performed	Assessment against Best Practices	The supply-chain security practices results are provided to the Pilot Site.	Assessment results	Assessment tool	Pilot Site (EPES representative)	3	

D2.3 - Requirements and Detailed Architecture Design

Scenario 2								
Scenario name:		Vendor Evaluation against EPES-specific guidelines						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Scenario Initiation	Deliver developed guidelines to EPES vendors	With the assistance of T5.5 Partners, the EPES vendors, or the Pilot Site acting on Vendors behalf, will use the guidelines to perform a self-assessment.	Provide input to the tool	Vendors' representatives)	Assessment tool	2	
2	Input provided	Input assessment	The provided input will be assessed against best practices and guidelines	Assess the input	Assessment tool	Assessment tool	2, 3	
3	Self-assessment performed	Recommendations for Security Improvements	The supply-chain security practices results are provided to the Vendor/Pilot Site.	Assessment results	Assessment tool	Vendors' representatives	3	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Pilot site practices	This will be the input to the tool regarding current pilot site practices, based on which the provided tool will perform the required assessment	
2	Vendor practices	This will be the input to the tool regarding current vendor practices, based on which the provided tool will perform the required assessment	
3	Self-assessment results	The results of the self-assessment performed by the vendors and Pilot Site, against the guidelines developed by T5.5 partners.	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.29 USE CASE 29 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
29	Distribution, DER, Customer Domains Process, Field, Operation Zones	Event simulator of a progressing wildfire and assessment of its impact on Distribution System

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	2023/3/13	Ektor Stasinos	Original Version	
0.2	2023/06/08	Ugo Stecchi	1st review	Approved
0.3	2023/06/23	Ektor Stasinos	2nd version according to the corrections	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	The aim of this Use Case is to assess the impact of wildfires in distribution system and provide an operational strategy to enhance its resilience, expanding T3.3.1 event simulator (which is mainly focused at windstorms and fragility-based modelling) to also include the modelling of wildfire events. Multiple scenarios will be considered in this framework, providing an operational plan which aims to enhance the system's resilient response against those HILF events, supporting DSO's decisions.
Objective(s)	The DSO will be able to model wildfire events and assess their impact in distribution system (line outages, spatiotemporal load shedding, wildfire's trajectory assessment). O1. Demonstration of increased energy system reliability and resilience / Use Case29 will provide the DSO an optimal scheduling strategy of power resources to enhance the resilience of the grid, considering the varying conditions during the spread of a progressing wildfire.
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
<p>The purpose of this Use Case is to capture the modelling of wildfire events. The presented scheme will assess the impact of wildfire events on distribution system (such as line outages, spatiotemporal load shedding, wildfire's trajectory assessment, etc.) by using a stochastic programming structure to capture the uncertainties. The goal of this Use Case is to provide an optimal operational scheme for enhancing distribution system resilience considering the varying conditions during the spread of a progressing wildfire. Eventually, this module will increase the distribution system resilience levels, mitigating the disruptive effects of a potential wildfire.</p>
Complete description
<p>In recent years, extreme weather events (EWEs) around the world have underlined the need for operative strategies that can significantly strengthen the power grid and enhance its resilience against those incidents. The effects of climate change are increasing both the frequency and the intensity of disruptive HILF events such as wildfires, floods, windstorms which often cause power outages to consumers and damages in power system infrastructure. Any operational framework dealing with the enhancement of power system (physical) resilience must take into account the unique nature of diverse HILF events. That means that each EWE has different spatial and temporal impact on power system infrastructure. Based on that, the aim of Use Case 29 is to enrich and expand the HILF events modular simulator tool features of T3.3.1 which mainly focuses at windstorms and fragility-based modelling, to also include wildfire events modelling.</p> <p>In the premises of this use case, the end users will obtain a tool which models wildfire events, assesses their spatial and temporal impact on distribution system (such as line outages and lines capacity reduction) and proposes a set of operational measures to enhance its resilience and to mitigate their disruptive effects. Therefore, a tool will be developed aiming at scheduling the distribution system resources operation to minimize load curtailments and the expected socioeconomic cost during such an emergency situation, using stochastic programming to capture the diverse uncertainties (load demand, RES generation, weather forecast etc.). By examining a large number of scenarios instead of mean values, the tool will provide final results that cover a wide spectrum of different most probable parameter values, including the ones that depict the worst case probable conditions. Additionally, in order to evaluate the distribution system line outages and to quantify the spatial and temporal load curtailments provoked by the extreme event, this scheme will assess the wildfire's propagation, taking into account the varying weather-related conditions. Therefore, this Use Case will deliver a toolkit to model the impact of wildfire events on distribution system in order to assess and enhance its resilience and will contribute to the improvement of the overall security and resiliency in power system.</p> <p>In conclusion, this use case will provide end users a framework which models wildfire events and assesses their impact on distribution system. It will also deliver an optimal operational strategy to enhance the network's resilience against this kind of natural disasters, supporting the DSO's decisions. Regarding C3PO features, this use case can also provide inputs to T3.3.2 as initiating events to the cascading simulators and can also provide wildfire event scenarios inputs for T3.4 and T3.5.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
A wildfire event occurrence
Prerequisites
<ul style="list-style-type: none"> • The topology of the network is well known and modelled. • An accurate weather forecast for the area of the grid is available and periodically updated (ambient temperature, wind speed, wind direction, solar radiation). • The location and characteristics of DERs are known. • The characteristics of distribution lines are known (capacity, length, diameter). • In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the DGs • Ideally some historical weather data to better calibrate the wildfire event generation

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
-
Level of depth
Detailed use case (medium)
Prioritisation
5
Generic, regional or national relation
Regional
Nature of the use case
Wildfire event modular simulator, resilience-oriented distribution system optimal operation (technical)
Further keywords for classification
Wildfire events modelling, wildfire impact assessment, distribution system, resilience-oriented operational measures

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors				
Grouping		Group description		
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.		
Actor name	Actor type	Actor description		Further information specific to this use case
System Operator (DSO)	Role	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity		Use Case 29 will receive the required input data from the DSO (network characteristics, generation units capacity, load demand, etc.) and will provide an optimal resilience-oriented scheduling of power resources to mitigate the disruptive effects of a wildfire event.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
Event simulator of a progressing wildfire and assessment of its impact on Distribution System (ESWDS)	Application / SW tool suite	Use Case 29 as part of C3PO software tool suite	-
C3PO tools	Application / SW tool suite	R2D2 Product delivering the assessment of HILF events impact and proposing optimal planning and mitigation measures for resilience enhancement.	Regarding C3PO features, this use case can provide inputs to T3.3.2 as initiating events to the cascading simulators and wildfire event scenarios inputs for T3.4 and T3.5.

Grouping		Group description	
Other actors			
Actor name	Actor type	Actor description	Further information specific to this use case
External weather service provider	Weather service provider	An actor that can provide weather-related data, day-ahead forecasts and historical data.	A weather service provider is responsible for periodic updates to the network operator regarding weather-related data and several parameters of an occurring extreme weather event.
SCADA - DMS	Control system	System providing periodic data, measurements and alarms to the system operator.	SCADA system have a constant access to real time picture of the entire network showing power system voltage, frequency, MW, MVAR, etc., supervising, monitoring and controlling power in real time.



D2.3 - Requirements and Detailed Architecture Design

			SCADA's supervision over optimal operation of power system, outages, power generation and associated resources are linked with this Use Case.
Fire Station	Fire Station	A structure for storing firefighting apparatuses such as fire engines and related vehicles, personal protective equipment, fire hoses and other specialized equipment.	A fire station can locate a wildfire and provide related data (its height, temperature, distribution line affected, etc.).

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Standard scenario	As a wildfire event hits the grid, its impact on distribution system is evaluated and an operational strategy is proposed to the DSO regarding the enhancement of the distribution grid resilient response	C3PO (ESWDS), DSO	A wildfire event that progresses through the network	<p>-The topology of the network is well known and modelled.</p> <p>-An accurate weather forecast for the area of the grid is available (hourly) and periodically updated (ambient temperature, wind speed, wind direction, solar radiation).</p> <p>-The location and characteristics of DERs are known.</p> <p>-The characteristics of distribution lines are known (capacity, length, diameter).</p> <p>-In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the DGs.</p> <p>-Ideally some historical weather data to better</p>	<p>-Wildfire event modular simulator tool.</p> <p>-Assessment of the wildfire's propagation, taking into account the varying weather-related conditions.</p> <p>-Evaluation of the spatial and temporal impact of the wildfire event (line outages, load curtailments).</p> <p>-Resilience-oriented optimal scheduling of distribution system resources to minimize the disruptive effects of the wildfire.</p> <p>-Detailed report of the actions taken and the rationale behind them.</p>

D2.3 - Requirements and Detailed Architecture Design

					calibrate the wildfire event generation.	
2	Insufficient data	Exceptional scenario: In case some of the required data is missing, use case 29 cannot deploy its features				

4.2 Steps – Scenarios

Scenario								
Scenario name:		Standard scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Loading weather forecasting and network characteristics	Input data, Starting process	Initial (normal) operation, Incorporation of network and weather-related data, optimal power flow calculation	Data gathering, Optimal Power Flow Calculation	DSO, Weather service provider	C3PO (ESWDS)	ID 1 - Weather forecasting (e.g., solar radiation, wind speed) and network characteristics	C3P_006, 007, 009, 010
2	Wildfire hits the network	Wildfire event modelling	Definition of the affected distribution line, wildfire and outage-related input data, Wildfire event modelling (at which line, characteristics)	Wildfire event modelling / Calculations	Fire Station	C3PO (ESWDS)	ID 2 - Acknowledgement of the affected distribution line, Wildfire characteristics (height, temperature)	C3P_010

D2.3 - Requirements and Detailed Architecture Design

3	Assessment of the wildfire's spatiotemporal propagation	Evaluation of wildfire's trajectory	Assessment of the wildfire's spatiotemporal propagation based on line and weather-related data	Assessment of the wildfire's spatiotemporal propagation / Calculations	C3PO (ESWDS)	C3PO (ESWDS)	-	C3P_010
4	Evaluation of the spatiotemporal impact of the wildfire event	Evaluation of wildfire's impact	Evaluation of the spatiotemporal impact of the wildfire event (total line outages, load curtailments)	Evaluation of the spatiotemporal impact of the wildfire event / Calculations	C3PO (ESWDS)	C3PO (ESWDS)	-	C3P_010
5	Application of operational measures to minimize the disruptive effects of the wildfire	Recommended operational measures	Application of operational measures to enhance the distribution system resilience and to minimize the disruptive effects of the wildfire	Resilience-oriented scheduling of power resources	C3PO (ESWDS)	DSO	ID 3 - A list of proposed operational measures to mitigate the wildfire's impact on distribution system based on wildfire's modelling	C3P_008

Scenario								
Scenario name:		Insufficient data						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Loading weather forecasting and network	Input data, Starting process	Incorporation of network, wildfire and weather-related data	Data gathering	DSO, Weather service provider, Fire Station	C3PO (ESWDS)	IDs 1,2 - Weather forecasting (e.g., solar radiation, wind speed) and	C3P_006, 007, 009, 010

D2.3 - Requirements and Detailed Architecture Design

	characteristics or wildfire hits the network						network characteristics, Acknowledgement of the affected distribution line, Wildfire characteristics (height, temperature)	
2	Insufficient data	-	If any of the required data is missing (i.e., network topology, which line is hit), C3PO will issue an alert to the DSO	Signal	C3PO (ESWDS)	DSO	Alert	-

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Weather forecasting and network characteristics	Weather forecasting (e.g., solar radiation, wind speed) and network characteristics	C3P_006,007,009,010
2	Wildfire hits the network	Acknowledgement of the affected distribution line, Wildfire characteristics (height, temperature)	C3P_010
3	Application of operational measures to minimize the disruptive effects of the wildfire	A list of proposed operational measures to mitigate the wildfire's impact on distribution system	C3P_008



6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.30 USE CASE 30 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
30	Distribution, DER, Customer Domains Process, Field, Operation Zones	Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	15/03/2023	Kaiyuan Pang	Initial draft	
0.2	02/06/2023	Ugo Stecchi	1st review	Approved
0.3	08/06/2023	Kaiyuan Pang, Ektor Stasinos	2nd draft	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	The use case aims to provide an integrated operation and restoration solution for distribution systems subject to catastrophic events, including flexible microgrid formation, sustainable microgrid scheduling, and frequency-aware restoration.
Objective(s)	1. Reduce service interruption costs in distribution systems subject to catastrophic events 2. Boost the restoration process in distribution systems subject to catastrophic events
Related business case(s)	BC1, BC2

1.4 Narrative of use case

Narrative of use case
Short description
<p>The use case aims to enhance distribution system resilience by determining the optimal operation and restoration activities after the occurrence of catastrophic events. The integrated operation and restoration solution provided by the use case includes a flexible microgrid formation scheme to separate the faulted system into multiple microgrids, a sustainable microgrid scheduling scheme to dispatch the stochastic power of distributed generators and electrical loads, and a frequency-aware restoration scheme to dispatch repair crews and pick up loads.</p>
Complete description
<p>To reduce service interruption costs and support fundamental facilities in a distribution system subject to catastrophic failures, a pragmatic and effective way is to separate the system into multiple microgrids to maintain the electrical connection between distributed generators (DGs) and critical loads (CLs). Forming microgrids is a dynamic process requiring a set of sequential switch operations to develop and extend the faulted distribution system. Subsequently, the formed microgrids should be sustainably scheduled to energize as many CLs as possible. In the microgrid scheduling scheme, a key task is to handle the stochastic power of DGs and loads in a robust and non-conservative manner to achieve a reasonable trade-off between system security and outage cost reduction. While the microgrids are operating, a tailored restoration scheme should be implemented to clear the existing faults and restore the system back to the normal operating state. During the restoration process, the repair crews should be dispatched in coordination with load pick to reduce system interruption time and accelerate load energization. Considering the potential strategies (microgrid formation, scheduling, and restoration) for distribution system resilience enhancement, the use case proposes an integrated operation and restoration strategy for distribution systems subject to catastrophic events. End users can obtain the solution to microgrid formation, microgrid scheduling, and system restoration by solving the following three models:</p> <p>Dynamic microgrid formation model for post-disruption distribution systems: the model provides the optimal microgrid topology to be formed and a set of sequential switch operations required to develop the faulted system to the desirable microgrids. After a catastrophic event that leads to multiple faults in the distribution system, the protection system is triggered to prevent the faults from spreading, resulting in only a small part of the system operating. To extend and interconnect the initial subsystems, the proposed dynamic microgrid formation model is two-stage. The first stage determines the final and optimal microgrid topology to be formed, and the second stage searches for a set of sequential switch operations toward the desirable microgrids. In the first stage, available DGs are flexibly allocated into microgrids with the objective of maximizing energized loads, and each microgrid is required to be operated radially for protection coordination and short current reduction. The switch operations provided by the second-stage model are frequency-aware, indicating that the frequency dynamics are calculated and constrained in each switch operation.</p> <p>Sustainable microgrid scheduling model for post-disruption distribution systems: after the microgrids are formed, it is crucial to schedule the microgrid in a sustainable manner to reduce affected customers and avoid potential operational failures. With the increasing penetration of renewable energy sources into the distribution system, power generation manifests high stochasticity and intermittency. Besides, the load power demand is uncertain due to the intrinsic stochasticity of customers' behaviors. The source-load stochasticity requires a robust microgrid scheduling</p>

D2.3 – Requirements and Detailed Architecture Design

scheme to balance the state fluctuation in the distribution system. The use case proposes a robust microgrid scheduling scheme considering the source-load stochasticity. The uncertain power of DGs and loads is formulated with the joint chance constraint to develop a non-conservative scheduling scheme that guarantees the overall violation of system states under a desirable probability. Furthermore, the proposed scheduling scheme is implemented with model predictive control to provide real-time dispatch values for DGs and loads in the distribution system.

Dynamic restoration model for post-disruption distribution systems: while the formed microgrids are sustainably operating, the existing faults should be cleared in order to restore the faulted distribution system back to normal operation. The use case proposes a dynamic distribution system restoration model considering the coordination between repair crew dispatch and cold load pickup. The repair crew dispatch is formulated with chance constraints to incorporate the stochastic repair time, which is updated dynamically according to the fault knowledge acquisition. Then the repair crew dispatch model is implemented with the model predictive control to restore the faulted distribution system step by step. After a fault is cleared, some unrecoverable areas can be energized, indicating that load pickups can be conducted to reduce outage costs. However, the restoration process for catastrophic events normally lasts for a long period, e.g., hours or even days, so the cold load effect should be considered to provide a safe operation. By modeling the cold load pickup power, the use case calculates the frequency dynamics subject to a load pickup, i.e., the rate of change of frequency, frequency nadir, and steady-state frequency. The load pickup decisions provided by the use case are under safe frequency conditions, i.e., the rate of change of frequency, frequency nadir, and steady-state frequency are maintained under pre-defined limits.

By executing the above three models chronologically, an integrated operation and restoration strategy for distribution systems subject to catastrophic events is obtained. After faults are detected in the distribution system, microgrids are first formed to reduce losses and support critical loads, and then the formed microgrids are scheduled in real-time to guarantee a safe and robust operation. Lastly, the system is restored to normal operation by dispatching repair crews and picking up cold loads.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Power forecasters are employed to evaluate the stochastic power of intermittent generators and loads, and the historical forecast data are stored and accessible
Prerequisites
Distribution system fault knowledge, e.g., fault locations and outage area, after the catastrophic event is known to the distribution system operator
Distribution system component availability, e.g., the status of generators and loads, is known to the distribution system operator

D2.3 – Requirements and Detailed Architecture Design

Other distribution system parameters, e.g., network model and pre-outage power flow, are uploaded and stored in the distribution system dispatch center.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC 12: Emergency & Restoration – Over-Frequency Protection module UC 17: Outage coordination and automated creation of topology files for Individual Grid Models UC 19: Emergency & Restoration - System Split module upgrade UC 23: Cooperative crisis handling in case of cascading effects
Level of depth
High
Prioritisation
High
Generic, regional or national relation
Regional (the use case focuses on the distribution system level)
Nature of the use case
Technical
Further keywords for classification
Distribution system resilience, microgrid formation, microgrid scheduling, distribution system restoration

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
System Operator	Role	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity	System Operator in this use case refers to the distribution system operator (DSO)
Energy Service Company	Role	A party offering energy-related services to the Party Connected to Grid, but not directly active in the energy value chain or the physical infrastructure itself. The Energy Service Company (ESCO) may provide insight services as well as energy management services	Energy Service Company in this use case is responsible for restoring the faulted distribution system back to the normal state

Grouping		Group description	
Software/Hardware components		Software/Hardware components for post-disruption distribution system operation and restoration	
Actor name	Actor type	Actor description	Further information specific to this use case
SCADA	Control system	Supervisory control and data acquisition (SCADA) is a control system architecture comprising computers, networked data communications and graphical user interfaces for high-level supervision of machines and processes. It also covers sensors and other devices, such as programmable logic controllers, which interface with process plant or machinery	SCADA system is used to provide real-time active power generation and frequency measurements

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
Post-Disruption Distribution System Operation and Restoration Module (PDDSORM)	Application / SW tool suite	Post-Disruption Distribution System Operation and Restoration Module is responsible for microgrid formation, microgrid scheduling, and system restoration in a distribution system subject to catastrophic events	PDDSORM is used to determine the feasible solution to microgrid formation, microgrid scheduling, and system restoration
C3PO tools	Application / SW tool suite	R2D2 Product delivering the assessment of HILF events impact and proposing optimal planning and mitigation measures for resilience enhancement.	Regarding C3PO features, this use case will take HILF events outage scenarios as inputs from T3.3.1 or use case 29 (initiating events).

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Flexible microgrid formation	A solution to separate the faulted distribution system into microgrids to reduce outage losses and support local loads	DSO	Fault knowledge and distribution system parameters have been uploaded and known	The initial state of the distribution system subject to catastrophic events	One/multiple microgrids are formed

D2.3 - Requirements and Detailed Architecture Design

2	Sustainable microgrid scheduling	A solution to schedule the formed microgrids sustainably	DSO	Microgrids have been successfully formed	Microgrids are operating without consideration of source-load stochasticity	Microgrids are operating robustly and sustainably considering the stochastic power of generators and loads
3	Dynamic distribution system restoration	A solution to restore the faulted distribution system back to the normal state	Energy Service Company	Fault knowledge and distribution system parameters have been uploaded and known	The initial state of the distribution system subject to catastrophic events	The pre-disruption operating state of the distribution system
4	Insufficient data	Exceptional scenario: In case some of the required data is missing, use case 44 cannot deploy its features				

4.2 Steps - Scenarios

Scenario								
Scenario name:		1 Flexible microgrid formation						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Fault knowledge and distribution system parameter collection	Data input	Obtain fault information, system parameters, and operating states	Provide necessary data to System Operator	DSO, C3PO (T3.3)	C3PO (PDDSORM)	1	C3P_007,009,010, C3P_001 (ideally),

D2.3 - Requirements and Detailed Architecture Design

2	First-stage solution	Determination of microgrid topology	The first-stage optimization model is solved to provide the final and optimal microgrid topology to be formed	Provide the final and optimal microgrid topology to be formed	-	-	2	C3P_007,008,009,010
3	Second-stage solution	Determination of switch operations	The second-stage optimization model is solved to provide the sequential switch operations to form the desirable microgrids	Provide sequential switch operations to form the desirable microgrids	-	-	3	C3P_007,008,009,010
4	Switch operation implementation	Switch operation	The sequential switch operations provided by the second-stage optimization model is implemented to the actual faulted distribution system	Implement the sequential switch operations to form microgrids	C3PO (PDDSORM)	DSO	1	C3P_007,008,009,010

Scenario								
Scenario name:		2 Sustainable microgrid scheduling						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs

D2.3 - Requirements and Detailed Architecture Design

1	Stochastic generator power forecast	Data input	The power of intermittent generators in the distribution system is forecasted regularly	Stochastic generator power forecast	DSO	C3PO (PDDSORM)	4	C3P_007,008,009,010
2	Stochastic load power forecast	Data input	The power of loads in the distribution system is forecasted regularly	Stochastic load power forecast	DSO	C3PO (PDDSORM)	5	C3P_007,008,009,010
3	Microgrid scheduling solution	Determination of microgrid scheduling schem	The the sustainable microgrid scheduling model is solved to provide real-time microgrid scheduling schemes	Provide real-time microgrid scheduling schemes	C3PO (PDDSORM)	DSO	6	C3P_007,008,009,010
4	Scheduling scheme implementation	Scheduling microgrid	Implement the microgrid scheduling schemes provided by step 3	Implement the microgrid scheduling schemes provided by step 3	DSO	DSO	1	C3P_007,008,009,010

Scenario								
Scenario name:		3 Dynamic distribution system restoration						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Restoration resource preparation	Data input	The restoration resources, including repair crews and supporting equipment, should be prepared before the restoration process starts	Prepare restoration resources	Energy Service Company (DSO)	C3PO (PDDSORM)	7	

D2.3 - Requirements and Detailed Architecture Design

2	Obtain real-time transportation information	Data input	The transportation time among repair stations and faulted components is obtained before each execution of the repair crew dispatch model	Provide real-time transportation time among repair stations and faulted components	Energy Service Company (DSO)	C3PO (PDDSORM)	8	
3	Stochastic repair time estimation	Data input	The stochastic repair time of faulted components is estimated and updated dynamically with chance constraints	Provide the estimation of the stochastic repair times of each faulted component	Energy Service Company (DSO)	C3PO (PDDSORM)	9	
4	Repair crew dispatch solution	Determination of repair crew dispatch scheme	The repair crew dispatch model is solved to provide the repair crew dispatch scheme	Provide the repair crew dispatch scheme	C3PO (PDDSORM)	Energy Service Company (DSO)	10	
5	Repair crew dispatch	Dispatching repair crew	The available repair crews are dispatched based on the solution at step 4	Dispatch repair crews	Energy Service Company (DSO)	Energy Service Company (DSO)	10	
6	Cold load pickup solution	Determination of cold load pickup scheme	The cold load pickup model is solved to provide the sequential load pickup scheme	Provide the sequential load pickup scheme	C3PO (PDDSORM)	Energy Service Company (DSO)	11	
7	Cold load pickup	Cold load pickup	Cold loads are picked up sequentially based on the solution at step 6	Pick up cold loads	DSO	DSO	11	

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		4 Insufficient data						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Fault knowledge and distribution system parameter collection	Data input	Obtain fault information, system parameters, and operating states	Provide necessary data to System Operator	DSO, C3PO (T3.3)	C3PO (PDDSORM)	1	C3P_007 ,009,010, C3P_001 (ideally),
2	Insufficient data	-	If any of the required data is missing (i.e., network topology, which line is hit), C3PO will issue an alert to the DSO	Signal	C3PO (PDDSORM)	DSO	Alert	-

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Fault knowledge, system parameters, and operating states	Detailed information regarding ongoing faults, network parameters, availability of components, and pre-outage operating states	C3P_001,006,007,008,009,010
2	Final and optimal microgrid topology to be formed	Final and optimal microgrid topology to be formed provided by the first-stage model of scenario “flexible microgrid formation”	C3P_001,006,007,008,009,010
3	Sequential switch operations to form the desirable microgrids	Sequential switch operations to form the desirable microgrids provided by the second-stage mode of scenario “flexible microgrid formation”	C3P_001,006,007,008,009,010

D2.3 – Requirements and Detailed Architecture Design

4	Predicted active power of generators in the distribution system	Predicted active power of generators provided by Production Responsible Party	C3P_001,006,007,008,009,010
5	Predicted active and reactive power of loads in the distribution system	Predicted active and reactive power of loads provided by Consumption Responsible Party	C3P_001,006,007,008,009,010
6	Real-time microgrid scheduling schemes	Real-time microgrid scheduling schemes provided by scenario “sustainable microgrid scheduling”	C3P_001,006,007,008,009,010
7	Availability of restoration resources	Number and location of repair crews provided by Energy Service Company	C3P_001,006,007,008,009,010
8	Real-time transportation time among repair stations and faulted components	Real-time transportation time among repair stations and faulted components provided by Energy Service Company	C3P_001,006,007,008,009,010
9	Estimation of the stochastic repair times of each faulted component	Estimation of the stochastic repair times of each faulted component provided by Energy Service Company	C3P_001,006,007,008,009,010
10	Repair crew dispatch scheme	Repair crew dispatch scheme provided by scenario “dynamic distribution system restoration”	C3P_001,006,007,008,009,010
11	Sequential load pickup scheme	Sequential load pickup scheme provided by scenario “dynamic distribution system restoration”	C3P_001,006,007,008,009,010

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
DG	Distributed generator
CL	Critical load

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.31 USE CASE 31 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
31	Transmission / Enterprise	DLR integration with IGMs and SCADA/EMS

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
1	30.03.2023	EMSS	-	Preliminary approved
2	25.04.2023	EMSS	Requirements definition	Preliminary approved
3	16.05.2023	SCC	Official review	Approved
4	04.07.2023	EMSS	Additional requirements definition	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Updating dynamic line ratings in SCADA applications and IGM models
Objective(s)	Automatic updating of current limits in the SCADA system and change of current limits in individual network models (IGM) in the process of intraday security analysis, as well as day-ahead analysis.
Related business case(s)	BC1

1.4 Narrative of use case

Narrative of use case
Short description
Automatic updating of current dynamic limits in SCADA/EMS system and updating of current limits in IGM models allows maximum use of available transmission capacities.
Complete description
<p>The Dynamic Line Rating (DLR) system is a tool for dynamic determination of power line current limits. In the Serbian TSO (EMS), there is a pilot project which goal is to install and use such a system. The transmission lines selected for the pilot project are OHL 110 kV no. 147/2 SS Bor 2 – SS Negotin, OHL 110 kV no. 151/4 SS Pančevo 2 – SS Alibunar and OHL- 110 kV no. 151/5 SS Alibunar - SS Alibunar.</p> <p>The first of the three transmission lines is located in the part of the network where there may be a problem of meeting the N-1 security criteria for higher power generation regimes in HPP Đerdap 2, especially in the case of maintenance of the transmission lines that evacuates energy from this power plant.</p> <p>The other two transmission lines are part of the "South Banat loop" to which two wind farms are connected, so it is necessary to maximize the transmission network capacity. The technical solution of the Ampacimon company was applied, which is based on the measurement of meteorological parameters on conductors in the most critical line sections. Within this pilot project, the following activities were carried out:</p> <p>Configuration of the DLR server, which gave the possibility of calculating dynamic transmission line limits, as well as short-term forecasting of these limits (up to 48 hours)</p> <p>Visualization, which allows the user to see the data from the DLR server on the website and download it in CSV format</p> <p>Integration into the SCADA system, which provides the visual display of dynamic limits</p> <p>Installing additional sensors to improve the accuracy of dynamic limits estimation (data exchange between sensors and DLR server is provided by mobile phone provider)</p> <p>Through the statistical analysis of data from the DLR system in the previous two years, it was established that the values obtained from the DLR system often differ with a large amplitude from the average seasonal limit of the transmission line. Bearing that in mind, in order to make the most of the DLR system, it is necessary to do the following in the R2D2 project:</p> <p>Automatic updating of current limits in the SCADA system (this is related to the alarming application, as well as to real-time security analyses) in National Control Centre (NCC)</p> <p>Change of current limits in individual network models (IGM) in the process of intraday security analysis, as well as day-ahead analysis (i.e. it is necessary to create software that will place the corresponding record from the CSV file in the appropriate place in the network model)</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Communication between DLR sensors and DLR server and communication between DLR server and SCADA/EMS already exist. Within the SCADA/EMS application, limits are used for real-time Contingency Analysis and Voltage - Var dispatching calculations.
Prerequisites
Values from DLR server should be provided as CSV files and also should be sent to SCADA/EMS system via certain communication protocol. In Linux crontab table added trigger that starts application every 5 minutes.

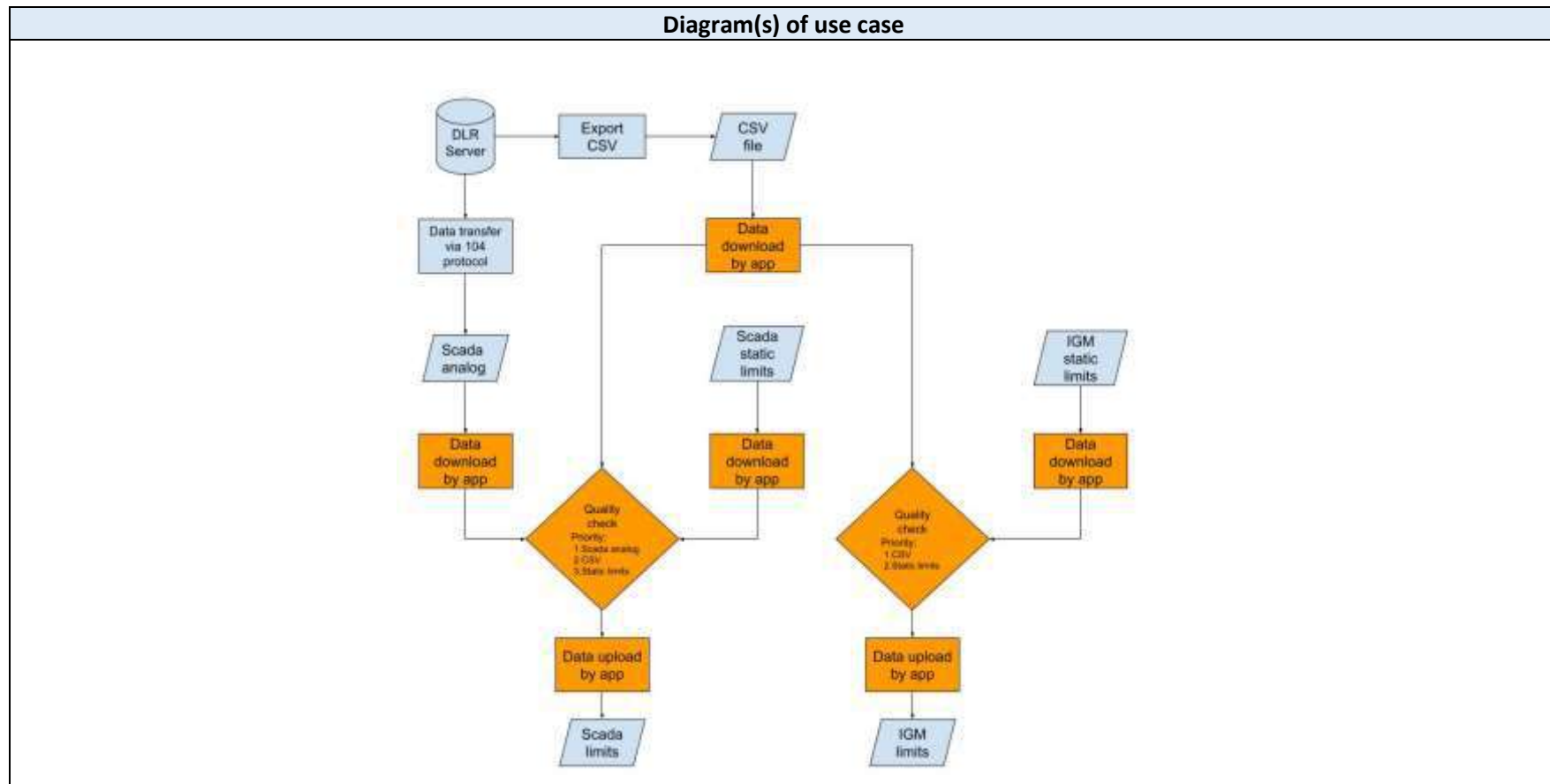
1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
High level of detail.
Prioritisation
High(4).
Generic, regional or national relation
National.
Nature of the use case
System functional requirements description.
Further keywords for classification
DLR, SCADA, limits, IGM.

1.8 General remarks

General remarks

2. Diagrams of use case



SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Software/Hardware components		Software/Hardware components used for DLR integration in real-time network applications and IGM models.	
Actor name	Actor type	Actor description	Further information specific to this use case
DLR Server	Server	DLR server collects all values from DLR sensors, sends it to SCADA/EMS system and also exports CSV files.	In this use case, values from DLR server are being used for implementation in SCADA limits, real-time network application and also IGMs.
SCADA/EMS	Control system	SCADA/EMS system is used for controlling, monitoring and analysing real-time network processes. The system consists of both software and hardware components and enables remote and on site gathering of data from equipment.	In this use case SCADA/EMS system receives values from DLR server and uses those values for real-time network calculations.
IGM server	Server	IGM server contains default data that is necessary for creating Individual Grid Model.	In this use case, values from CSV file that is exported from DLR server, are used as the new current limits in IGM.
EMMA Application	DLR Software Application	A software application program is a computer program designed to carry out a specific task other than one relating to the operation of the computer itself, typically to be used by end-users.	EMMA DLR Application is used to transfer DLR limits from DLR server into SCADA/EMS and IGMs

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO)	System Operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSO receives values from DLR server and uses those values to implement them in SCADA limits, real-time network applications and IGM models.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1.	SCADA basic scenario	In this scenario application reads DLR values (received from DLR server via 104 protocol) from Scada Analog and writes them into Scada Limit for certain lines.	TSO / EMMA DLR Application	Every 5 minutes (DLR limits update period)	Scada limits on lines with DLR sensors have static values that are not dynamically updated	Current limits in the SCADA system are updated with new values from DLR server
2.	IGM basic scenario	In this scenario application reads forecasted current limits from CSV file that is exported from DLR server and writes them into IGM.	TSO / EMMA DLR Application	Manual activation by operator	Forecasted limits in the IGM models have static values that are not dynamically updated	Forecasted limits in the IGM models are updated with new values from DLR server
3.	SCADA exceptional scenario	In this scenario, the application sees that the validity flag of the measurements coming via the 104 protocol is not good (the connection to the DLR server is broken) and then reads the csv files and writes those values to the SCADA limits for certain lines.	TSO / EMMA DLR Application	Bad validity flag of the measurements coming via the 104 protocol	Scada limits on lines with DLR sensors have static values that are not dynamically updated	Current limits in the SCADA system are updated with new values from DLR server

4.2 Steps – Scenarios

Scenario								
Scenario name:		SCADA basic scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Every 5 minutes (DLR limits update period)	Real-time DLR current limits download	Application reads limits which have arrived in SCADA as analogue values	Data downloading	TSO / SCADA/EMS (Analog)	TSO / EMMA DLR Application	1	EMM_042, EMM_065
2.	Real-time DLR current limits are downloaded	Real-time DLR current limits upload	Application writes limits into SCADA limits for each line with DLR sensors.	Data uploading	TSO / EMMA DLR Application	TSO / SCADA/EMS (limits)	1	EMM_042, EMM_067

Scenario								
Scenario name:		IGM basic scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	The application is started manually by operator	Forecasted current limits download	Application reads forecast limit values from CSV file	Data downloading	TSO / DLR Server	TSO / EMMA DLR Application	2	EMM_042, EMM_066
2	Forecast current limits are downloaded	Forecasted current limits upload	Application writes values of the forecast current limits to IGM models	Data uploading	TSO / EMMA DLR Application	TSO / IGM server	2	EMM_042, EMM_068

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		SCADA exceptional scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Bad validity flag of the measurements coming via the 104 protocol	Real-time DLR current limits download via csv file.	Application reads limits from CSV file which has exported from DLR server	Data downloading	TSO / DLR server	TSO / EMMA DLR Application	2	EMM_066
2	Real-time DLR current limits are downloaded	Real-time DLR current limits upload	Application writes limits into SCADA limits for each line with DLR sensors.	Data uploading	TSO / EMMA DLR Application	TSO / SCADA/EMS system (limits)	2	EMM_042, EMM_067

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Analogue values with quality flags of DLR limits in SCADA/EMS	Real-time DLR current limits from DLR server arrived into SCADA/EMS as analogue values.	EMM_065, EMM_067
2	DLR limits from CSV file	Real-time and forecasted limits from CSV file which is exported from DLR server	EMM_066, EMM_067, EMM_068
3	Quality flag	Quality of DLR system calculation	EMM_065, EMM_066

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
DLR server	Server which collects all measurements from DLR sensors, exports them as CSV file and sends it to SCADA/EMS system.
SCADA limits	Current limits for network elements in SCADA/EMS.
IGM	IGM – Individual Grid Model means a data set describing power system characteristics (generation, load and grid topology) and related rules to change these characteristics during capacity calculation, prepared by the responsible TSOs, to be merged with other individual grid model components in order to create the common grid model.
EQ file	A file used to create IGM. This file contains data related to grid elements, such as current limits, name, electric parameters...

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.32 USE CASE 32 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
32	Distribution, DERs, Customer Premises / Field, Operation	Planning and operation for a resilient multi-energy microgrid

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	03/05/2023	Dawei Qiu		Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	The use case aims to develop an optimal planning and operation strategy of an advanced multi-energy microgrid for load restorations, involving the pre-positioning as well as the routing and scheduling of mobile power resources.
Objective(s)	<p>The overall objective is to plan and operate a resilient multi-energy microgrid towards the maximisation of load restorations. The specific objectives can be listed as below:</p> <p>Develop a resilience-oriented planning method for MEMG with mobile power sources.</p> <p>Develop a smart control strategy for mobile power sources to enhance the resilience of MEMG.</p> <p>The essential loads of MEMG can be fully supplied with a cost-effective solution.</p> <p>The response time of mobile power sources can be real-time by adopting the advanced AI-based learning approach.</p> <p>The restoration time can be significantly reduced under the optimal routing and scheduling strategies of mobile power sources.</p>
Related business case(s)	BC1, BC2, BC5

1.4 Narrative of use case

Narrative of use case
Short description
<p>The use case aims to enhance the system resilience of a multi-energy microgrid by planning and operating the mobile sources. Specifically, a three-level defender-attacker-defender model is developed to plan the optimal sizing and pre-positioning of mobile sources in networked microgrids with decentralized control; an advanced learning-based algorithm is developed to control the routing and scheduling of mobile sources in a coupled energy-transportation network to maximize the load restorations of a multi-energy microgrid.</p>
Complete description
<p>Extreme weather events, characterized by their high impact and low probability (HILP), can disrupt system components and cause severe damage. The increasing interdependencies between different energy sectors, e.g., power, gas, and heat, further exacerbate the consequences of HILP events. Considering the potentially serious disruptions, the primary objective of a resilient energy system during extreme events is to maintain the uninterrupted supply of essential loads across different energy sectors, rendering a system-wise load restoration problem. In this Use Case, the planning and operation problems of a multi-energy microgrid (MEMG) is developed to coordinate various small-sized (mobile) energy sources effectively that offers a promising solution to enhance system resilience. The objective of this Use Case is to develop a multi-level strategic planning model and a series of model-free smart control algorithms to optimally design and operate the decentralized mobile sources under the MEMG concept for enhancement of resilience. Specifically, there two models:</p> <ol style="list-style-type: none"> 1) This model focuses on developing a comprehensive resilience-driven planning for optimal design of microgrids, which includes the sizing and pre-positioning of mobile power sources (MPSs). The model will be particularly useful in situations where several MEMGs are operating in a networked fashion. The objective is to develop a three-level defender-attacker-defender (DAD) model for optimal sizing and pre-positioning of MPSs in networked microgrids with decentralized control. The upper-level problem (UL) will aim to optimize results against certain contingencies such as line outages, while the middle-level problem (ML) and lower-level problem (LL) will be merged as a subproblem to select the contingencies that can cause the most severe damage. An adaptive genetic algorithm (GA) will be used to search for sizing and positioning decisions, which will capture various potential attack plans. The decentralized control approach will be based on a consensus algorithm and AC optimal power flow to model microgrid operations and capture technical constraints related to voltage and power loss. Incorporation of uncertainties related to renewable energy sources and load profiles will be done using stochastic programming. 2) This model focuses on the advanced control of mobile power sources (MPSs), such as electric vehicles (EVs), mobile energy storage systems (MESSs), and mobile emergency generators (MEGs), in MEMGs with flexible distributed energy resources (DERs) that can significantly improve the resilience of the microgrid during extreme events through islanding schemes. In addition, some internal lines could be damaged when an outage occurs. To address the core system uncertainties and dynamics while ensuring fast response of these decentralized MPSs, a model-free data-driven approach called multi-agent reinforcement learning (MARL) will be applied to deliver optimal control decisions by utilizing experiences acquired from repeated interactions with the resilience-driven MEMGs. Additionally, digitalization of district MEMGs will provide unique opportunities for effective management of the energy system during extreme events by turning off non-essential demand when the network is

stressed while maintaining the supply of essential demand. This model aims to address key challenges related to advanced control of MPSs and quantify the benefits of digitalization in enhancing the resilience of MEMGs.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Line and energy component outages within the multi-energy microgrid are known when planning and operating the mobile sources. The uncertain RES and load data can be accessed.
Prerequisites
Network topology and technical parameters of multi-energy microgrid
Network topology and technical parameters of transportation network
Models and technical parameters of mobile sources
Microgrid outage knowledge, e.g., locations of power distribution lines and energy components

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC 5: Optimal routing of intervention workforce to perform maintenance task. UC 22: Prevention and mitigation of cascading effects in case of extreme weather events. UC 30: Resilience-oriented Microgrid planning strategies considering system's stability and dynamic characteristics.
Level of depth
High
Prioritisation
5
Generic, regional or national relation
Regional
Nature of the use case

D2.3 - Requirements and Detailed Architecture Design

Describe the functional requirements of a system and document the design of a system
Further keywords for classification
Multi-energy microgrid, mobile sources, energy-transportation network

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
System Operator (DSO)	Role	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity	Use Case 29 will receive the required input data from the DSO (network characteristics, generation units capacity, load demand, etc.) and will provide an optimal resilience-oriented scheduling of power resources to mitigate the disruptive effects of a wildfire event.

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Other actors			
Actor name	Actor type	Actor description	Further information specific to this use case
MPS	Resource	Mobile power source	
MESS	Resource	Mobile energy storage system	
MEG	Resource	Mobile emergency generator	
EV	Resource	Electric vehicle	
RC	Resource	Repair crew	
DER	Resource	Distributed energy resources	
Transportation Operator	Resource	Transportation Operator	

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Planning for a resilient MEMG	To capture the impact of extreme events, multiple line outages happen in the power network within the MEMG. Then, the MPSs can be utilized to provide essential energy supply for resilience enhancement.	MEMG	Multiple line outages occur in the multi-energy network	A cost-oriented planning approach can be employed to determine the optimal capacities of mobile power sources under normal operation.	The optimal capacities of various mobile power sources are planned by the proposed resilience-oriented defender-attacker-defender model,

D2.3 - Requirements and Detailed Architecture Design

						which can ensure that the overall system resilience level is above a pre-defined value (e.g., 70%) during extreme events.
2	Operation for a resilient MEMG	Develop an advanced control algorithm to route and schedule MPSs in a coupled energy-transportation network for MEMG resilience enhancement.	MPS	Multiple line outages occur in the multi-energy network	An optimal energy management system is employed to minimize the operation cost of a MEMG in the normal condition.	MPSs are decentralized controlled to route to the damaged location in the transportation network and provide essential energy supply for the MEMG in the energy network. The load restoration quantity can be maximized by the routing and scheduling behaviors of MPSs.

4.2 Steps – Scenarios

Scenario	
Scenario name:	Planning for a resilient MEMG

D2.3 - Requirements and Detailed Architecture Design

Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1.1	Pre-event MEMG normal planning	Normal planning	Before an event happens, normal planning of mobile power sources is conducted	Planning decision	MEMG	MPS	Power and/or energy capacities as well as locations under normal planning	
1.2	Outage simulator (attacker)	Detect outages	Find the severe outage that can cause the largest load shedding	Knowledge update	DSO	MEMG	The most severe outage that causes the lowest resilience level	
1.3	Resilient planning under the severe outage obtained from 1.2 (defender)	Resilient planning	Resilience-oriented planning is conducted to find the optimal capacities of mobile power sources that can maintain the resilience level of an MEMG over a pre-defined value	Planning decision	DSO	MPS	Power and/or energy capacities as well as locations under resilience-oriented planning	
1.4	Outage simulator (attacker)	Detect outages	Find the severe outage that can cause the largest load shedding under the resilient planning results from 1.3	Knowledge update	DSO	MEMG	The most severe outage that causes the lowest resilience level	
1.5	Resilient planning under the severe outage obtained from 1.4 (defender)	Resilient planning	Resilience-oriented planning is conducted to find the optimal capacities of mobile power sources that can maintain the resilience level of an MEMG over a pre-defined value	Planning decision	DSO, MEMG	MPS	Power and/or energy capacities as well as locations under resilience-oriented planning (the attacker and defender will be run iteratively until meeting the requirement of the pre-defined resilience level.)	

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Operation for a resilient MEMG						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
2.1	Outage information after an extreme event	Detect outages	When an outage occurs, the damaged line ID will be updated	Knowledge update	DSO	MPS	Damaged line ID	
2.2	MEMG system condition	Detect load conditions	The load conditions of MEMG will be updated after the outage occurs	Knowledge update	MEMG	MPS	Load shedding quantity	
2.3	Transportation system condition	Detect transport conditions	The road conditions including road congestion, travelling time will be updated after the outage occurs	Knowledge update	Transportation operator	MPS	Traffic volume, travelling time	
2.4	MPS condition	Detect mobile source conditions	The availability of MPSs to behave routing and scheduling decisions will be updated	Knowledge update	MPS	MPS	MEG: power capacity; MESS: storage state-of-the-charge (SoC); EV: arriving time, battery SoC; RC: available resources.	
2.5	Routing in transportation network	Routing	An advanced control algorithm is employed to route MPSs to the optimal/damaged locations	Routing decision	MPS	MPS	Interactions between MPSs and the transportation network	
2.6	Scheduling in energy-network	Scheduling	An advanced control algorithm is employed to	Scheduling decision	MPS	MPS	Interactions between MPSs and the energy network	

D2.3 - Requirements and Detailed Architecture Design

			schedule MPSs to provide essential energy supply and repair the damaged lines					
2.7	Load restoration of MEMG	Load restoration	Essential loads are gradually supplied given the routing and scheduling behaviours of MPSs	Resilience enhancement	MEMG	MEMG	Resilient operation of the MEMG	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1.1	Power and/or energy capacities as well as locations	The optimal sizing and location decisions of MPSs under normal planning	
1.2	The most severe outage against the normal planning results	The most severe outage scenario that causes the largest load shedding or lowest resilience level under the normal planning results from 1.1	
1.3	Power and/or energy capacities as well as locations	The optimal sizing and location decisions of MPSs under resilience-oriented planning against the severe outage scenario from 1.2	
1.4	The most severe outage against the resilient planning results	The most severe outage scenario that causes the largest load shedding or lowest resilience level under the resilient planning results from 1.3	
1.5	Power and/or energy capacities as well as locations	The optimal sizing and location decisions of MPSs under resilience-oriented planning against the severe outage scenario from 1.4	
2.1	Damaged line ID	MPS observes the damaged line ID to evaluate the outage condition of the MEMG	

D2.3 - Requirements and Detailed Architecture Design

2.2	Load shedding quantity	MPS observes the load shedding quantity to evaluate the load shedding condition of the MEMG	
2.3	Traffic volume, travelling time	MPS observes the traffic information to make routing decisions in the transportation network	
2.4	Available resources	The available resources are evaluated by MPS themselves to make the potential routing and scheduling decisions	
2.7	Load restoration quantity	MPS are awarded some benefits in maximizing the load shedding quantity of the MEMG	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Multi-energy microgrid	MEMG
Microgrid central controller	MGCC
Distributed energy resource	DER
Mobile power source	MPS
Mobile energy storage system	MESS
Mobile emergency generator	MEG
Electric vehicle	EV
Repair crew	RC



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.33 USE CASE 33 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
33	Transmission, Distribution / Enterprise, Operation, Station, Field, Process	Detection of anomalies associated with cybersecurity through the characterization of traffic in the perimeter, levels of control and supervision, operation and in physical environments.

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	14/04/2023	Alex Alhambra	Upgraded to new template	
0.2	22/05/2023	Alex Alhambra	Comments added from revision	Approved
0.3	19/06/2023	Aida Carrillo	Changes accepted after revisions.	Approved
0.4	10/01/2024	Elena Montojo	Upgraded to new template	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	The scope of this use case is to detect threats affecting perimeter, control and supervision, operation and environment levels.
Objective(s)	Deployment of a combination of Cybersecurity tools to track different aspects of the system (perimeter and internal network traffic, vulnerabilities present in the system using passive scanning with port mirroring and other methods that include a minimum intrusion in the network, specific industrial network protocols, etc.), so that an alarm is sent to the Cybersecurity team of the TSO/DSO/RCC. Whenever an anomaly is detected in the system
Related business case(s)	BC1, BC3

1.4 Narrative of use case

Narrative of use case
Short description
The goal is to monitor EPES in order to detect advanced threats.
Complete description
The monitoring system from a cybersecurity landscape will correlate the perimeter, control and supervision, operation and environment levels by collecting data from sensors, critical equipment and information systems, both structured and unstructured, to detect anomalies that may be capable of causing events, such as blackouts, effects on human health, loss of supervision, unmet demand, interruptions of operations and communications at different levels of national and transnational interconnected systems.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
This use case does not take into account extreme events, only possible cyberattacks
Prerequisites
Data and equipment available in order to know what are we going to monitor
Be able to send perimeter logs to the collector Be able to send logs associated with operation technologies to the collector. Be able to send logs of safety and physical security platforms to the collector. Identification of platforms associated with the environment and integration with collector. Characterization of data flows between operating systems, segments and equipment

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC27, UC34, UC35, UC7, UC10, UC11
Level of depth
High
Prioritisation
5
Generic, regional or national relation
Generic. The idea is to detect this anomalies worldwide.
Nature of the use case
Functional requirement
Further keywords for classification
Cybersecurity, Anomaly detection, T5.3

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	Role	Distribution system operator' means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU).	
TSO	Role	Transmission system operator' means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU).	
RCC	Role	Regional coordination centre' means regional coordination centre established pursuant to Article 35 of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5	

D2.3 - Requirements and Detailed Architecture Design

		June 2019 on the internal market for electricity. Regional coordination centres shall complement the role of transmission system operators by performing the tasks of regional relevance assigned to them.	
System Operator	Role	TSO or DSO	System operator will support through their knowledge on EPES system, helping the analyst to conclude about legitimate movements or cybersecurity incidents.

Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
CISO	Role	Employee responsible of cybersecurity in TSO/DSO and his/her team.	If demo partner site has a CISO role, its objective is to determine and apply cybersecurity measures whenever an alert is reported from an analyst in order to secure the system.

Grouping		Group description	
Other actors			
Actor name	Actor type	Actor description	Further information specific to this use case
Carmen	Product	Product related to anomaly detection.	Used for the development of PRECOG, also will be used in demo partners for recollecting data
Claudia	Product	Product related to anomaly detection in Windows O.S.	EDR used for anomaly detection, mainly on windows assets. This

D2.3 - Requirements and Detailed Architecture Design

			product combines with Carmen in order to have high cyber capabilities and should be installed if possible. Also we can develop some specific version for other O.S. systems or lightweight versions.
Argos	Product	Product related to ruling detection.	Detects produces alerts using rules.
Firewall	Product	Product used as an IDS/IPS	Would be used to integrate logs and additional information in our technologies. Optional if demo site has one or more available.
Intelligence units	Query used in the product	This intelligence units will allow the analyst to collect more information and correlate it to extract advanced anomalies that will not depend only on one asset but correlating different data sources along the network.	Analysts create this intelligence units to detect advanced threats.
List	Filtering actor integrated in Carmen	Lists allow the analyst to reduce the event logs to search in more detail the anomalies	Lists are used as a tool work in the analysis procedures.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Outgoing communications to corporate segments and internet	Communications from OT networks to IT could be used for information exfiltration. Extracting information from an OT network (such as assets, network, internet access points and so on) could expose vulnerabilities that can exploit industrial resources.	Firewall (optional), Carmen	An illegal outbound connection will trigger an alert.	Sending perimeter logs to Carmen (defined in taxonomy section). Network must have available a port mirror communication to extract passively the information required, as mentioned in prerequisites.	The output should be analysed by cybersecurity analysts in order to confirm the alert state (False positive, security incident...). If there is a security incident, then procedures should be apply based on company politics and state legislation. Based on the final conclusion about the alert, the cybersecurity team must investigate and create new intelligence units to detect complex anomalies and feedback the system.

D2.3 - Requirements and Detailed Architecture Design

2	Incoming communications from corporate segments to OT segments or from public addresses directly from Internet.	Inbound communications from other networks must be detected and analysed if they are anomalous. Attackers could pivot from other networks to implant backdoors, command and control or to send malicious commands to disrupt or destroy EPES systems.	Firewall (optional), Carmen	An illegal inbound connection will trigger an alert.	Ditto	Ditto
3	Illegal asset connected	Non-authorized IT assets should be detected whenever they send communications related to its initial connection. Attackers can connect directly their equipment in order to implant backdoors, modify registers or disrupt communication between specific devices to produce outages.	Firewall (optional), Carmen	A new detected device paired with IP-MAC not seen previously in the network will trigger an alert.	Ditto	Ditto
4	Illegal OT commands	Anomalous OT commands that are not included in a baseline are detected in order to alert and confirm if it is legit. Attackers could modify packets from specific protocols (IEC61850, IEEE C37.118...) to modify communications	Carmen, specific protocol dissector, firewall (optional)	A first time command will trigger an alert. Also an old command with newly established communications (IP source-IP destination.) will trigger an alert.	Ditto	Ditto

D2.3 - Requirements and Detailed Architecture Design

		and alter the programs of different assets (RTU, IED, PLC...)				
--	--	---	--	--	--	--

4.2 Steps – Scenarios

Scenario								
Scenario name:		Outgoing communications to corporate segments and internet						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Detection	Non-standardized communications to corporate network segments	The communication is detected from network traffic. Traffic comes through port mirror from the agreed networks (IT/OT, control, supervision...)	Monitoring and detecting.	Firewall (optional), Carmen, Claudia, Argos, (Carmen or Argos as an IDS/SIEM, Claudia as an EDR),	Carmen, Argos	1,5	
2	Validate data flow models	Non-standardized communications from OT segments to IT segments (or Internet connections)	Once the communication is detected, it must be validated. Validation needs support from demo site to validate the network traffic between segments or assets.	Traffic validation	Firewall (optional), Carmen, Claudia, Argos, (Carmen or Argos as an IDS/SIEM, Claudia as an EDR),	Carmen, Argos	1, 2, 5	
3	Communications validation	Regular analysis following a diamond model methodology. Also using structured and non-structured	Now that the communication flow is validated, it is time to validate the information itself from this communication.	Validation services	Firewall (optional), Carmen, Claudia, Argos, (Carmen or Argos as an IDS/SIEM, Claudia as an EDR),	Carmen, Argos	1, 2	

D2.3 - Requirements and Detailed Architecture Design

		for gathering and making intelligence units.						
4	Case escalation	Alert and notification creation	Whenever an analyst manages the alert, it should be close determining its state. False positive or security incident, basically. Analysts can be supported by demo partners to cooperate together in the notification and escalation. Any further actions will depend on the government and demo partner site procedures.	Validation and incident confirmation	Firewall (optional), Carmen, Claudia, Argos, (Carmen or Argos as an IDS/SIEM, Claudia as an EDR),	Event manager tool, System Operator, Cybersecurity analyst, CISO...	1, 2, 3	

Scenario								
Scenario name:		Incoming communications from corporate segments to OT segments or from public addresses directly from Internet.						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Detection	Communication from external OT network (or Internet connections)	The communication is detected from network traffic. Traffic comes through port mirror from the agreed networks (IT/OT, control, supervision...)	Monitoring and alerting services	Firewall (optional), Carmen, Claudia, Argos, (Carmen or Argos as an IDS/SIEM, Claudia as an EDR),	Carmen, Argos	1,5	-

D2.3 - Requirements and Detailed Architecture Design

2	Data flow validation	Non-standardized communications from IT segments to OT segments (Or Internet connections)	Once the communication is detected, it must be validated. Validation needs support from demo site to validate the network traffic between segments or assets.	Validation services	Firewall (optional), Carmen, Claudia, Argos, (Carmen or Argos as an IDS/SIEM, Claudia as an EDR),	Carmen, Argos	1, 2, 5	-
3	Communication validation	Regular analysis following a methodologies	Now that the communication flow is validated, it is time to validate the information itself from this communication.	Validation services	Firewall (optional), Carmen, Claudia, Argos, (Carmen or Argos as an IDS/SIEM, Claudia as an EDR),	Carmen, Argos	1, 2	-
4	Escalation	Alert and notification creation	Whenever an analyst manages the alert, it should be close determining its state. False positive or security incident, basically. Analysts can be supported by demo partners to cooperate together in the notification and escalation. Any further actions will depend on the government and demo partner site procedures.	Escalation and/or validation	Firewall (optional), Carmen, Claudia, Argos, (Carmen or Argos as an IDS/SIEM, Claudia as an EDR),	Event manager tool, System Operator, Cybersecurity analyst, CISO...	1, 2, 3	-

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Illegal asset connected						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Connection	A non-authorized asset is detected	A connection coming from discovering protocols is detected with a new pair (IP-MAC)	Monitoring and alerting services	Firewall (optional), Switches on network, anomalous asset connected	Carmen, Claudia, Argos, (Carmen or Argos as an IDS/SIEM, Claudia as an EDR),	1, 5	-
2	Escalation	Analyst or automated detection escalates the event.	Detection should be confirmed by the dispatcher or system operator. Also the detection should be supported by an in-situ check of the new asset	Escalation/confirmation	Firewall, Carmen, Claudia, Argos, dispatcher, SIEM, EDR...	Carmen, Argos	1, 2	-
3	Action	Allow or deny and make investigations	Dispatchers or end users will allow or deny the communications.	Resolution	Analyst, system operator	Event manager tool, System Operator, Cybersecurity analyst, CISO...	1, 2, 3, 4	-

Scenario								
Scenario name:		Illegal OT commands						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs

D2.3 - Requirements and Detailed Architecture Design

1	Detection	Non-authorized protocol command	Protocols use commands in order to send and receive information. Most of time is always same communication. For legitimating communications, PRECOG will use lists to combine certain network characteristics to filter non-interesting traffic for the analyst. The main definition of what is legitimate and what is not.	Monitoring and detection	Firewall, Claudia, dispatcher, EDR...	Carmen, Argos, SIEM,	Carmen, Argos	1, 5	1
2	Escalation	Analyst or automated detection escalates the event.	The analyst will decide whether the packet is legit or not. Also some communications can be automated in order to improve analyst capabilities	Escalation and implication	Firewall, Claudia, dispatcher, EDR...	Carmen, Argos, SIEM,	Carmen, Argos	1, 3	2
3	Action	Allow or deny and make investigations	After the resolution of the event, the analyst will start an investigation if an incident is declared. Also, it could be as a permitted communication or a denegation in the system.	Resolution service.	Analyst, system operator		Event manager tool, System Operator, Cybersecurity analyst, CISO...	1, 2, 5	3

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Data	Detection exchanges data from the anomalous communication: IP source, IP destination, MAC, timestamp, protocol, command (if applies). All this information is exchanged through PRECOG in all the events.	PRE_013
2	Validation	Process that exchanges information about properties and also validation from the analyst and from the system operator	PRE_013
3	Alert	Alert is a small report with the notification itself from the anomalous finding. In this alert notified to the demo partner site the information exchanged is all the context found about the anomalous event, also the one included in ID1.	PRE_013
4	Escalation	The escalation information exchanged is the alert within ID1 and ID2.	PRE_013
5	Feedback	This information exchange allows us to correlate detection with escalation in order to feed the system. Feedback is also to improve Carmen lists in order to normalize usual traffic	PRE_001

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Backdoor	Type of malware that hides in equipment so the attackers can connect remotely.
EPES	Electrical Power and Energy Systems
CISO	Employee responsible of cybersecurity in TSO/DSO and his/her team.
PRECOG	One of the products/solutions of R2D2, “Prevention Systems For Energy Infrastructures Security”
EDR system	Endpoint Detection Response. Is a system to gather and analyze security threat-related information from computer workstations and other endpoints, with the goal of finding security breaches as they happen and facilitating a quick response to discovered or potential threats
OT	Operation Technologies (industrial)
IT	Information Technologies (businesses)

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.34 USE CASE 34 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
34	Transmission, Distribution / Enterprise, Operation, Station, Field, Process	Pattern detection and correlation with information from other cyberattacks in order to detect potential threats

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	29/03/2023	Alex Alhambra		
0.2	14/04/2023	Alex Alhambra	Upgraded to new template.	Approved
0.3	19/06/2023	Aida Carrillo	Changes accepted after revisions. Cleaned resolved comments after receiving approvals	Approved
0.4	10/01/2024	Elena Montojo	Upgraded to new template	

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	<p>The scope of this use case is to detect unknown threats affecting perimeter, control, supervision, operation and environment levels, based on their similarity to known threats.</p> <p>Environment level refers to all the perimeter around IT segment, i.e. DMZ, corporative...</p> <p>So both of this levels are also covered by UC51. But this will be based on the data we gather regarding the demo site.</p>

D2.3 – Requirements and Detailed Architecture Design

Objective(s)	Rising an alarm when an anomalous and potentially dangerous behaviour observed in the system is similar enough to already known cyber threats, yet not equal and thus, not being detected by traditional Cybersecurity tools.
Related business case(s)	BC1, BC3

1.4 Narrative of use case

Narrative of use case
Short description
Development of an intelligent module capable of characterizing different cyber threats based on the information collected from the different parts of TSO/DSO/RCC by the various Cybersecurity tools deployed in the system. The intelligent module will make use of various ML algorithms and techniques for calculating a similarity degree between a potential threat and previously seen threats, so that the Cybersecurity team of the TSO/DSO receives an alarm when the above mentioned similarity is high enough.
Complete description
This use case proposes the detection of unknown threats (zero-day threats or APTs) based on their similarity to already observed ones. In order to do so, already known threats will be characterized and clustered combining various ML algorithms attending to the tactical and/or operational intelligence these threats use. After this initial clustering, when any suspicious behaviour is observed, it is possible, not only to consider the presence of an APT in the system attending to its similarity to already known threats, but also to predict still unobserved/undetected behaviours or future cascading effects, based on this similarity. As a result, it is possible for Cybersecurity teams of final users to carry on an early detection of threats and to advance possible recovering actions, in case these threats succeeded.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
This use case does not cover the detection of already known cyber threats, which is already covered by use cases UC32 and UC33.
Prerequisites
Cybersecurity tools for the tracking and collection of information of the system (perimeter and internal network traffic, vulnerabilities present in the system, specific industrial network protocols, etc.) and information of the use of operational/tactical threat intelligence must be deployed in the TSO/DSO system for the intelligent module to analyze this information.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC24, UC25, UC26, UC32, UC33
Level of depth
High
Prioritisation
5
Generic, regional or national relation
Generic. Could apply to all demo partners.
Nature of the use case
Functional requirement
Further keywords for classification
Cybersecurity, Artificial Intelligence, Machine Learning, T5.4

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	Role	‘Distribution system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU).	
TSO	Role	Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the	

D2.3 - Requirements and Detailed Architecture Design

		internal market for electricity and amending Directive 2012/27/EU).	
RCC	Role	'Regional coordination centre' means regional coordination centre established pursuant to Article 35 of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity. Regional coordination centres shall complement the role of transmission system operators by performing the tasks of regional relevance assigned to them.	
Grouping		Group description	
R2D2 actors			
Actor name	Actor type	Actor description	Further information specific to this use case
CISO	Role	Employee responsible of cybersecurity in TSO/DSO and his/her team.	
Grouping		Group description	
Other actors			
Actor name	Actor type	Actor description	Further information specific to this use case
Carmen	Product	Product related to anomaly detection	Used for the development of PRECOG, also will be used in demo partners for recollecting data
Claudia	Product	Product related to anomaly detection	EDR used for anomaly detection, mainly on windows assets
Argos	Product	Product related to ruling detection	Detects alerts using rules
Firewall	Product	Product used as an IDS/IPS.	Would be used to integrate logs and additional information in our technologies. Optional if demo site has them available.
Intelligent Cybersecurity Module	Product	Threat Detection module based on ML	This module assesses the probability of an observed activity to be indicative of the presence of a

D2.3 - Requirements and Detailed Architecture Design

			threat in the system based on the activity's similarity to already known threats.
--	--	--	---

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Potential threat detection/attribution	Detection of the presence of a potential, unknown, cyber threat and potential attribution of authorship	Intelligent Cybersecurity Module	Potentially dangerous tactical or operational intelligence detection in the system	Cybersecurity tools deployed in the system detect potentially dangerous activity	If the potentially dangerous behaviour detected is similar enough to any of the already known cyber threats, an alarm is raised and the list of similar threat actors is attached to it

D2.3 - Requirements and Detailed Architecture Design

2	Intelligent Cybersecurity Module training	Training of the Intelligent Cybersecurity Module	Intelligent Cybersecurity Module	New intelligence is added to the threat intelligence database and the Intelligent Cybersecurity Module is trained offline	There is an existing database of threat intelligence	Existing threats in the database are clustered in an n-dimensional space and grouped by similarity.
---	---	--	----------------------------------	---	--	---

4.2 Steps – Scenarios

Scenario								
Scenario name:		Potential threat detection/attribution						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchange d (IDs)	Requirement, R-IDs
1	Tactical/Operational intelligence detection	Potential Threat detected	Potentially dangerous activity in tactical or operational plane is detected by Cybersecurity tools deployed in the system	Monitoring and alerting services	Monitoring and alerting services (Carmen, Claudia, Argos, Firewall, etc.)	Intelligent Cybersecurity Module	1	
2	Tactical/Operational intelligence normalization and analysis	Threat Intelligence normalization	Potentially dangerous activity observed in previous step (exchanged information id 1) is normalized and preprocessed to be converted in numerical format (n-dimensional arrays) which can later serve as inputs for ML algorithms. Results of preprocessing	Threat Intelligence Normalization service	Intelligent Cybersecurity Module	Intelligent Cybersecurity Module	1, 2, 3	

D2.3 - Requirements and Detailed Architecture Design

			(information exchange id 2) is then analysed and compared to already known cyber threats by the Intelligent Cybersecurity Module. The module calculates a measure of similarity to already known threats. The output of the module (exchanged information id 3) is a measure of similarity to each group of known threats.					
3	Tactical/Operational intelligence is similar enough to one or more already known cyber threats	Unknown threat detection	If the degree of similarity associated to the detected intelligence (exchanged information id 3) is higher to a previously configured threshold value, an alarm of presence of unknown threat is raised with data from the observed activity which triggered step 1 (exchanged information id 1) and data regarding already known threats which were similar enough (within the specified similarity threshold) (exchanged information id 4)	Threat detection service	Intelligent Cybersecurity Module	Cybersecurity team in TSO/DSO	1, 3, 4	

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Intelligent Cybersecurity Module training						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Intelligent Cybersecurity training start	Threat Intelligence normalization and preprocessing	Available operational and tactical threat intelligence (exchanged information id 1) is normalized and preprocessed to be converted in numerical format (n-dimensional arrays) which can later serve as inputs for ML algorithms (exchanged information Id 2).	Threat Intelligence Normalization	Intelligent Cybersecurity Module	Intelligent Cybersecurity Module	1, 2	
2	Tactical/Operational intelligence analysis	N-Dimensional clustering	Normalized threat intelligence (exchanged information id 2) is clustered in an n-dimensional space using ML. As a result, a set of groups/clusters (exchanged information id 3), each of them composed by different elements and characterized by a centroid point: the point in the n-dimensional space which is closest to all the elements in the cluster.	Intelligent Cybersecurity Module	Intelligent Cybersecurity Module	Intelligent Cybersecurity Module	2, 3	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Observed suspicious activity	Potentially dangerous tactical or operational intelligence detected by Cybersecurity tools deployed in the system	
2	Degree of similarity	Measure of similarity between 1 and tactical/operational intelligence associated to already known threats	
3	Potential threats	Subset of already known threats potentially present in the system	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
APT	Advanced Persistent Threat
ML	Machine Learning
CISO	Employee responsible of cybersecurity in TSO/DSO and his/her team.
PRECOG	One of the products/solutions of R2D2, “Prevention Systems For Energy Infrastructures Security”
EDR	Endpoint Detection Response. Is a system to gather and analyze security threat-related information from computer workstations and other endpoints, with the goal of finding security breaches as they happen and facilitating a quick response to discovered or potential threats
IDS	Intrusion Detection System. Is a monitoring system that detects suspicious activities and generates alerts when they are detected.



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.35 USE CASE 35 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
35	Transmission, Distribution / Operation	Upstream studies to validate the use of TSO/DSO means during crisis situations

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	2023/03/07	RTEi - César Clause	Original version	
0.2	2023/05/25	RTEi - César Clause	Use case update in revision process	Approved
0.3	2024/01/03	RTEi - Anouar Guesrami, EMSS – Srđan Subotić	UC redefinition	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	The aim of this Use Case is to determine, validate and coordinate remedial actions at both TSO and DSO levels to prepare for crisis situations
Objective(s)	Enhance the TSO/DSO coordination by allowing the validation of remedial actions from both sides that could be implemented then within real time operations. The expected final outcome is a common platform where TSO and DSO can exchange network models and related inputs (for instance, remedial actions proposal) and validate them in this platform for real time use.
Related business case(s)	BC1, BC4, BC5



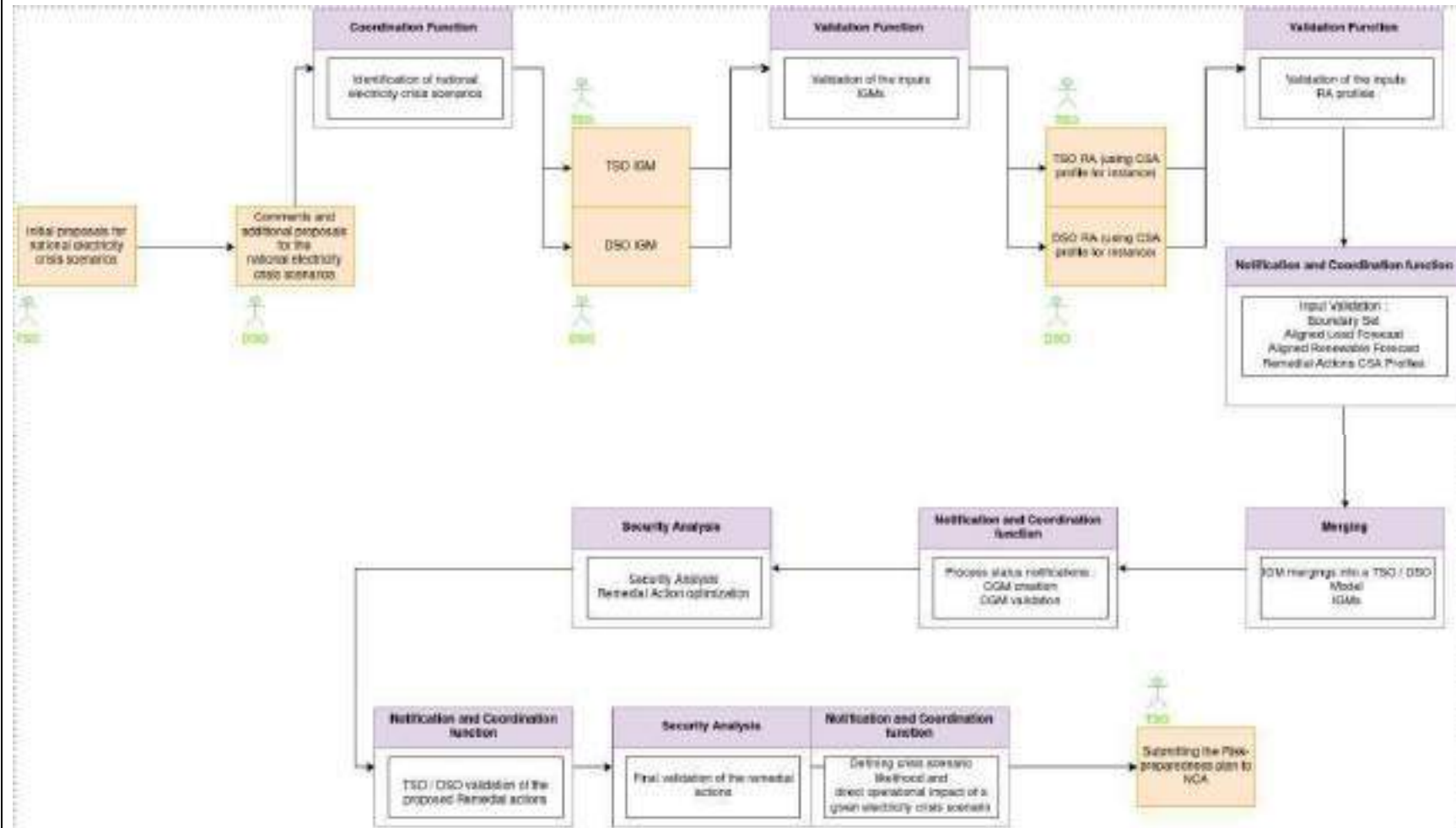
1.4 Narrative of use case

Narrative of use case	
Short description	
Enhance the TSO/DSO coordination by allowing the validation of remedial actions from both sides that could be implemented then within real time operations. The expected final outcome is a common platform where TSO and DSO can exchange network models and related inputs (for instance, remedial actions proposal) and validate them in this platform for real time use.	
Complete description	

D2.3 - Requirements and Detailed Architecture Design

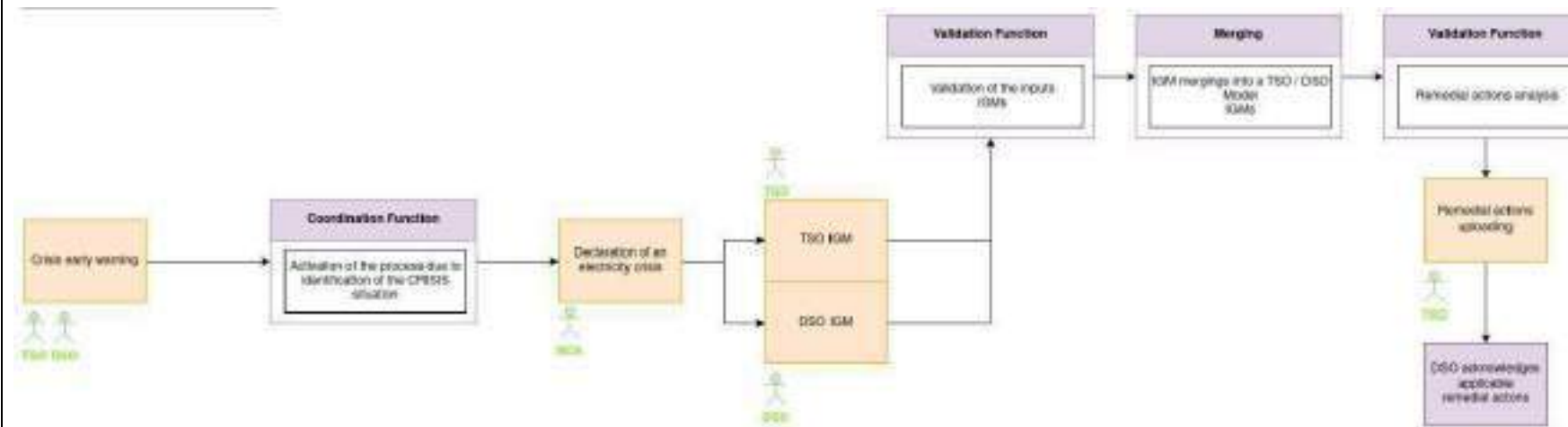
The overall process to be covered in the use case is described in a simplified way below:

Pre-crisis scenario:

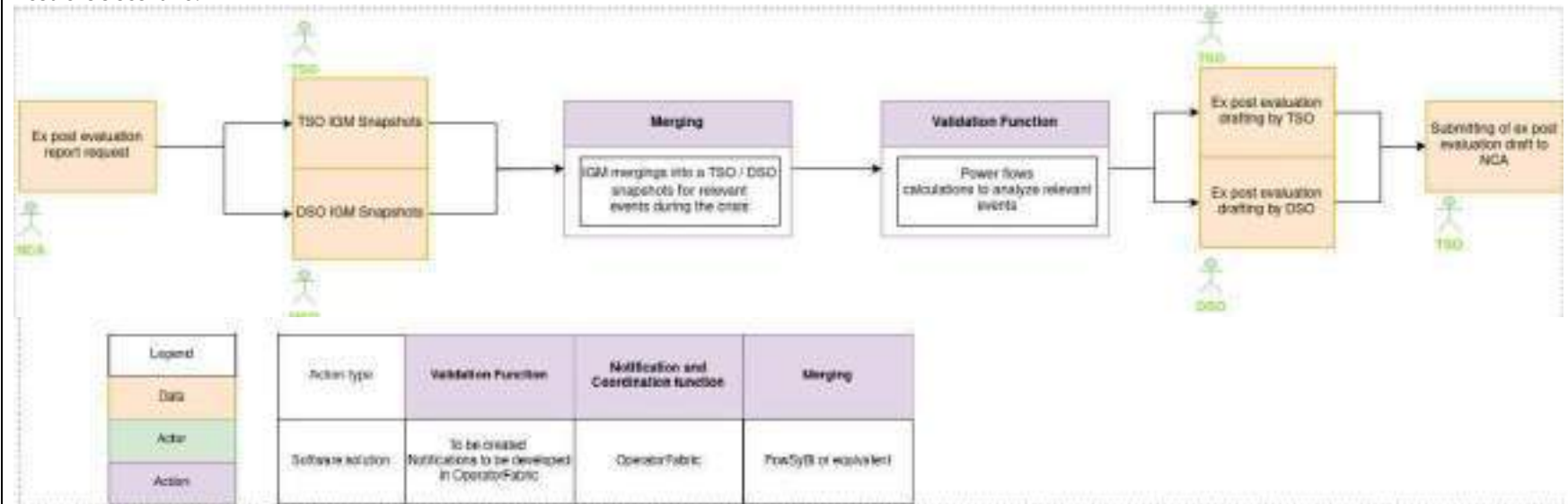


D2.3 - Requirements and Detailed Architecture Design

Crisis response scenario:



Post-crisis scenario:



1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
IGMs for TSO and DSO are available
Common RA are available and ready to be shared
Prerequisites
Consistent models at TSO and DSO levels, especially on formats ('CGMES', 'MATPOWER', 'IEEE-CDF', 'PSS/E', 'UCTE', 'XIIDM', 'POWER-FACTORY')
Aligned forecasts for the load, the wind and solar infeed.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC17
Level of depth
Low
Prioritisation :
4 – This use case is very important due to the growing interdependence of transmission and distribution system operation.
Generic, regional or national relation
Regional
Nature of the use case
Design of a system
Further keywords for classification
Grid model, Remedial actions, TSO-DSO coordination, Crisis situations

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	System Operator	Distribution System Operator (DSO) means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU).	DSO creates distribution grid models collaborates with TSO in all activities.

D2.3 - Requirements and Detailed Architecture Design

TSO	System Operator	Transmission System Operator (TSO) means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU).	TSO: <ul style="list-style-type: none"> - Propose crisis scenarios - Calculates parameters to assess crisis scenarios - Creates transmission grid models - Merges transmission and distribution grid models - Harmonizes RAs with DSOs - Draft the Risk Preparedness Plan - Draft the Ex post evaluation Report
NCA	Governmental authority or regulatory authority	National competent authority means a national governmental authority or a regulatory authority designated by a Member State in accordance with EU regulation 2019/941 Article 3.	NCA is responsible for risk-preparedness in the electricity sector. NCA monitor risk-preparedness activities and approves key documents.
NRA	regulatory authority	Regulatory authorities means regulatory authorities referred to in Article 57(1) of Directive (EU) 2019/944;	NRA take part in consultations in pre-crisis activities, crisis response and post-crisis activities
Market Participants	Producer or costumer or electricity trader	Market participant means market participant as defined in point (25) of Article 2 of Regulation (EU) 2019/943;	Market participants take part in consultations in pre-crisis activities, crisis response and post-crisis activities
Grouping		Group description	
Software/Hardware components		Software/Hardware components used in TSO-DSO coordination during crisis situations	
Power flow software	Calculation software	A software used to calculate power flows and voltages in the base case as well as after contingencies. In addition, it can merge grid models and assess Remedial Actions.	In this use case it is used to merge grid models and assess Remedial Actions.

D2.3 - Requirements and Detailed Architecture Design

IRIS Communication platform	Communication platform	A communication platform is a software solution that facilitates external and internal messaging and data exchange.	IRIS communication platform is used for communication between TSO and DSOs.
-----------------------------	------------------------	---	---

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Pre-crisis scenario	TSO in collaboration with DSO, market participants and relevant bodies drafts the Risk-preparedness plan	TSO / DSO	Regular annual repetition	Risk-preparedness plan is not drafted	Risk-preparedness plan is drafted
2	Crisis response scenario	TSO and DSO collaborates in Risk-preparedness plan implementation during a electricity crisis	TSO / DSO	A crisis situation has been identified	Risk-preparedness plan is drafted	Risk-preparedness plan is implemented
3	Post-crisis scenario	TSO and DSO collaborates in crisis response analysis and ex post crisis evaluation report drafting	TSO / DSO	A crisis situation has been completed	Ex post evaluation report is not drafted	Ex post evaluation report is drafted

4.2 Steps – Scenarios

Scenario								
Scenario name:		Pre-crisis scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Regular annual repetition	Initiation of the national electricity crisis scenarios identification	TSOs drafts initial proposals for national electricity crisis scenarios and requests from DSOs and relevant market participants to comment on these proposals and to identify additional national electricity crisis scenarios if possible, all according to Regulation 2019/941 Article 5(2)	Data uploading	TSO / IRIS communication platform	DSO, market participants / IRIS communication platform	1	
2	Request for national electricity crisis scenarios identification has been sent	Setting the proposals for the national electricity crisis scenarios by DSO and market participants	DSO and market participants comment on TSO's proposal for national electricity crisis scenarios and define additional proposals for the national electricity crisis scenarios and send them to TSO	Data uploading	DSO, market participants / IRIS communication platform	TSO / IRIS communication platform	2	

D2.3 - Requirements and Detailed Architecture Design

3	DSO and market participants proposals for crisis scenarios identification have been set	Identification of national electricity crisis scenarios	TSO sends to NCA, NRA, TSO and relevant market participants completed identified national electricity crisis scenarios	Data uploading	TSO / IRIS communication platform	NCA, NRA, DSO, market participants / IRIS communication platform	3	
4	National electricity crisis scenarios have been identified	DSO grid models uploading	DSO uploads grid models and available remedial actions corresponding to an initial condition of the electricity system and season(s) of the year when the crisis scenario is relevant	Data uploading	DSO / IRIS communication platform	TSO / IRIS communication platform	4, 5, 6	
5	DSO grid models have been uploaded	DSO grid models downloading	TSO downloads DSO grid models for merging	Data downloading	TSO / IRIS communication platform	TSO / power flow analysis software	4, 5, 6	
6	DSO grid models have been downloaded	Grid models merging	TSO merges the TSO and DSO grid model files in a consistent common grid model	Data processing	TSO / power flow analysis software	TSO / power flow analysis software	-	
7	Grid models have been merged	Remedial actions analysis	TSO carries out power flows calculations to select remedial actions corresponding to a list of initiating event(s), a chain of event(s) and the evolution of the crisis scenario	Data processing	TSO / power flow analysis software	TSO / power flow analysis software	-	

D2.3 - Requirements and Detailed Architecture Design

8	Remedial actions have been analyzed	Remedial actions uploading	TSO informs DSO on the most likely impacts of the crisis scenario, potential consequences, and potential measures (including remedial actions) that mitigate the relevant risk	Data uploading	TSO / power flow analysis software	TSO, DSO / IRIS communication platform	6, 7	
9	Remedial actions have been uploaded	DSO acknowledges remedial actions	DSO acknowledges the most likely impacts of the crisis scenario, potential consequences, and potential measures (including remedial actions) that mitigate the relevant risk	Acknowledgement	DSO / IRIS communication platform	TSO / IRIS communication platform	8	
10	Remedial actions have been acknowledged by DSO	Exchange of input information on crisis scenario likelihood and direct operational impact of a crisis scenario	TSO and DSO exchange information on assessed frequency of occurrence of an initiating event, expected energy not served percentage (EENS%) and loss of load expectation (LOLE)	Data uploading	TSO, DSO / IRIS communication platform	TSO, DSO / IRIS communication platform	9, 10, 11	
11	Information on crisis scenario likelihood and direct operational impact has been exchanged	TSO calculates crisis scenario likelihood and direct operational impact of a crisis scenario and sends results to DSO for verification	Based on input data, TSO defines crisis scenario likelihood and direct operational impact of a given electricity crisis scenario and informs DSO	Data processing	TSO / IRIS communication platform	DSO / IRIS communication platform	12, 7	

D2.3 - Requirements and Detailed Architecture Design

12	Crisis scenario likelihood and direct operational impact have been calculated and submitted to DSO	DSO acknowledges the crisis scenario likelihood and direct operational impact	DSO acknowledges the crisis scenario likelihood and direct operational impact	Acknowledgement	DSO / IRIS communication platform	TSO / IRIS communication platform	13, 14	
13	DSO has confirmed crisis scenario likelihood and direct operational impact	TSO submits the proposal on scenarios descriptions	TSO submits the detailed proposal on crisis scenario description according to Regulation 2019/941 Article 5(2) to NCA, NRA, DSO and market participants	Data uploading	TSO / IRIS communication platform	NCA, NRA, DSO market participants / IRIS communication platform	15	
14	TSO has submitted the scenarios descriptions	NCA, NRA, DSO and market participants comment on scenarios descriptions	NCA, NRA, DSO and market participants comment on scenarios descriptions	Data uploading	NCA, NRA, DSO market participants / IRIS communication platform	TSO / IRIS communication platform	16	
15	NCA, NRA, DSO and market participants have commented on scenarios descriptions	TSO submits the Risk-preparedness plan to NCA	TSO submits the Risk-preparedness plan to NCA	Data uploading	TSO / IRIS communication platform	NCA / IRIS communication platform	17	

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Crisis response scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	A crisis situation has been identified	Crisis early warning	TSO sends to DSO data that indicates upcoming crisis or vice versa	Data uploading	TSO, DSO / IRIS communication platform	DSO, TSO / IRIS communication platform	18	
2	Crisis early warning has been sent	Crisis early warning acknowledgement	DSO confirms to TSO upcoming crisis or vice versa	Acknowledgement	DSO, TSO / IRIS communication platform	TSO, DSO / IRIS communication platform	19	
3	Crisis early warning has been acknowledged	Declaration of an electricity crisis - warning	TSO sends to NCA information about upcoming crisis and suggests declaration of an electricity crisis	Data uploading	TSO / IRIS communication platform	NCA / IRIS communication platform	20	
4	Warning on declaration of an electricity crisis has been sent	Declaration of an electricity crisis	NCA informs NRA, TSO, DSO and relevant market participants that an electricity crisis has been declared and part of the Risk-preparedness plan that is to be carried out	Data uploading	NCA / IRIS communication platform	NRA, TSO, DSO, market participants / IRIS communication platform	21	
5	Electricity crisis has been declared	Grid models uploading	DSO uploads grid models and available remedial actions (according to the Risk-Preparedness Plan and real conditions in electricity system)	Data uploading	DSO / IRIS communication platform	DSO / IRIS communication platform	4,5,6	

D2.3 – Requirements and Detailed Architecture Design

6	DSO grid models have been uploaded	Grid models downloading	TSO downloads DSO grid models for merging	Data downloading	TSO / IRIS communication platform	TSO / power flow analysis software	4,5,6	
7	DSO grid models have been downloaded	Grid models merging	TSO merges the TSO and DSO grid model files in a consistent common grid model (according to the Risk-Preparedness Plan and real conditions in electricity system)	Data processing	TSO / power flow analysis software	TSO / power flow analysis software	-	
8	Grid models have been merged	Remedial actions analysis	TSO carries out power flows calculations to select remedial actions	Data processing	TSO / power flow analysis software	TSO / power flow analysis software	-	
9	Remedial actions have been analyzed	Remedial actions uploading	TSO informs DSO on the most effective remedial actions	Data uploading	TSO / power flow analysis software	TSO, DSO / IRIS communication platform	6	
10	Remedial actions have been uploaded	DSO acknowledges remedial actions	DSO acknowledges applicable remedial actions	Acknowledgement	DSO / IRIS communication platform	TSO / IRIS communication platform	22	

Notes:

- Steps 5-10 are carried out every day in day-ahead and intra-day operational planning process

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Post-crisis scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Crisis completion is officially declared	Ex post evaluation report request	NCA requests from TSO and DSO to draft ex post evaluation report in predefined template	Data uploading	NCA / IRIS communication platform	TSO, DSO / IRIS communication platform	23	
2	Ex post evaluation report has been requested	Grid models snapshots uploading	DSO uploads grid models snapshots for relevant events during the crisis	Data uploading	DSO / IRIS communication platform	DSO / IRIS communication platform	4,5	
3	DSO grid models snapshots has been uploaded	Grid models downloading	TSO downloads DSO grid models snapshots for merging	Data downloading	TSO / IRIS communication platform	TSO / power flow analysis software	4,5	
4	DSO grid models snapshots has been downloaded	Grid models snapshots merging	TSO merges the TSO and DSO grid model snapshots in a consistent common grid model for relevant events during the crisis	Data processing	TSO / power flow analysis software	TSO / power flow analysis software	-	
5	Grid models snapshots have been merged	Relevant events analysis	TSO carries out power flows calculations to analyze relevant events to draw conclusions for ex post evaluation report draft	Data processing	TSO / power flow analysis software	TSO / power flow analysis software	-	

D2.3 – Requirements and Detailed Architecture Design

6	Relevant events analysis has been completed	Ex post evaluation drafting by TSO	TSO uploads ex post evaluation report draft and request additional data from DSO to be included	Data uploading	TSO / IRIS communication platform	DSO / IRIS communication platform	24	
7	Ex post evaluation drafting by TSO has been completed	Ex post evaluation drafting by DSO	DSO returns to TSO completed ex post evaluation report draft and comments on TSO draft	Data uploading	DSO / IRIS communication platform	TSO / IRIS communication platform	25	
8	Ex post evaluation drafting by DSO has been completed	Submitting of ex post evaluation draft to NCA	TSO returns to NCA completed ex post evaluation report draft	Data uploading	TSO / IRIS communication platform	NCA / IRIS communication platform	26	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Identified national electricity crisis scenarios – request for scenarios, TSO proposal	See electricity crisis scenario definition	
2	Identified national electricity crisis scenarios – comments on TSO proposals, DSO and market participants' proposals	See electricity crisis scenario definition	
3	Identified national electricity crisis scenarios – completed document	See electricity crisis scenario definition	
4	Distribution IGM	See IGM definition	
5	Transmission IGM or CGM	See IGM and CGM definition	
6	Remedial actions	See RA definition	
7	Crisis scenario impacts	The most likely impacts of the crisis scenario i.e. potential consequences	

D2.3 – Requirements and Detailed Architecture Design

8	Agreed remedial actions – acknowledgement	See the definition	
9	Assessed frequency of occurrence of an crisis scenario initiating event	-	
10	Expected energy not served percentage (EENS%)	The EENS is defined as the expected amount of energy not being served to consumers by the system during the period considered due to system capacity shortages or unexpected severe power outages.	
11	Loss of load expectation (LOLE)	LOLE equals the expected number of loss-of-load days with events, regardless of event length, in a given year	
12	Crisis scenario likelihood	The probability of the occurrence of a certain electricity crisis scenario	
13	Crisis scenario likelihood – acknowledgement	See information no. 12	
14	Direct operational impact – acknowledgement	See information no. 7	
15	Crisis scenarios descriptions – proposal	See the definition	
16	Crisis scenarios descriptions – comments	NCA, NRA, DSO and market participants comments on scenarios descriptions	
17	Risk-preparedness plan	See Risk-preparedness plan definition	
18	Crisis – early warning	See electricity crisis definition	
19	Crisis – early warning acknowledgement	See electricity crisis definition	
20	Declaration of an electricity crisis – warning	See electricity crisis definition	
21	Declaration of an electricity crisis – announcement	See electricity crisis definition	
22	Agreed remedial actions – acknowledgement	See RA definition	

D2.3 – Requirements and Detailed Architecture Design

23	Ex post evaluation report – template	See ex post evaluation report definition	
24	Ex post evaluation report – drafted by TSO	See ex post evaluation report definition	
25	Ex post evaluation report – complemented by DSO	See ex post evaluation report definition	
26	Ex post evaluation report – completed document	See ex post evaluation report definition	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
Individual Grid Model (IGM)	Individual Grid Model (IGM) means a data set describing power system characteristics (generation, load and grid topology) and related rules to change these characteristics during remedial actions optimization process, prepared by the responsible TSO, to be merged with individual distribution grid models in order to create the common grid model (reformulated definition of EU regulation 2015/1222 to fit this use case needs).
Common Grid Model (CGM)	Common Grid Model (CGM) means a data set agreed between TSO and various DSOs describing the main characteristic of the power system (generation, loads and grid topology) and rules for changing these characteristics during the remedial action optimization process (reformulated definition of EU regulation 2015/1222 to fit this use case needs).
CGMES	The CGMES (Common Grid Model Exchange Specification) is an IEC technical specification (TS 61970-600-1, TS 61970-600-2) based on the IEC CIM (Common Information Model) family of standards. It was developed to meet necessary requirements for TSO data exchanges in the areas of system development and system operation.

D2.3 - Requirements and Detailed Architecture Design

Remedial Actions (RA)	Remedial action is any measure applied by a TSO or DSOs, manually or automatically, in order to maintain operational security, as well as to relieve physical congestion on their networks (reformulated definition of EU regulation 2015/1222 to fit this use case needs).
Electricity crisis	Electricity crisis means a present or imminent situation in which there is a significant electricity shortage, as determined by the EU Member States or Energy Community contracting party and described in their risk-preparedness plans, or in which it is impossible to supply electricity to customers;
Electricity crisis scenario	Detailed proposal on crisis scenario description according to EU regulation 2019/941 Article 5(2)
Risk preparedness plan	Plan drafted according to EU regulation 2019/941 Articles 10-13
Ex post evaluation report	Report drafted according to EU regulation 2019/941 Article 17

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.36 USE CASE 36 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
36	Transmission / Operation	Validation of network model integrity

1.2 Version management

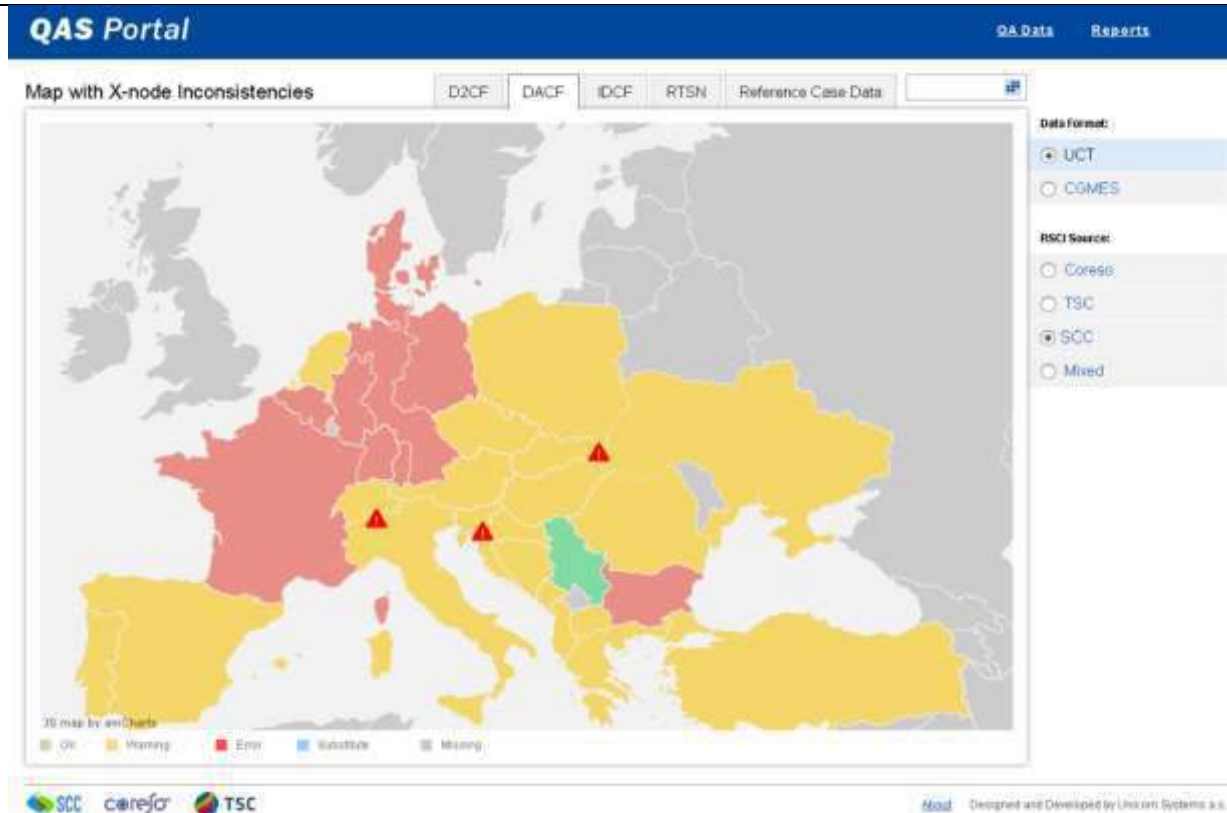
Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	10.03.2023	SCC	Initial version	SCC proposal
0.2	06.04.2023	SCC	First full version	UC36 development is agreed between GUARD and SCC
0.3	10.04.2023	GUARD	Update of full version	Version 02 approved by GUARD
0.4	11.04.2023	SCC	Version submitted on Alfresco for review	Version approved by GUARD and SCC
0.5	20.04.2023	EMSS, GUARD, SCC	SCC made changes based on EMSS and GUARD comments	Version approved by SCC
0.6	16.06.2023	SCC	Actor additional actor list is added in track	Version approved by EMSS and SCC
0.7	19.06.2023	GUARD	Changes accepted	Approved by GUARD
0.8	29.06.2023	GUARD	Merge of scenario 1 and 2	Approved
0.9	05.07.2023	EMSS	Harmonization of KSI application	Approved
0.10	07.07.2023	GUARD	Changes agreed and confirmed	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Introduce verification process of data integrity using blockchain technology in TSO-RCC operational planning procedures.
Objective(s)	Implement an application for signing files on the side of the file producer and application for the verification of data integrity on the side of the file receiver.
Related business case(s)	BC1, BC3

1.4 Narrative of use case

Narrative of use case
Short description <p>In order to improve network model cybersecurity, TSOs and RCCs could use KSI Blockchain technology to create KSI signature file, which represents unique cryptographic proof that protects integrity, signing time and signing identity of the network model. Confidential network model is created by file producer, signed, and forwarded to the file receiver together with KSI signature file, which can be then used to solve problems of integrity, provenance, security, immutability, and audit. File receiver uses proofs to validate the model to ensure that it is original and not tampered or changed (accident, malicious change, bit flip, corruption, etc). Even if a single bit in data or in proof has been changed then verification would result in error with corresponding message, allowing the file receiver (or whoever performs verification) to start an investigation.</p>
Complete description <p>Individual Grid Model (IGM) is "a data set describing power system characteristics (generation, load and grid topology) and related rules to change these characteristics during capacity calculation, prepared by the responsible TSOs", according to the definition from the EU Regulation 2015/1222. IGMs are statistical mathematical models, created in order to represent the forecasted state of the TSO power system for a defined timestamp and a given forecast time horizon (intraday – several hours ahead, day ahead, two days ahead, etc.).</p> <p>After creation by TSOs, IGMs are provided to RCCs in order to perform its validation (checking for syntax and semantics errors). If some discrepancies from the predefined rules are detected, TSOs are informed about these issues via Quality Assessment Service (QAS) portal, so TSOs could provide expected corrections of IGMs. Figure F1 presents the look of SCC's QAS portal, where certain syntax and semantic errors of IGMs are displayed.</p>



After validation and correction of IGMs, the process of merging of IGMs is launched by one RCC. The result of this process is Common Grid Model (CGM), which is also validated using the QAS portal. CGM is the basis for all other RCC services, since all of them include load flow calculations. Currently, on ENTSO-E level, CGM creation is organised based on rotational principle, which means that one Main RCC produces necessary CGMs and delivers them to all other RCCs and all TSOs. This means that CGMs are created by different RCCs each month. CGMs are then used by all RCCs and all TSOs in order to provide other services (outage planning, cross-border capacity calculation, regional operational security coordination, etc.), so it could be concluded that in the process of network model exchange there are 2 sides:

File producers are:

- All TSOs regarding IGMs,
- Main RCC regarding CGMs;

File receivers are:

D2.3 – Requirements and Detailed Architecture Design

- Main RCCs regarding IGMs and all RCCs regarding CGMs,
- All TSOs regarding CGMs.

IGMs and CGMs are considered confidential data. The process of network model validation does not include data integrity checking, so this cybersecurity test is planned to be introduced via this UC. Validation of network model integrity will be done in two connected cycles of data exchange:

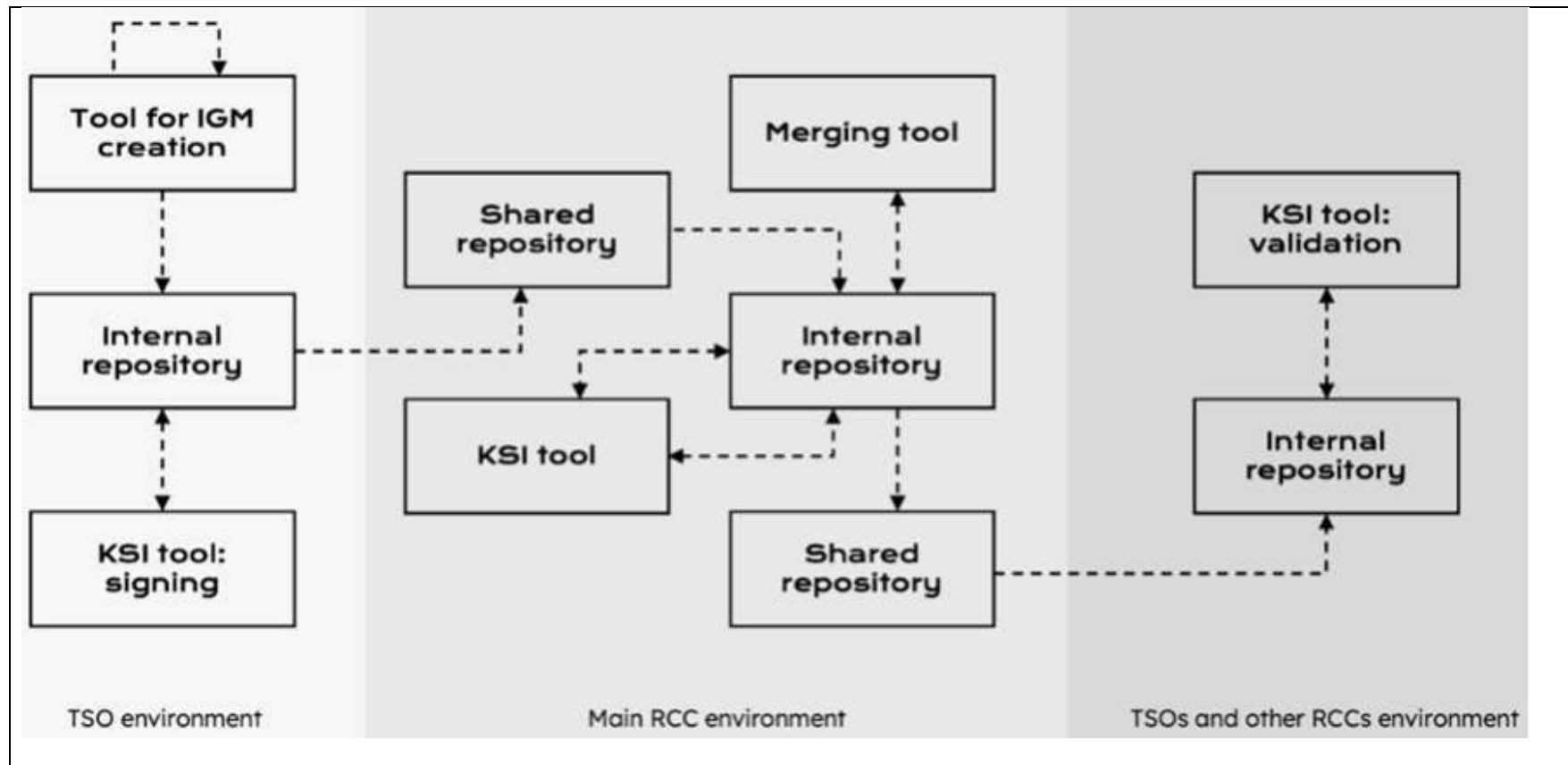
First cycle – IGM validation:

- TSO creates IGM,
- Using KSI Blockchain technology TSO signs the IGM and creates KSI signature file,
- IGM and KSI signature file are delivered to main RCC,
- Main RCC performs file integrity validation and proves that untampered IGM is used;
- KSI signature file is stored on the RCC system as a proof.

Second cycle – CGM validation:

- Main RCC creates CGM,
- Using KSI Blockchain technology main RCC signs the CGM and creates KSI signature file,
- CGM and KSI signature file are delivered to other RCCs and all TSOs,
- Other RCCs and all TSOs perform file integrity validation and prove that untampered CGM is used.
- KSI signature file is stored on the RCC and TSO system as a proof.

All other ways of using blockchain technology for network model integrity (e. g. in interaction between file producer and tool vendor during testing of the tool dedicated for creation of the mentioned file) will be explored during the development phase of this UC.



1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
This UC does not address the process of IGM/CGM creation.
This UC does not relate to the IGMs/CGMs created in CGMES file format, but only to the IGMs/CGMs created in UCTE file format.
Prerequisites
File producer environment must have internet access, since internet connection is needed for the signing process.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
Medium.
Prioritisation
4
Generic, regional, or national relation
Generic
Nature of the use case
Description of the business cases and general components of the system.
Further keywords for classification
IGM, CGM, data integrity, RCC services

1.8 General remarks

General remarks
Expected value for the TSO and RCC: The ability to respond to malicious activity, human error, and general data corruption if network planning is based on false or broken data. This leads to reducing energy service disruptions and damage.
Provides evidence that can be used to solve disputes between network participants.
It is possible to enable third-party auditability and regulatory aspects (at a national or EU level).

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Transmission System Operator (TSO) – EMSS	System operator	‘Transmission system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)	TSOs perform following tasks: <ul style="list-style-type: none"> ● First cycle – IGM validation: TSO creates IGM, Using KSI Blockchain technology TSO signs the IGM and creates KSI signature file, TSO delivers IGM and KSI signature file to main RCC; ● Second cycle – CGM validation: CGM and KSI signature file are delivered to TSOs, TSOs perform file integrity validation and prove that untampered CGM is used. KSI signature file is stored on the TSO system as a proof.
Regional coordination centre (RCC) – SCC	Regional coordination body	‘Regional coordination centre’ means regional coordination centre established pursuant to Article 35 of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal	RCC perform following tasks: <ul style="list-style-type: none"> ● First cycle – IGM validation: IGM and KSI signature file are delivered to main RCC, Main RCC performs file integrity validation and proves that untampered IGM is used;

D2.3 – Requirements and Detailed Architecture Design

		market for electricity. Regional coordination centres shall complement the role of transmission system operators by performing the tasks of regional relevance assigned to them.	<p>KSI signature file is stored on the RCC system as a proof.</p> <ul style="list-style-type: none"> • Second cycle – CGM validation: Main RCC creates CGM, Using KSI Blockchain technology main RCC signs the CGM and creates KSI signature file, CGM and KSI signature file are delivered to other RCCs, Other RCCs perform file integrity validation and prove that untampered CGM is used. KSI signature file is stored on the RCC system as a proof.
--	--	--	--

Grouping		Group description	
Software and hardware		Software and hardware used in the validation of network model integrity	
Actor name	Actor type	Actor description	Further information specific to this use case
IGM creation tool	Software	Desktop application specialised for creation of IGMs.	TNA tool will be used to create IGMs using data of TSO equipment, production, consumption, exchanges and topology status.
Shared repository	File server	File server is a computer attached to a network that provides a location for shared disk access, i.e. storage of computer files that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network.	Dedicated location/directory/folder on file server will be used as shared repository where other actors could access and download/upload data.

D2.3 – Requirements and Detailed Architecture Design

TSO Internal repository	File server	File server is a computer attached to a network that provides a location for shared disk access, i.e. storage of computer files that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network.	Dedicated location/directory/folder on file server will be used as internal repository for storing final data and reports in TSO.
RCC Internal repository	File server	File server is a computer attached to a network that provides a location for shared disk access, i.e. storage of computer files that can be accessed by the workstations that are able to reach the computer that shares the access through a computer network.	Dedicated location/directory/folder on file server will be used as internal repository for storing final data and reports in RCC.
Merging tool (CGM creation tool)	Software	Server application specialised for creation of CGMs.	eTNA tool will be used to create CGMs using IGMs.
KSI Tool	Software	KSI Tool is used to sign and validate models.	Tool signs the data and returns unique signatures that are later used to validate the model's integrity. If IGM or CGM access is requested, KSI Tool is used to perform an integrity check using previously provided unique signatures.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	IGM and CGM validation	This scenario covers the process of integrity validation of IGM and CGM	TSO, RCC, Other TSO and RCC	Input data necessary for the IGM creation are available and the time has come for TSO to create IGM for some future timestamp according to the operational procedure. Input data necessary for the CGM creation are available and the time has come for Main RCC to create CGM for some future timestamp according to the operational procedure.	TSO has all necessary information about expected topology, exchanges, production and consumption for its transmission system. Main RCC has information about scheduled net positions for all TSOs in the Continental Europe Synchronous Area, including IGMs for all TSOs from that area for the upcoming timestamps	Integrity of IGM is confirmed on the RCC side. The integrity of CGM is confirmed on the TSO and other RCC sides.

4.2 Steps – Scenarios

Scenario								
Scenario name:		IGM and CGM validation						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs

D2.3 - Requirements and Detailed Architecture Design

1	Input data necessary for the IGM creation are available and the time has come for TSO to create IGM for some future timestamp according to the operational procedure.	TSO creates IGM	Using information about expected topology, exchanges, production and consumption of its transmission system, TSO creates IGM for some future timestamp according to the Intraday or Day ahead congestion forecast procedure.	Data import, file format conversion and load flow calculation	TSO)	TSO (IGM creation tool)	1	
2	IGM is created	IGM storing	Created IGM is stored in TSO internal repository	Data transmission	TSO (IGM creation tool)	TSO (TSO internal repo)	2	
3	IGM is stored	TSO creates KSI signature file	Using the KSI tool and IGM as input file, TSO creates KSI signature file that represents an unchangeable proof of data integrity.	Execution of KSI tool signing function	TSO (TSO internal repo)	TSO (KSI tool)	2	
4	KSI signature file is created	KSI tool returns signature	KSI signature file is returned	Execution of KSI tool signing function	TSO (KSI tool)	TSO (TSO internal repo)	3	
5	Both, IGM and KSI signature files, exists in the repository	TSO uploads IGM and KSI signature file	TSO uploads IGM and KSI signature file to the shared repository for the Main RCC to access these.	Data upload	TSO (TSO internal repo)	Main RCC (Shared repo)	2, 3	
6	IGM and KSI signature file are downloaded from repositories	Main RCC downloads IGM and KSI signature	Main RCC downloads IGM and corresponding signature from share repo to internal repo	Data download	Main RCC (Shared repo)	Main RCC (RCC Internal repo)	2, 3	

D2.3 - Requirements and Detailed Architecture Design

			for validation and further use.					
7	IGM and KSI signature file are downloaded from repositories	Main RCC performs file integrity validation	Using the KSI tool, RCC performs IGM integrity validation.	Execution KSI tool verification function	Main RCC (RCC Internal repo)	Main RCC (KSI tool)	2, 3	
8	Validation of IGM integrity is performed	KSI tool returns validation result.	Based on the verification outcome, the KSI tool returns the result that is stored in a database.	Execution KSI tool verification function	Main RCC (KSI tool)	Main RCC (RCC Internal repository)	4	
9	Input data necessary for the CGM creation are available and the time has come for Main RCC to create CGM for some future timestamp according to the operational procedure	Main RCC creates CGM	Using scheduled net positions and IGMs from all TSOs in the Continental Europe Synchronous Area, Main RCC creates CGM for some future timestamp according to the Intraday or Day ahead congestion forecast procedure.	Data import from internal repository, file format conversion and total adjustment and load flow calculation	Main RCC (RCC Internal repository)	Main RCC (Merging tool)	2	
10	CGM is created	CGM storing	Created CGM is stored in RCC internal repository	Data transmission	Main RCC (Merging tool)	Main RCC (RCC Internal repository)	5	
11	CGM is stored	Main RCC creates KSI signature file	Using the KSI tool and CGM as input file, Main RCC creates KSI signatures that represent an unchangeable proof of data integrity.	Execution KSI tool signing function	Main RCC (RCC Internal repository)	Main RCC (KSI tool)	6	

D2.3 - Requirements and Detailed Architecture Design

12	KSI signature file is created	KSI tool returns the signature	KSI signature file is returned to Main RCC	Execution KSI tool signing function	Main RCC (KSI tool)	Main RCC (RCC Internal repository)	3	
13	CGM and KSI signature is delivered to the shared repository	Main RCC sends CGM and KSI signature to shared repository	CGM is sent to the shared repository.	Data upload	Main RCC (RCC Internal repository)	Main RCC (Shared repository)	6	
14	Both, CGM and KSI signature files, exists in the repository	TSOs and other RCCs take CGM and KSI signature file from shared repositories	TSOs and other RCCs download CGM and KSI signature files, each from its own repository.	Data download	Main RCC (Shared repositories)	TSOs and other RCCs (TSO/RCC internal repository)	3, 6	
15	CGM and KSI signature file are downloaded from repositories	TSOs and other RCCs perform file integrity validation	Using the KSI tool, TSOs and other RCCs perform CGM integrity validation.	Execution KSI tool verification function	TSOs and other RCCs (TSO/RCC internal repository)	TSOs and other RCCs (KSI tool)	3, 6	
16	Validation of CGM integrity is performed	KSI tool returns validation result.	Based on the verification outcome, the KSI tool returns the results that is stored in a database.	Execution KSI tool verification function	TSOs and other RCCs (KSI tool)	TSOs and other RCCs (internal repository)	4	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Information about expected topology, exchanges, production and consumption	In order to created new IGM, beside equipment parameters (which are static throughout the year), following variable (on the hourly level) information is needed on TSO level:	

D2.3 – Requirements and Detailed Architecture Design

		Topology – planned energization status of overhead lines and transformers, Exchanges – forecasted values of active and reactive power flows on interconnection lines, Production – active and reactive production of all generating units, Consumption – active and reactive consumption of all network nodes.	
2	IGM	Individual Grid Model (IGM) is "a data set describing power system characteristics (generation, load and grid topology) and related rules to change these characteristics during capacity calculation, prepared by the responsible TSOs", according to the definition from the Regulation 2015/1222.	
3	KSI signature file	KSI signature file is a cryptographic proof for signing time and integrity. KSI Blockchain technology uses only hash functions, meaning that no user data would be stored in signature nor in blockchain. Document hash is registered in KSI Blockchain which returns a unique signature as a result. The size of the signature is around 2.5 kB.	
4	Integrity validation result	The integrity validation result represents two possible outputs. If a signed data (e.g. IGM or CGM) has been changed (by error, mistake or cyber-attack) the verification returns an error which indicates that the data is not the original signed version. Integrity check returns an OK response if integrity verification is successful.	

D2.3 – Requirements and Detailed Architecture Design

5	Scheduled net positions	<p>Net Position is the netted sum of electricity exports and imports for each market time unit for a bidding zone.</p> <p>The output of a market coupling process, i.e. energy exchanges, results in new requirements for TSOs and market coupling operators (scheduled "net positions").</p> <p>Scheduled "net positions" is a multilateral exchange between one scheduling area and a group of other scheduling areas involved in market coupling.</p>	
6	CGM	<p>Common Grid Model (CGM) is defined as a "Union-wide data set agreed between various Transmission System Operators (TSOs) describing the main characteristic of the power system (generation, loads and grid topology) and rules for changing these characteristics during the capacity calculation process", according to the definition from the Regulation 2015/1222.</p> <p>The CGM is not only used for operational tasks but also for market and asset management/grid planning activities like: operational security calculations, capacity calculations, outage coordination.</p>	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
CGM	Common Grid Model is defined as a “Union-wide data set agreed between various Transmission System Operators (TSOs) describing the main characteristic of the power system (generation, loads and grid topology) and rules for changing these characteristics during the capacity calculation process”, according to the definition from the Regulation 2015/1222.
ENTSO-E	European Network of Transmission System Operators for Electricity represents 39 electricity transmission system operators (TSOs) from 35 countries across Europe, thus extending beyond EU borders. ENTSO-E was established and given legal mandates by the EU's Third Package for the Internal energy market in 2009, which aims at further liberalising the gas and electricity markets in the EU.
EU	European Union is a supranational political and economic union of 27 member states that are located primarily in Europe.
IGM	Individual Grid Model is "a data set describing power system characteristics (generation, load and grid topology) and related rules to change these characteristics during capacity calculation, prepared by the responsible TSOs", according to the definition from the Regulation 2015/1222.
KSI	KSI is a blockchain technology designed in Estonia and used globally to ensure networks, systems, and data are free of compromise, all while retaining 100% data privacy. A blockchain is a distributed public ledger – a database with a set of pre-defined rules for how the ledger is appended by the distributed consensus of the participants in the system. Due to its widely witnessed property, blockchain technology makes it also impossible to change the data already on the blockchain. With KSI Blockchain deployed in Estonian government networks, history cannot be rewritten by anybody and the authenticity of the electronic data can be mathematically proven. It means that nobody – neither hackers, nor system administrators, nor even the government itself – can manipulate the data and get away with it.
QAS	Quality Assessment Service portal is web application designed and developed by Unicorn Systems a. s. in order to present validation results of IGMs and CGMs to the dedicated users.



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.37 USE CASE 37 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
37	Distribution DER / Enterprise, Operation, Station, Field, Process	Energy data tokenization

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	24.02.2023	HEDNO	Preliminary idea of needs	
0.2	31.03.2023	GUARD	UC description with GUARDS perspective	
0.3	04.04.2023	HEDNO	Review and update existing definition	Approved
0.4	05.04.2023	GUARD	Respond for clarifications	Approved
0.5	06.04.2023	HEDNO	Finalisation of UC definition	Approved
0.6	12.04.2023	GUARD, HEDNO	Finalisation of UC definition	Approved
0.7	24.04.2023	HEDNO	Respond to comments and proposed minor changes	Approved
0.8	28.04.2023	GUARD	Minor changes proposed under 4.2	Approved
0.9	27.04.2023	GUARD	Added preliminary requirements, updated 3.1, 4.1 – 5.0, added some comments	Approved
1.0	03.05.2023	HEDNO	Respond to comments and proposed minor changes	Approved

D2.3 - Requirements and Detailed Architecture Design

1.1	03.05.2023	HEDNO, GUARD	Revision done by HEDNO, agreed to move next phases with UC	Approved
-----	------------	--------------	--	----------

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	The scope of this Use Case is the enhancement of the DSO's data protection. Data to be secured for the network operator involve SCADA system, as well as AMI from telemetered customers.
Objective(s)	Improved DSO's trust in data. Even if a single bit of data is changed, by mistake or through attack, next verification would return an error indicating that data could not be trusted. Successful verification indicates that data can be used for analysis, investigations or billing validation without having concerns in data manipulation.
Related business case(s)	BC1, BC3

1.4 Narrative of use case

Narrative of use case
Short description Collected energy measurements data from telemetered clients (AMI - smart meters) and SCADA systems are stored in DSO's internal databases. Measurement interval varies from 15 to 30 minutes depending on measurement point. Collected data is stored for at least a couple of months to several years depending on data type and governing regulations. Data is stored for plenty of purposes, such as analytics, or even billing verification. Consumption data provided by AMI, give the network operator the ability to have increased observability over the power consumed by the customer, and thus contribute to the reduction of fraudulent behaviours. The data from smart meters can also be used by network operators for the utilisation of potential flexibility and demand side management, or even for the participation of a customer to a local flexibility market. Finally, data from SCADA are of utmost importance for the DSO, as power flow analysis over the MV lines and possible necessary remote control commands are strongly dependent on them. It is crucial for DSO to have absolute trust in stored data to perform aforementioned activities and to take decisions based on the results. Blockchain technology is used to deliver the added trust factor for the collected and stored data by applying data registration in blockchain (data itself is not stored on blockchain, instead tokens are issued) and provenance of data registrations (each data entry from specific measurement point is linked together) making the data entries immutable and verifiable, periodically and before use.

Complete description

Cyber security is a critical aspect for DSO systems nowadays. As both IT and OT are continuously being upgraded, cyber security enhancement is considered of high priority. The DSO's policies and next-year strategies around cyber security involve cyber-risk management and awareness, in line with ISO 27110, ISO 27001 Standards, as well as with NIS and NIS-2 Directive. The main vulnerabilities concerning the grid operator are the following ones: A cyber attack, conducted by a malicious outside user, could affect the quality of data exchanged between the systems. Moreover, an internal incident, i.e. a user mistake or even a not normal backup process execution, may lead to data corruption, and as a result is also one of the major concerns of a DSO.

For the scope of the R2D2 Project and due to security policies applied by the Greek DSO, a replica of the actual system is built, where all real data from Xanthi SCADA are being stored. Furthermore, data from AMI for all available telemetered MV and major LV customers are stored as well. As a result, datasets from both SCADA measurements and AMI are simulated in an isolated environment to be examined for pilot purposes, where the same policies and Standards with the actual systems are applied.

Use case implementation has to follow the DSO data use patterns and needs. For that, DSO shall describe the needs for tokenization: different datasets that are being collected (size, data format, etc) from telemetered clients and SCADA system, collection intervals, data grouping (data from different clients in single entry or independently, or even preferably with a unique customer ID); and interfacing possibilities and needs in order to consume the service. GUARD needs these inputs to adjust the overall architecture and development approach.

Overall process:

- DSO collects data from measurement points;
- These data entries are tokenized with blockchain to provide immutability proofs for the data. Tokenization process could also:
- link together the data entries to form an immutable chain for further strengthening the integrity protection.;
- Tokenize entries individually (each collection round) or in bulk (daily basis (e.g. data from AMI per customer));
- Tokenization process returns cryptographic proofs (tokens) for integrity and registration time verification;
- Tokens are stored in the database, either with the data or independently. In either case there is a need to keep the link between data and its tokens;
- These tokens are later used for data verification that is configured to occur periodically or on demand (before use),
- If there are changes in data or modification to tokens then data verification would return an error indicating that data could not be trusted;
- Otherwise verification returns with an OK message indicating that data is intact and it could be trusted.

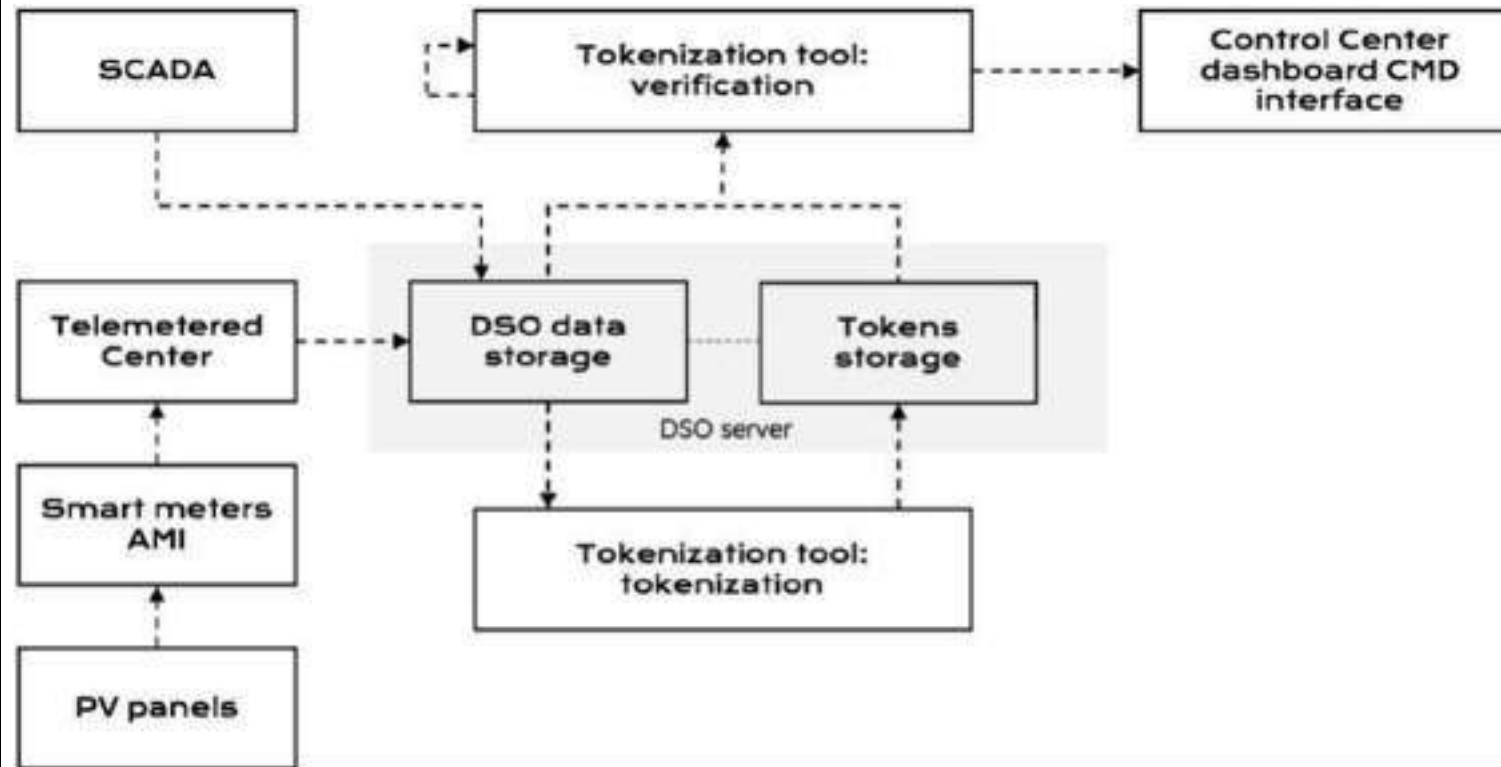
DSO defines and describes:

- Data format and metadata;
- Data grouping: single measurement point or multiple;
- Registration interval and granularity (collection interval or once a day), this will affect storage overhead;
- Provenance need, identification of data source;
- Verification needs (offline, online);

D2.3 - Requirements and Detailed Architecture Design

- Interfacing options and possibilities of the used systems and solutions in order to tokenize and verify data.
- GUARD defines and describes:

- Request/response endpoints for tokenization, verification, and any other that may be needed;
- Environment requirements to deploy the software (SW & HW);
- Suggestions on how to link data and its tokens.



1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
The energy data tokenization Use Case will be examined in a simulated environment (replica of the actual SCADA system), due to security policies
Prerequisites
SCADA data availability
AMI data availability for all pilot's telemetered customers

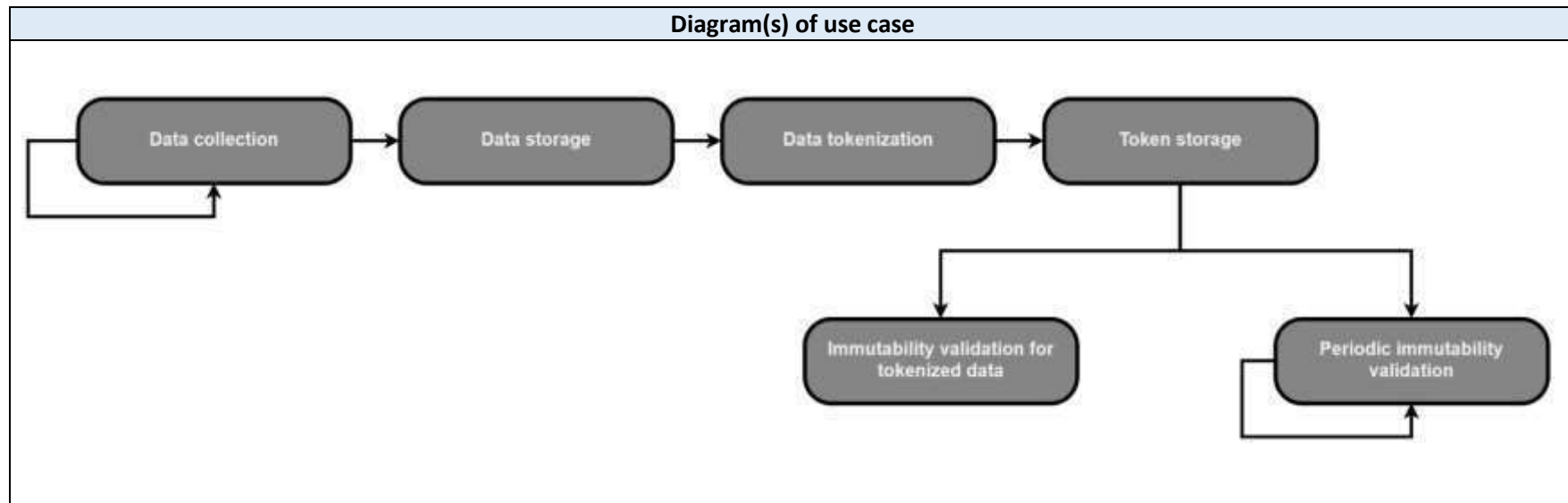
1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
Level of depth
high
Prioritisation
5
Generic, regional or national relation
National – to be examined only in the region of the pilot
Nature of the use case
This UC indicates certain functionalities of the PRECOG R2D2 toolkit.
Further keywords for classification
Data tokenization, data protection, Cyber-security enhancement

1.8 General remarks

General remarks

2. Diagrams of use case



SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
DSO	System Operator	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity.	The DSO is responsible for the security of data stored in its databases. In this UC, a replica of the actual system will be used for pilot purposes, where all data from SCADA and AMIs will be collected and stored.
Grouping		Group description	
Tools		Tools represent a system component(s) that participates in a business transaction. Within a given business transaction a tool assumes a specific function or a set of functions.	
Actor name	Actor type	Actor description	Further information specific to this use case
Tokenization tool (PRECOG)	Cybersecurity, data protection	Part of a PRECOG toolset, it is a cybersecurity tool that provides tokenization mechanisms for the data to protect its immutability. Provides verification mechanisms to validate data integrity and tokenization time of data.	Responsible for tokenizing the provided data, it returns a token for later integrity and time verification. Provides verification mechanisms for the tokenized data and associated token, verification returns verification results that are either OK or error. In case of errors a specific error code and message is returned.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Tokenization of measurement data	DSO collects data from measurement points and tokenizes it to provide immutability proofs for that data.	DSO	Time trigger to collect data	There is collected data from measurement points and rules defined for storage and protection	Data is being tokenized periodically according to defined rules. Data and tokens are stored in database(s) and ready for automatic and manual immutability checks.

4.2 Steps – Scenarios

Scenario								
Scenario name:		Tokenization of measurement data						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Time trigger to collect data	Data collection	DSO collects data from measurement points: SCADA systems and AMI smart metres.	Automatic data collection services.	DSO	DSO	1	
2	New data received	Data storage	New measurement data is stored in the database.	Data storage.	DSO	DSO	1	
3	Data tokenization	Data tokenization	New measurements are stored in the database and data tokenization tool tokenizes the data based on defined tokenization rules. Tokenization process returns a token for later validation.	Tokenization process (Tokenization tool (PRECOG))	DSO	DSO / Tokenization tool (PRECOG)	1, 2	
4	Token is received from the tokenization process.	Token storage	Token is stored in the database keeping the link between tokenized data and token itself.	Tokenized Data storage	DSO / Tokenization tool (PRECOG)	DSO	2	
5	Data access or use.	Immutability validation for tokenized data	There is a need to access and use the data, before that data immutability shall be validated. Validation returns an OK result if there are no errors found.	Immutability validation (Tokenization tool (PRECOG))	DSO	DSO	1, 2	

D2.3 - Requirements and Detailed Architecture Design

6	Time trigger event	Periodic immutability validation	Processes could be running in the background to periodically validate the stored data, e.g. once a week, to find any data corruption or changes in the database sooner rather than later whenever the data is being accessed or used.	Immutability validation (Tokenization tool (PRECOG))	DSO	DSO	1, 2	
7	Step nr. 5 or 6 completed	Result of validation	Tokenization tool returns a message (OK or error) to indicate whether the data is original or not.	Immutability validation (Tokenization tool (PRECOG))	Immutability validation (Tokenization tool (PRECOG))	DSO	3	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	SCADA and AMI data	SCADA data: periodic measurements, involving the pilot MV lines. More specifically, for the main feeder of each pilot MV line S, V, I are available with time granularity of 30min. AMI data: periodic measurements of MV and major LV telemetered customers. More specifically P, Q for each telemetered client, as well as V, I for some of them. Time granularity 15min	
2	Tokens	Tokens represent cryptographic proofs for data integrity and registration time. Tokens are stored in the database, either with the data or independently. In either case there is a need to keep the link between data and its tokens.	



D2.3 - Requirements and Detailed Architecture Design

3	Tokenization validation message	Tokenization tool returns a message (OK or error) to indicate whether the data is original or not.	
---	---------------------------------	--	--

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition

8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.38 USE CASE 38 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
38	Distribution, DER / Enterprise, Operation, Station, Field, Process	DSO grid balancing data tokenization

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	14.06.2023	GUARD	Creation of UC	
0.2	20.06.2023	ELEK	Revision done	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	This UC will involve distribution systems infrastructure (both OT and IT) dealing with balancing the energy within the nominal operational parameters at DSO level. Dispatchable producers and consumers enabled to provide balancing services for the distribution network are also involved in the UC.
Objective(s)	O1 - To provide authenticity proofs for grid balancing messages that DSO is publishing for participants in grid operation, mainly intended for the energy producers and balancers.
Related business case(s)	BC3

1.4 Narrative of use case

Narrative of use case
Short description
Providing cryptographic proofs to energy grid data so it can be trusted by all the parties involved in the energy production, balancing and generation process. A data authenticity validation is needed for both, solving disputes and for auditing purposes.
Complete description
<p>Slovenian pilot collects consumption, production and energy quality data and stores it in internal data storage. Energy quality is being assessed periodically and in case of intervention requests to either decrease or increase energy production or balancing is generated and sent out to grid participants. This data is then used for business related activities according to the request by DSO.</p> <p>The Slovenian energy grid balancing legislative framework is based on the Resolution on the National Energy Programme 1 (ReNEP), the Energy Act 2 EZ-1) and the Environment Protection Act 3 (ZVO1). Five Slovenian electricity distribution companies own the distribution grid and rent it to the DSO, who operates it as a public utility service. All the generators, distributors and suppliers, as well as the TSO, are predominantly or wholly state-owned and no international investment is present. Due to the level of state ownership, the whole electricity sector is arguably fully vertically integrated.</p> <p>Based on the current market status the approach is that it is important for anyone to trust the data and to be sure the provided data is authentic and has not been changed (by error, intentional, mistake or cyber-attack). GUARD offers tokenization technology that creates unique cryptographic proofs that protects published data integrity, signing time and origin.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Grid balance data is being shared between DSO<-->RES.
Message sharing platform in operation (User accounts database communication).
Market participant's motivation for trading based on rules and demand.
Grid balancing data not trusted by grid participants
Prerequisites
Energy data available for energy quality assessment to derive the balancing decisions.



D2.3 – Requirements and Detailed Architecture Design

Server environment to deploy needed services, for tokenization and validation.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
UC37 Energy data tokenization
Level of depth
Specialised use case
Prioritisation
3 (medium)
Generic, regional or national relation
Generic, National
Nature of the use case
Technical use case
Further keywords for classification

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
System Operator	Role	A party responsible for operating, ensuring the maintenance of and, if necessary, developing the system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution or transmission of electricity.	
Consumer	Role	A party that consumes energy.	In this UC, the consumer is enabled to provide balancing services
Producer	Role	A party that generates energy.	In this UC, the producer is enabled to provide balancing services
Grouping		Group description	
Tools		Tools represent a system component(s) that participates in a business transaction. Within a given business transaction a tool assumes a specific function or a set of functions.	
Actor name	Actor type	Actor description	Further information specific to this use case
Tokenization tool (PRECOG)	Application	Part of a PRECOG toolset, it is a cybersecurity tool that provides tokenization mechanisms for the data to protect its immutability. Provides verification mechanisms to validate data integrity and tokenization time of data.	Responsible for tokenizing the provided data, it returns a token for later integrity and time verification. Provides verification mechanisms for the tokenized data and associated token, verification returns verification results that are



D2.3 – Requirements and Detailed Architecture Design

			either OK or error. In case of errors a specific error code and message is returned.
Balancing data creation system	Application	SW component responsible for the calculation and identification of the balancing capacity to request to the balancing providers	
DSOs server	Server	A computer program or device that provides a service to another computer program and its user, also known as the client.	DSOs internal database

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Tokenization of energy grid balancing data	Energy production, consumption and quality data is collected and stored. This data is being continuously assessed and balancing data is derived from it. Balancing data is then tokenized and stored in the database with the token. When data is being shared with grid participants it is published with associated tokens for participants to validate data integrity, origin and signing time, providing trust for the data.	DSO	Time trigger to collect data. Creation of balancing data	Collected production, consumption and quality data is stored, assessed and balancing data is derived	Balancing data is tokenized periodically according to defined rules. Data and tokens are stored in database(s) and ready for automatic and manual immutability checks.

4.2 Steps – Scenarios

Scenario								
Scenario name:		Tokenization of energy grid balancing data						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Time trigger to collect data	Collection of energy production, consumption and quality data	Energy production data is automatically collected by producers and then shared with DSO. Energy consumption data is collected by DSO. All collected data is stored in DSOs internal database.	Automatic data collection services	DSO Producer	DSO (DSOs internal database)	1	
2	Collection of energy production, consumption and quality data	Assessment of energy production, consumption and quality data	Grid balancing data is created based on existing data	Data assessment and grid balancing data creation	DSO	DSO (DSOs internal database)	1, 2	PRE_006
3	Grid balance assessment result tokenization	Tokenization of grid balancing data	Tokenization reads the data and tokenizes it based on defined tokenization rules. Tokenization process returns a token for validation	Tokenization process (Tokenization tool (PRECOG))	DSO	DSO (Tokenization tool (PRECOG) and DSOs internal database)	2, 3	Pilot to follow: <ul style="list-style-type: none"> • PRE_002 or PRE_003 • PRE_004 • PRE_005 • PRE_011 GUARD to follow: PRE_011
4	Token is received from the tokenization process.	Token storage	Token is stored in DSOs internal database keeping the link between tokenized grid balancing data and token itself.	Tokenized Data storage	DSO (Tokenization tool (PRECOG))	DSO	3	Pilot to follow: PRE_012

D2.3 – Requirements and Detailed Architecture Design

5	Data access or use by DSO or other grid participant	Data validation for tokenized grid balancing data	Balancing data validation against the token for its authenticity.	Authenticity validation (Tokenization tool (PRECOG))	DSO (Tokenization tool (PRECOG))	DSO Other grid participant	2, 3	Pilot to follow: <ul style="list-style-type: none"> • PRE_011 GUARD to follow: <ul style="list-style-type: none"> • PRE_009 • PRE_011 Other grid participant to follow: <ul style="list-style-type: none"> • PRE_011
---	---	---	---	--	----------------------------------	-------------------------------	------	--

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Energy production, consumption and quality data		
2	Grid balancing data		
3	Token	Tokens represent cryptographic proofs for data authenticity. Tokens are stored in the database, either with the data or independently. In either case there is a need to keep the link between data and its tokens otherwise it's not possible to validate data.	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.39 USE CASE 39 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
39		Innovative solution for OPDE Risk Register

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	01.12.2023	SCC	Initial version.	SCC proposal.
0.2	13.12.2023	EMSS	List of actors should be updated, as well as requirements. Several comments regarding scenarios.	Official revision of the UC – approved with comments.
0.3	18.12.2023	CyberNoesis	Few general comments on the UC.	Approved with comments.
1.0	03.01.2024	SCC	Finalisation of UC according to EMSS and CyberNoesis comments.	Approved.

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Improve communication process between ENTSO-E bodies and TSO/RCC representatives regarding information security risk treatment in line with OPDE Security Plan procedure that is established by the ENTSO-E.

D2.3 – Requirements and Detailed Architecture Design

Objective(s)	<p>Develop specific platform that could improve process of submission and update of risks related to OPDE by:</p> <ul style="list-style-type: none"> • Providing centralised place for all OPDE risks; • Making easier communication on dedicated risk issues among concern participants; • Providing access to the specific information based on the “need to know” principle; • Increasing traceability of changes regarding risk information; • Developing friendly user interface. <p>Design platform together with CyberNoesis and ENTSO-E information security experts. Implement platform in SCC premises and test it in front of ENTSO-E information security experts.</p>
Related business case(s)	BC3, BC4

1.4 Narrative of use case

Narrative of use case
<p>Short description</p> <p>In order to protect operational planning data from cyber-attacks, ENTSO-E developed OPDE platform. Information security protection of OPDE platform is based on the document “OPDE/ATOM Security Plan”, where a set of specific information security measures is defined. Each year independent external auditor is reviewing the implementation status of these information security measures at TSO and RCC operational environment (common name for TSOs and RCCs is in this context is Party). Each Party is obligated to provide update of existing information security risks and submission of new risks based on the independent auditor’s report.</p> <p>This process of submission and update of information security risks related to the OPDE platform is currently performed based on shared secured repository and exchange of .docx templates, which creates delay in risk review process and perplex communication between ENTSO-E information security bodies and Parties. This UC is focused on developing specialised IT tool that could support and improve monitoring and communication during risk treatment process that is currently established on the ENTSO-E level. OPDE Risk Register will be based on the following functionalities:</p> <ul style="list-style-type: none"> • Enable entry form for risk submission and modification; • Display all submitted risks and their information based on the “need to know” principle on centralised place; • Enable fast, secure and simple communication between users on the specific risk; • Log all changes of data in the system. <p>Complete description</p>

In past decade ENTSO-E recognized the need to protect TSOs' information-communication systems, IT networks and operational planning data from cyber-attacks. For the secure and optimal exchange of operational planning data between TSOs and RCCs, ENTSO-E has been developing the Operational Planning Data Environment (OPDE). The OPDE, specified by Art. 114 of the SOGL, is the information platform that is supporting the data exchange between TSOs and RCCs associated with the operational planning processes, especially with the process of creation of Common Grid Model. OPDE is also the foundation of the data exchange platform for running the five core services of RCCs. OPDE has been a platform for the best experience and practice sharing between TSOs' for strengthening of cybersecurity.

In order to access OPDE, all TSOs and RCCs signed "Minimum Viable Solution Agreement for OPDE and ATOM" (also known as MVS), where one of the annexes represent "OPDE/ATOM Security Plan" – a set of information security measures that should be fulfilled by every Party before granting its access to the OPDE. These information security measures are based on ISO/IEC 27001 standard, but they contain stricter requirements compared with this international standard. MVS and all annexes are confidential and cannot be distributed without appropriate reason and signing of NDA.

Each year, independent external auditor reviews the implementation status of information security measures at Parties' operational environment. Each Party is obligated to provide update of existing information security risks and submission of new risks based on the independent auditor's report. General information about the risk, risk description and planned mitigation strategy are exchanged using .docx template on shared secure repository. It often happens that some fields in these templates are not filled or that last version of certain risk document is unknown – in general, complex communication between ENTSO-E information security bodies and Parties is happening due to not existing communication platform. On the other hand, when templates are received, based on them ENTSO-E bodies have to make appropriate changes in the risk register which currently represent .xlsx table on shared secured location. Based on this explanation, it is clear that whole process could be jeopardised by unintentional mistakes and that there is no traceability of actions for many participants that are part of this process.

In order to reduce manual work and improve communication regarding OPDE risks, this UC is focused on developing specialised IT tool that could support and improve monitoring and communication during risk treatment process that is currently established on the ENTSO-E level. OPDE Risk Register will be based on the following functionalities:

- Enable entry form for risk submission and modification;
- Display all submitted risks and key information based on the "need to know" principle on centralised place;
- Enable fast, secure and simple communication between users on the specific risk;
- Log all changes of data in the system.

The tool will be hosted in SCC premises and each named user from different parties will have access to it. One Party could have several named users, depending on the number of people working on information security tasks. Each named user accesses OPDE Risk Register with individual credentials (user name and password). User from particular company has ability to submit, see and edit only risks related to its own Party. On the other hand, ENTSO-E information security bodies (that have responsibility to assess risk status and approve risk closure or acceptance) will have their own named users which could see and edit all submitted risks from all Parties. The tool will have risk entry form, as well as separate communication channel for each risk – there simple chat communication could be done between Party and ENTSO-E information security bodies.

D2.3 - Requirements and Detailed Architecture Design

All changes on the platform are recorded, and logs could be seen and downloaded only by hosting administrator on the request of ENTSO-E information security bodies.

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
OPDE Risk Register does not take into account potential changes of the given ENTSO-E business process which could happen in 2024 after enforcing document “OPDE Security Plan 2.0”.
ENTSO-E should support design phase of this tool in order to create the tool most adapted to this business process.
Prerequisites
All users will have to have enabled VPN connection to the SCC IT environment in order to access the tool.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
None.
Level of depth
Medium.
Prioritisation
4
Generic, regional, or national relation
Generic
Nature of the use case
Description of the business cases and general components of the system.
Further keywords for classification
Information security, ENTSO-E, OPDE, risk register

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
General approach for actor definition		An actor represents anything that interacts with or within the system. This can be a human, company, machine, or a computer program. Actors initiate activity with the system. An actor represents a role that a user plays; i.e., a user is someone playing a role while using the system. Each actor uses the system in different ways (otherwise they should be the same actor).	
Actor name	Actor type	Actor description	Further information specific to this use case
Party user	Regular user of the tool.	User coming from TSO or RCC side that provides risk information to the OPDE Risk Register, monitors risk treatment in its company and provide update of risk status in OPDE Risk Register.	User from specific TSO or RCC could submit new risk to the OPDE risk register, or make changes on the existing risk that was submitted by its company. Also, this user could communicate with ENTSO-E representatives in order to provide explanation for certain data related to certain risk (risk level, deadlines, mitigation strategies, ...).

D2.3 – Requirements and Detailed Architecture Design

ENTSO-E information security body user	Managerial user of the tool.	ENTSO-E information security body controls yearly audit process during which the level of implementation of “OPDE/ATOM Security Plan” controls for each Party is assessed. Also, this body continuously communicate with Parties in order to keep risk register update. Finally, this body approves which parties could access OPDE and which have restricted or no access based on the overall information security status.	User from ENTSO-E information security body could review risk information provided by all users of the tool. Also, this user could communicate with Party representatives in order to retrieve explanation for certain data related to certain risk (risk level, deadlines, mitigation strategies, ...). Finally, this user could request from hosting administrator to receive the list of logs.
Hosting administrator	Actor responsible to maintain the tool.	Company responsible to host the tool and to provide all designed functionalities to the users.	This actor has access to the back-end databases and scripts and front-end user interfaces and is the only entity that has insight in the system logs.
OPDE risk register	R ² D ² tool.	Specialised IT tool that could support and improve monitoring and communication during risk treatment process that is currently established on the ENTSO-E level.	This tool will be developed as described in this UC.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition
1	Risk submission	This scenario covers the process of risk submission by Parties	Party user	Detection of certain information security risk related with OPDE (usually after yearly report of the independent external auditor).	User accounts are created on OPDE Risk Register for all requested users. All information about risk is known.	All concerned users are informed about submission of new risk.
2	Risk review	This scenario covers the process of risk review by ENTSO-E information security bodies. Also, Parties can review risks that were submitted by their users.	ENTSO-E information security body user	ENTSO-E information security body users are informed about new submitted risk.	ENTSO-E information security bodies organised meeting to review new or newly updated risks.	ENTSO-E information security bodies made decision regarding the status of new or newly updated risks.
3	Chat communication	This scenario explains communication between representatives of Party and ENTSO-E information security bodies regarding issues on the specific risk	Party user and ENTSO-E information security body user	There is a need to provide comments on certain risk – detected issues with provided information, pass deadlines, ...	/	All concerned users are informed about new comment.
4	Risk modification	Following exchanged information in chat, Party can make requested changes – that is presented in this scenario.	Party user	There is a need to change risk information based on the requirements of ENTSO-E information security bodies.	/	All concerned users are informed about modification of risk.



D2.3 – Requirements and Detailed Architecture Design

5	Export data from the tool	Different export options are presented in this scenario.	Party user, ENTSO-E information security body user and Hosting administrator	There is a need to process data outside the tool in order to gather some new information or		
---	---------------------------	--	--	---	--	--

4.2 Steps – Scenarios

Scenario								
Scenario name:		Risk submission						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	Detection of certain information security risk related with OPDE (usually after yearly report of the independent external auditor	Logging on into the OPDE Risk Register	Party user is logging on into the OPDE Risk Register using credentials.	Logging on	Party user	OPDE Risk Register	1	C3P_039, C3P_043



D2.3 - Requirements and Detailed Architecture Design

2	Party user is logged on	Risk submitting	Party user fill all available fields and thus provides: general information about risk, risk description, risk classification for several criteria and risk mitigation strategy.	Data upload	Party user	OPDE Risk Register	2	C3P_040
3	Risk is submitted.	Risk notification	Party user can save entered data in the Risk Entry form keeping them available for her/him only. Only when "Submit risk" button is used the risk is submitted to the official database. In that moment notification is created in order to inform all concerned users about this change in the system. This notification is sent to all concerned users via e-mail server.	Generation of notification	OPDE Risk Register	E-mail server	3	C3P_042

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Risk review						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	ENTSO-E information security body users are informed about new submitted risk	Review of risk information by ENTSO-E information security body users	ENTSO-E information security body users receive notification via e-mail about submission of new risk. In OPDE Risk Register table these users can see key information for all submitted risks by all Party users. By using "More info" button for specific risk in this table, these users receive window showing all information about defined risk attributes. Detailed view can be obtained for all submitted risks in OPDE Risk Register.	Review and analysis of data	ENTSO-E information security body user	OPDE Risk Register	2	C3P_042, C3P_043, C3P_046, C3P_047



D2.3 - Requirements and Detailed Architecture Design

2	Review of risk information by ENTSO-E information security body users is completed	Review of risk information by concern Party users	All Party users that are coming from the same company receive notification via e-mail about submission of new risk related to their company. In OPDE Risk Register table these users can see key information for all submitted risks by Party users from their company only. By using "More info" button for specific risk in this table, these users receive window showing all information about defined risk attributes. Detailed view can be obtained only for submitted risks in OPDE Risk Register which are related with the Party user's company.	Review and analysis of data	Party user	OPDE Risk Register	2	C3P_042, C3P_043, C3P_046, C3P_047
---	--	---	---	-----------------------------	------------	--------------------	---	------------------------------------

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Chat communication						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	There is a need to provide comments on certain risk – detected issues with provided information, pass deadlines, ...	Feedback from ENTSO-E information security body	Following review of new submitted risk, ENTSO-E information security body user informs Party about some issues in the risk form, or confirms status of the risk.	Upload comments on specific risk	ENTSO-E information security body user	OPDE Risk Register	4	C3P_041, C3P_045
2	Feedback from ENTSO-E information security body is submitted.	Notification regarding submitted chat info	OPDE Risk Register creates notification after chat information on specific risk is saved in the system.	Generation of notification	OPDE Risk Register	E-mail server	3	C3P_042
3	Notification regarding submitted chat info is generated.	Feedback from Party	After receiving notification that ENTSO-E information security body user provided comment on specific risk, Party user analysis request and provide appropriate response.	Upload comments on specific risk	Party user	OPDE Risk Register	4	C3P_042, C3P_043, C3P_045



D2.3 - Requirements and Detailed Architecture Design

4	Feedback from Party is received	Finalisation of risk communication	Following several rounds of comments exchange between ENTSO-E information security body user and Party user, ENTSO-E information security body user confirms risk closure or acceptance, so chat communication could be finished.	Upload comments on specific risk	ENTSO-E information security body user	OPDE Risk Register	4	C3P_045
5	Risk communication is completed	Final notification	OPDE Risk Register creates notification after chat information on specific risk is saved in system.	Generation of notification	OPDE Risk Register	E-mail server	3	C3P_042

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Risk modification						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	There is a need to change risk information based on the requirements of ENTSO-E information security bodies.	Modification of risk information	Party user is requested to provide more information for certain risk attributes, e.g. better explanation of risk description, update of mitigation strategy, etc.	Modification of risk information	Party user	OPDE Risk Register	2	C3P_041, C3P_043, C3P_045
2	Risk is modified.	Notification regarding risk modification	In moment when Party user submit changes in the risk entry form, notification is created in order to inform all concerned users about this change in the system	Generation of notification	OPDE Risk Register	E-mail server	3	C3P_042
3	There is a need to accept/close the risk based on the approval of ENTSO-E information security bodies.	Modification of risk information	Party user is requested by to change the status of the risk, based on agreed decision.	Modification of risk information	Party user	OPDE Risk Register	2	C3P_045



D2.3 - Requirements and Detailed Architecture Design

4	Modification of risk information is completed	Notification regarding risk modification is generated.	In moment when Party user submit changes in the risk entry form, notification is created in order to inform all concerned users about this change in the system	Generation of notification	OPDE Risk Register	E-mail server	3	C3P_042
---	---	--	---	----------------------------	--------------------	---------------	---	---------

D2.3 - Requirements and Detailed Architecture Design

Scenario								
Scenario name:		Export data from the tool						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	There is a need to process data outside the tool in order to gather some new information.	Export of risk register list with full risk information	User can export all data related to the concerned risks in .csv file format. Party users can export data concerning risks correlated with their company only, while ENTSO-E information security body user can download all data concerning all submitted risks in OPDE Risk Register.	Data export	OPDE Risk Register	Party users or ENTSO-E information security body users	5	C3P_043, C3P_048
2	Log list is requested by ENTSO-E information security body user for forensics purposes	Export of log list data	Hosting administrator has possibility to see and export logs from the system.	Data export	OPDE Risk Register	Hosting admin	5	C3P_043, C3P_044, C3P_048

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Credentials	User name and password	
2	Risk information	Detailed information about risk according to ENTSO-E practise.	
3	Text notification	Short text message that informs users about some activities on the system – only non-confidential information is provided.	
4	Chat information	Rich text that describes some remarks/comments or response to it.	
5	Export file	Export file in .csv file format	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
ATOM	All TSO Network for non-real time Operational and Market related data is initial name for a dedicated communication network on which the OPDE is running for high security and service levels. Current name of this network is Physical Communication Network (PCN).
ENTSO-E	European Network of Transmission System Operators for Electricity represents 39 electricity transmission system operators (TSOs) from 35 countries across Europe, thus extending beyond EU borders. ENTSO-E was established and given legal mandates by the EU's Third Package for the Internal energy market in 2009, which aims at further liberalising the gas and electricity markets in the EU.

D2.3 – Requirements and Detailed Architecture Design

MVS	Minimum Viable Solution is short name for “Minimum Viable Solution Agreement for OPDE and ATOM” – agreement which has a scope to organise the collaboration between the TSOs, RCCs and Service Providers for the setting up, implementation and operation of the OPDE platform for the efficient storage, exchange and management of the data used for operational planning processes.
NDA	Non-Disclosure Agreement is legally enforceable contract that creates a confidential relationship between an entity who has sensitive information and an entity who will gain access to that information.
OPDE	Operational Planning Data Environment is a brand new, state of the art, ‘system of systems’ digital platform that connects the different TSOs to central elements and vice versa. It is designed on the basis of a layered architecture consistent with the SmartGrid Architecture Model. The OPDE is used for the secure and optimal exchange of operational planning data between TSOs and RCCs.
RCC	Regional Coordination Centre means regional coordination centre established pursuant to Article 35 of Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity. Regional coordination centres shall complement the role of transmission system operators by performing the tasks of regional relevance assigned to them.
SOGI	System Operation Guideline is the short name for Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation.
TSO	Transmission System Operator means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity (Directive(EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU)



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section

10.40 USE CASE 40 FORM

1. Description of the use case

1.1 Name of use case

Use case identification		
ID	Area/ Domain(s)/Zone(s)	Name of use case
40	Distribution and customer premise / from field to enterprise	IoT data security enforcement

1.2 Version management

Version management				
Version No.	Date	Name of author(s)	Changes	Approval status
0.1	21.12.2023	Mihkel	First draft	Needs further review and content from partners
0.2	23.01.2024	Lucas Pons (ETRA)	update	Approved

1.3 Scope and objectives of use case

Scope and objectives of use case	
Scope	Scope must cover the following topic: IoT devices management tool: IoT devices opt-in, Data push/pull services (standardized API) connected to datahubs/data sources. This UC focus on the IoT devices management activities and how they could benefit from the security enforcement paradigm and the set of tools proposed by R2D2.
Objective(s)	To enhance the tasks related to IoT management, namely: <ul style="list-style-type: none"> • IoT devices opt-in • Data push/pull • Data tampering detection and prevention from IoT platform
Related business case(s)	BC1, BC5

1.4 Narrative of use case

Narrative of use case
Short description
<p>This UC will concentrate on the analysis and enhancement of the tasks related to the IoT devices management, with the focus on the enforcement of the security without breaking the IoT paradigm.</p> <p>To test this UC part, a subsystem of the Greek pilot that use IoT technologies have been selected. This subsystem is composed by some Smart meters deployed across Xanthi and a control centre that receive its measurements. The data is exchanged in a IoT fashion, using MQTT protocol. These data include the real time electrical measurements and the hourly consumption profiles.</p> <p>The UC will change the processes related to the consumption profile data exchange using MQTT between the Smart meters and the IoT control centre. The idea will be to use a mechanism of tokenization of the data 'at the edge' (where it is read, before sending it), and use this token data to check the integrity at the control centre upon reception of data. Any data change or corruption happened during the transmission will result in the rejection of the data received.</p>
Complete description
<p>In last years, the usage of IoT devices in the energy sectors is increasing. These types of devices connect through specific IoT communication protocols and have some particularities on the way they are handled. This UC will concentrate on the analysis and enhancement of the tasks related to the IoT devices management, with the focus on the enforcement of the security without breaking the IoT paradigm.</p> <p>To test this UC part, a subsystem of the Greek pilot that use IoT technologies have been selected. This subsystem is composed by some Smart meters deployed across Xanthi and a control centre that receive its measurements. The data is exchanged in a IoT fashion, using MQTT protocol. These data include the real time electrical measurements and the hourly consumption profiles.</p> <p>Both the Smart meters and the control centre have been developed by ETRA and are operated by HEDNO. The control centre is deployed in the HEDNO infrastructure in Xanthi whilst part of the Smart meters are located in HEDNO infrastructures (EV charging points, HEDNO offices HVAC, etc.), and part are at the end user's homes.</p> <p>The UC will change the processes related to the consumption profile data exchange using MQTT between the Smart meters and the IoT control centre. This data exchange is particularly important and prone to data tampering, as this data is used for billing purposes. The idea will be to 'tokenize' the data to be sent 'at the edge' (where it is read, before sending it), and check its integrity at the control centre upon reception. Any data change or corruption happened during the transmission will result in the rejection of the data received.</p> <p>In order to do so, the tokenization tool component developed as part as the PRECOG set of tools will be used by the Smart meters and the control centre.</p>

1.5 Key performance indicators (KPI)

See Annex VI.

1.6 Use case conditions

Use case conditions
Assumptions
Smart meters are already deployed and connected to the IoT control system
IoT Control centre is deployed and periodically receives data from Smart meters
Prerequisites
Smart meter has internet access to blockchain remote infrastructure provided by GUARD.

1.7 Further information to the use case for classification/mapping

Classification information
Relation to other use cases
Level of depth
Prioritisation
3
Generic, regional, or national relation
National – to be examined only in the region of the pilot
Nature of the use case
Further keywords for classification
Data tokenization, data protection, Cyber-security enhancement

1.8 General remarks

General remarks

2. Diagrams of use case

SGAM use case diagrams are presented in Annex IV.

3. Technical details

3.1 Actors

Actors			
Grouping		Group description	
Based on Harmonised Electricity Market Role Model ver 2022		An actor represents a party that participates in a business transaction. Within a given business transaction an actor assumes a specific role or a set of roles. An actor is a composition of one or more roles and as such does not appear in the model.	
Actor name	Actor type	Actor description	Further information specific to this use case
Distribution System Operator (DSO) – HEDNO	System operator		
Meter	Physical device	A physical device containing one or more registers.	They will be Smart meters deployed to measure electrical consumption profiles

D2.3 - Requirements and Detailed Architecture Design

Grouping		Group description	
Software and hardware		Software and hardware used in the validation of network model integrity	
Actor name	Actor type	Actor description	Further information specific to this use case
Tokenization tool	Cybersecurity, data protection	Part of a PRECOG toolset, it is a cybersecurity tool that provides tokenization mechanisms for the data to protect its immutability. Provides verification mechanisms to verify data immutability and tokenization time of data.	Responsible for tokenizing the provided data, it returns a token for later immutability and time verification. Provides verification mechanisms for the tokenized data and associated token, verification returns verification results that are either OK or error. In case of errors a specific error code and message is returned.

3.2 References

References						
No.	References type	Reference	Status	Impact on use case	Originator / organisation	Link

4. Step by step analysis of use case

4.1 Overview of scenarios

Scenario conditions						
No.	Scenario name	Scenario descriptions	Primary actor	Triggering event	Pre-condition	Post-condition



D2.3 - Requirements and Detailed Architecture Design

1	Normal scenario	This scenario represents the behaviour of the system when data is exchanged with no problems between Smart meters and IoT control centre	Dso, Smart meters	Periodical	Smarty meters are deployed and have consumption profile data ready to transmit to the IoT platform for billing purposes	IoT platform receives data and is certain the data is accurate
2	Data tampering scenario	This scenario represents the behaviour of the system when data tampering is applied to the message send by the Smart meter	Dso, Smart meters	Periodical, data tampering detected	Smarty meters are deployed and have consumption profile data ready to transmit to the IoT platform for billing purposes.	IoT platform discards the fake data and Dso is warned appropriately



4.2 Steps – Scenarios

Scenario								
Scenario name:		Normal scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	periodical	Data gathering	Smart meter acquires consumption profile data from physical devices responsible of continuous power aggregation	Data gathering	Smart meter	Smart meter gateway application	Consumption profile measurements	
2	Consumption profile ready to send	Message generation	Smart meter gateway application	Message generation	Smart meter gateway application	Smart meter gateway application	Consumption profile message	
3	Message ready	Message signing	Gateway application sends message to KSI tool	Signing	Smart meter gateway application	KSI tool	Consumption profile message	
4	Message ready to sign	Signing	KSI tool request signing of data (involving blockchain)	Signing	KSI tool	Blockchain	Consumption profile message	
5	Message signed	Signing processing	Blockchain provides cryptographic proof	Signing	Blockchain	KSI tool	confirmation	
6	Message signed	Signing Response	KSI tool Provides information about the signature	Signing	KSI tool	Smart meter gateway application	Data signature	
7	Signature available	Message transmission	Smart meter gateway application transmits message and signature to IoT Control centre	Data transmission	Smart meter gateway application	IoT control centre	Consumption profile message + Data signature	

D2.3 - Requirements and Detailed Architecture Design

8	Message received	Message integrity checking	IoT control centre sends message to KSI tool	Signature checking	IoT control Centre	KSI tool (Control centre)	Consumption profile message + Data signature	
9	Integrity checking request	Integrity checking	KSI tool Assess the validity of the message signature using blockchain data	Signature checking	KSI tool	IoT control Centre	confirmation	
10	Confirmation available	data storage	Upon successful confirmation, the data is stored	Data storage	IoT control Centre	IoT control Centre (Database)	Consumption profile measurements	

Scenario								
Scenario name:		Data tampering scenario						
Step No.	Event	Name of process / activity	Description of process / activity	Service	Information Producer (actor)	Information receiver (actor)	Information exchanged (IDs)	Requirement, R-IDs
1	periodical	Data gathering	Smart meter acquires consumption profile data from physical devices responsible of continuous power aggregation	Data gathering	Smart meter	Smart meter gateway application	Consumption profile measurements	
2	Consumption profile ready to send	Message generation	Smart meter gateway application	Message generation	Smart meter gateway application	Smart meter gateway application	Consumption profile message	
3	Message ready	Message signing	Gateway application sends message to KSI tool	Signing	Smart meter gateway application	KSI tool	Consumption profile message	

D2.3 - Requirements and Detailed Architecture Design

4	Message ready to sign	Signing	KSI tool request signing of data (involving blockchain)	Signing	KSI tool	Blockchain	Consumption profile message	
5	Message signed	Signing processing	Blockchain provides cryptographic proof	Signing	Blockchain	KSI tool	confirmation	
6	Message signed	Signing Response	KSI tool Provides information about the signature	Signing	KSI tool	Smart meter gateway application	Data signature	
7	Signature available	Message transmission	Smart meter gateway application transmits message and signature to IoT Control centre	Data transmission	Smart meter gateway application	IoT control centre	Consumption profile message + Data signature	
8	Message received	Message integrity checking	IoT control centre sends message to KSI tool	Signature checking	IoT control Centre	KSI tool (Control centre)	Consumption profile message + Data signature	
9	Integrity checking request	Integrity checking	KSI tool Assess the validity of the message signature using blockchain data	Signature checking	KSI tool	IoT control Centre	confirmation	
10	Signature available	Integrity assessment and storage	IoT platform receives signature mismatching. Data is rejected and notification to EMMA GIMAN is sent	Incident notification	IoT control Centre	EMMA Giman	Incident details	

5. Information exchanged

Information exchanged			
Information exchanged, ID	Name of information	Description of information exchanged	Requirement, R-IDs
1	Consumption profile measurements	Raw consumption profile measurements: active and reactive energy consumed in kW/h	
2	Consumption profile message	Text message in JSON format comprising the Consumption profile measurements	
3	Signature data	Binary data that summarizes the data stored in the blockchain	

6. Requirements (optional)

This form can only contain requirement IDs – for more information see Annex III.

7. Common terms and definitions

Common terms and definitions	
Term	Definition
KSI Blockchain	<p>KSI is a blockchain technology designed in Estonia and used globally to ensure networks, systems, and data are free of compromise, all while retaining 100% data privacy.</p> <p>A blockchain is a distributed public ledger – a database with a set of pre-defined rules for how the ledger is appended by the distributed consensus of the participants in the system. Due to its widely witnessed property, blockchain technology makes it also impossible to change the data already on the blockchain.</p> <p>With KSI Blockchain deployed in Estonian government networks, history cannot be rewritten by anybody and the authenticity of the electronic data can be mathematically proven. It means that nobody – neither hackers, nor system administrators, nor even the government itself – can manipulate the data and get away with it.</p>



8. Custom information (optional)

Custom information (optional)		
Key	Value	Refers to section



11. ANNEX II: USE CASE REVISION FORM

1. Use case additional information (to be filled out by Author)

Use case author:

Other involved partners:

1. Tick the related R²D² task(s):

3CPO

<input type="checkbox"/>	Task 3.1 Security assessment through advanced IT technologies
<input type="checkbox"/>	Task 3.2 Dynamic Cyber-Risk Status Evaluation
<input type="checkbox"/>	Task 3.3 Spatial and Temporal Modelling and Quantification of Cascading Physical Events
<input type="checkbox"/>	Task 3.4 Resilience-driven investment and operational planning to mitigate or prevent cascading effects
<input type="checkbox"/>	Task 3.5 Operation and Planning of Advanced Multi-Energy Microgrids for Enhancement of Resilience

IRIS

<input type="checkbox"/>	T4.1 Optimal resources coordination management for TSOs and DSOs during crisis
<input type="checkbox"/>	T4.2 Emergency and restoration
<input type="checkbox"/>	T4.3 Multi-energy TSO-DSO planning coordination

PRECOG

<input type="checkbox"/>	T5.1 Identification and authentication of energy IoT and edge devices
<input type="checkbox"/>	T5.2 Energy tokens and trading certificates security
<input type="checkbox"/>	T5.3 Cybersecurity Events Management tools
<input type="checkbox"/>	T5.4 Deep learning data analytics for security
<input type="checkbox"/>	T5.5 Device origin and supply chain

EMMA

<input type="checkbox"/>	T6.1 – Equipment inspection through autonomous images acquisition
<input type="checkbox"/>	T6.2 – Optimal Asset management
<input type="checkbox"/>	T6.3 – Resource management in case of critical events
<input type="checkbox"/>	T6.4 - Maintenance coordination and planning

If you have selected more than one task, what is the primary task of your use case? _____



D2.3 - Requirements and Detailed Architecture Design

2. Tick the related R²D² scenario(s):

<input type="checkbox"/>	System Operator Scenario
<input type="checkbox"/>	Distributed Energy Resources Scenario

3. Tick the selected pilot site(s) for demonstration:

<input type="checkbox"/>	Greece
<input type="checkbox"/>	Serbia
<input type="checkbox"/>	Slovenia
<input type="checkbox"/>	Spain

4. Please answer the questions:

Question: How innovative is the use case and what is innovation?
Answer:

Question: If the use case is not innovative, why is it necessary?
Answer:

Question: How and why the use case is important?
Answer:

Question: Does the use case align with the project environment (business scenarios, objectives and products)?
Answer:

Question: Is the use case in line with relevant EU regulation (market principles, cyber security...)?
Answer:

Question: Is this already done at ENTSO-E level or some region? If it is already done, why the use case is needed?
Answer:

Question: What KPIs might be assigned to the use case? Please suggest KPI name, KPI description and reference to use case objectives.
Answer:

Question: What does it take for a use case to be scalable / replicable?
Answer:

Question: How do you plan to demonstrate the use case?
Answer:



D2.3 - Requirements and Detailed Architecture Design

Question: Does the R²D² consortium have sufficient resources to implement and demonstrate the use case (man power, time, knowledge, available pilot site, needed equipment...)? Please explain the role of each partner involved in developing and demonstrating the use case.

Answer:

2. Use case revision (to be filled out by Auditor)

Please answer the questions and provide requested explanations:

Question: Do you think the use case definition is done correctly (refers to use case definition form)?

Answer: Yes/Mostly Yes/ Mostly No/No

Please provide explanation:

Question: Do you think the additional information about use case (refers to section 1 of this form) is plausible?

Answer: Yes/Mostly Yes/ Mostly No/No

If not, please provide explanation:

Question: Do you think the use case should be carried out as part of the R²D² project?

Answer: Yes/No

If no, please provide explanation:

Question: Do you have any recommendations to improve use case definition?

Answer: Yes/No

If yes, please provide recommendations:

12. ANNEX III: FULL INFORMATION REQUIREMENTS TABLE

req ID	Description	Clasification	Type	Rationale	Acceptance criteria	Priority	Comments
C3P_001	Data of historical experiences with extreme weather.	C3PO	Functional and data requirements	Need such data to better characterize the event simulation and the asset behaviour.	Database of relevant event and network performance data	5	Ideally this will include the following: - Event simulation: trajectory, intensity and duration of event - Network asset performance: failure probability of assets and restoration times
C3P_002	Switches available in the feeders must be controllable	C3PO	Operational requirements	This is required for network reconfiguration algorithms	Availability or remotely control switches in pilot lines	5	
C3P_003	The topology of the grid at pilot sites must be known in advance	C3PO	Operational requirements	Several functionalities of the C3PO tool rely on the topology of the grid	Topology description in a standard format exists for the pilot sites.	5	
C3P_004	Pilot sites must identify critical nodes of the grid	C3PO	Operational	Critical nodes of the grid are the ones whose		4	



D2.3 - Requirements and Detailed Architecture Design

			requirements	security must be preserved the most.			
C3P_005	EMMA ETER component shall be able to import historical supply point information read from Smart meters	C3PO	The scope of the product	to be able to analyse end users behaviour		4	Data will be accessed by means of CSV files provided by the DSO
C3P_006	C3PO must have access to weather forecast of the pilot site locations	C3PO	Functional and data requirements	C3PO physical resilience-related tools need such data to assess the impact of extreme weather events on power system	Weather forecast (ambient temperature, wind speed and direction, solar radiation) in hourly basis in json format	5	The components (in C3PO platform premises) which will receive this info are T3.3 and use case 44. These components will assess the impact of extreme weather events on power systems.
C3P_007	The topologies of pilot site networks must be well known and modelled	C3PO	Functional and data requirements	C3PO toolkits need network data for the assessment of HILF events spatiotemporal impact and for providing resilience-oriented optimal operational measures	Topology model in json format	5	
C3P_008	In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the dispatchable DGs, RES and ESS units	C3PO	The scope of the work	These units are crucial for strategies related to the resilience enhancement of the grid		5	



D2.3 - Requirements and Detailed Architecture Design

C3P_09	The location and technical characteristics of DERs must be known	C3PO	Operational requirements	DERs characteristics (min/max capacity, etc.) must be known for providing resilience-oriented optimal operational strategies	DERs technical characteristics in a standard format (e.g., json)	5	
C3P_010	The characteristics of distribution lines must be known	C3PO	Operational requirements	The characteristics of distribution lines must be known for the scope of use case 44	The characteristics of distribution lines (capacity, length, diameter) in a standard format (e.g., json)	4	
C3P_011	Protection Settings for customising cascading simulators (T3.3)	C3PO	Functional and data requirements	This data is needed for developing the cascading simulators in a way that accurately represent the system operation and cascading propagation.	Real protection settings of demo sites	4	Protection can include overload protection, over- and under-frequency load shedding, etc. - in general, the protection in place at the demo sites.
C3P_012	The C3PO investment planning tool (T3.4) will require the investment costs of different infrastructure solutions, such as undergrounding lines and flood protection.	C3PO	Functional and data requirements	Need such data to develop realistic investment portfolios that reflect real investment options at the demo sites.	Database of historical, current and future cost projections of different infrastructure solutions.	4	If this data is not known or depends on case-by-case, cost estimates will be useful to better tailor the proposed investment portfolios.
C3P_013	The C3PO tool to be developed in T3.4 requires the portfolio of operational flexibility options	C3PO	Functional and data requirements	These operational flexibility options will be required to be compared with infrastructure solutions in order to develop optimal investment portfolios.	List and details of operational flexibility solutions at demo sites.	4	Examples can include battery storage systems, demand side management, existing microgrids, etc.



D2.3 - Requirements and Detailed Architecture Design

	available at the demo sites.						
C3P_014	Historical performance indicators of the system under extreme events	C3PO	Performance requirements	These performance indicators are necessary in order to try and benchmark the reliability and resilience performance of the demo sites against the extreme events to be modelled and quantified.	Historical performance indicators, and details of the extreme events the system was exposed at.	4	Such performance indicators will first help define and benchmark the indicators to be used in the studies (T3.3) and then develop the investment portfolios to optimize these indicators.
C3P_015	C3PO Static Risk Assessment Tool should perform a comprehensive cyber security risk assessment of the EPES environment, considering cyber threats, vulnerabilities and attack scenarios.	C3PO	The scope of the product			5	
C3P_016	C3PO Static Risk Assessment Tool should allow users (DSO/TSO operators) to define existing assets, assets criticality, and security controls to create an accurate representation of the system's security posture.	C3PO	Functional and data requirements			5	



D2.3 - Requirements and Detailed Architecture Design

C3P_017	C3PO Static Risk Assessment Tool should assess risk considering: asset criticality, threats likelihood and identified vulnerabilities criticality.	C3PO	Functional and data requirements			5	
C3P_018	C3PO Static Risk Assessment Tool should provide guidance and recommendations (including countermeasures) for mitigating identified risks and vulnerabilities.	C3PO	Functional and data requirements			5	
C3P_019	C3PO Static Risk Assessment Tool should provide access control to ensure that only authorized users have access to the system.	C3PO	Usability and humanity requirements			3	
C3P_020	C3PO Static Risk Assessment Tool should be accessible through standard web browsers and compatible with different devices, such	C3PO	Usability and humanity requirements			3	



D2.3 - Requirements and Detailed Architecture Design

	as desktops, tablets, and smartphones.						
C3P_021	C3PO Dynamic CyberRisk Evaluation tool shall evaluate dynamically the EPES' Cyber-Risk Status considering assets' criticality, identified existing and emerging cyber threats as well as existing technical vulnerabilities.	C3PO	The scope of the product			5	
C3P_022	C3PO Dynamic CyberRisk Evaluation tool should consume threat related information and technical vulnerabilities from the Cyber Threat Intelligence tool.	C3PO	Functional and data requirements			4	
C3P_023	C3PO Dynamic CyberRisk Evaluation tool should consider DSO/TSO's assets' criticality, controls and their topology to assess risk values.	C3PO	Functional and data requirements			5	
C3P_024	C3PO Dynamic CyberRisk Evaluation tool should provide	C3PO	Usability and humanity			3	



D2.3 - Requirements and Detailed Architecture Design

	near real-time alerts / notifications to experts when new technical vulnerabilities are identified, allowing for timely response and mitigation.		requirements				
C3P_025	C3PO Dynamic CyberRisk Evaluation tool should evaluate risks utilizing T5.4 Deep Learning Data Analytics Module.	C3PO	Functional and data requirements			5	
C3P_026	Access to Dynamic CyberRisk Evaluation tool will be authenticated and web-based	C3PO	Usability and humanity requirements			4	
C3P_027	The Cyber Threat Intelligence Tool should collect cyber threat information from external sources to share with R2D2 components.	C3PO	Functional and data requirements			5	
C3P_028	The Cyber Threat Intelligence Tool should disseminate sanitized indicators of compromise identified by R2D2 components, to the CTI community.	C3PO	Functional and data requirements			3	



D2.3 - Requirements and Detailed Architecture Design

C3P_029	The Cyber Threat Intelligence Tool should enforce a sharing policy abiding to the DSO/TSO's information classification policies.	C3PO	Security requirements			3	Will disseminate sanitized indicators of compromise identified by R2D2
C3P_030	The Cyber Threat Intelligence Tool should support widely accepted formats of cyber threat information sharing.	C3PO	Operational requirements			5	
C3P_031	The Cyber Threat Intelligence Tool should be able to generate alerts and notifications based on predefined rules.	C3PO	Functional and data requirements			3	
C3P_032	Access to Cyber Threat Intelligence Tool will be authenticated and web-based.	C3PO	Usability and humanity requirements			4	
C3P_033	SCADA S, V, I measurements availability over the main feeders of pilot MV lines	C3PO	Functional and data requirements	Those data needed for power flow calculations in C3PO T3.3 cascading simulators		5	In case of an extreme weather event, the cascading simulators may need S, V, I data for the main buses of MV feeders to calculate power flows



D2.3 - Requirements and Detailed Architecture Design

C3P_034	Metering equipment up-running, available data via DLMS/COSEM protocol	C3PO	Functional and data requirements	Those data may be needed for power flow calculations in C3PO T3.3 cascading simulators		5	Data from AMI / consumption may be necessary for power flow calculations in the cascading simulators
C3P_035	Output of T3.4 Operational planning module is sent to DSO via MQTT protocol	C3PO	Functional and data requirements	Output of T3.4 tool, related to the optimal mitigation plan, must be forwarded to the DSO in MQTT protocol by the C3PO tool		4	For the GR pilot, MQTT protocol is the most preferable and supported by HEDNO
C3P_036	The characteristics of mobile sources must be well known and modelled	C3PO	Operational requirements			5	
C3P_037	The outage scenarios of power lines and electrical components must be well observed	C3PO	Functional and data requirements			5	
C3P_038	The characteristics of critical/non-critical loads must be known	C3PO	Functional and data requirements			4	
C3P_039	OPDE RR – User management - Log in using user name and password, including possibility to create user groups.	C3PO	Functional and data requirements	In order to apply access restriction.	Log in screen is available and different user groups have different access capabilities.	5	



D2.3 – Requirements and Detailed Architecture Design

C3P_040	OPDE RR – Risk entry form aligned with ENTSO-E practise.	C3PO	Functional and data requirements	In order to input/edit data in tool and to developed a tool useful for ENTSO-E business process.	All fields from ENTSO-E risk form template are available in the tool and after submitting the risk, all information is stored in tool database.	5	
C3P_041	OPDE RR – Dashboard for displaying statistical risk information using bar charts and pie charts.	C3PO	Functional and data requirements	In order to see certain trends in risk delivery, risk closure, risk type, etc. per Party or in general.	Several graphs are available on home page.	3	
C3P_042	OPDE RR – E-mail notification after saving information in tool.	C3PO	Functional and data requirements	In order to inform person that there is some change on the platform, since is not monitored continuously.	After saving certain information in the tool e-mail is received on the e-mail addresses of dedicated users.	2	
C3P_043	OPDE RR – Restriction of data access/modification based on the “need to know” principle.	C3PO	Functional and data requirements	Information security requirement.	Different users can see/modify different risk information and communication channels based on predefined principles.	5	
C3P_044	OPDE RR – Log list that displays all changes of data in the tool.	C3PO	Functional and data requirements	Increase traceability of data changes and provide forensics in case of dispute.	After making changes on risk entry form, log list is updated with new entry	4	



D2.3 - Requirements and Detailed Architecture Design

					explaining who, when and what changed.		
C3P_045	OPDE RR – Communication channel between appointed users for each risk separately.	C3PO	Functional and data requirements	In order to avoid confidential discussions via e-mails.	Chat between different users is performed.	5	
C3P_046	OPDE RR – Simplified view of all submitted risks in tabular form.	C3PO	Functional and data requirements	In order to have better overview on all risks and their key attributes.	List of all risks and they key attributes is available – different users see different lists according their access rights.	4	
C3P_047	OPDE RR – Detailed view of each submitted risk separately.	C3PO	Functional and data requirements	In order to see all risk information.	By selecting one risk from simplified table of risks, user can see all information for that particulars risk.	4	
C3P_048	OPDE RR – Export of risk data in .csv file format	C3PO	Functional and data requirements	In order to provide processing of collected data in other tools.	After exporting risk data, .csv file is generated with all expected information.	3	
EMM_002	Maintenance UAV shall flight in manual or autonomous	EMMA	The scope of the product	The UAV could be used in automatic or manual way	UAV flying mode can be changed	3	



D2.3 - Requirements and Detailed Architecture Design

EMM_003	the recorded flight path of the AUV shall be presented over a map	EMM A	Usability and humanity requirements			2	
EMM_004	EMMA GUI shall feature a credential validation screen allowing openid	EMM A	Security requirements		The login - password form is presented before accessing the GUI	5	
EMM_005	To have access to a historical dataset of substations measurements (mainly P,Q,V,I)	EMM A	Functional and data requirements	Train AI algorithms	Being able to read the dataset with the software	5	
EMM_006	To receive Real-Time measurements (or simulated Real-Time data) from substations (mainly P,Q,V,I)	EMM A	Functional and data requirements	To test EMMA models	Being able to read the measurements with the software	5	
EMM_007	if abnormal high temperatures are captured by UV camera pointing to a transformer an alarm shall be sent in MQTT protocol	EMM A	The scope of the work	Heating should be a triggering for maintenance actions	Images containing temperature problems raise an alarm	5	
EMM_008	To acquire images	EMM A	Functional and data requirements	To perform images recognition techniques (to train risk assessment and predictive maintenance models).	To store the images in the internal database	5	



D2.3 - Requirements and Detailed Architecture Design

EMM_009	(OPC tool) Collection of outage plans from stakeholders (TSOs, RCCs, PES users)	EMM A	Functional and data requirements		Data available in database	5	
EMM_010	EMMA ARGOS component must feature a web application for upload images and videos	EMM A	The scope of the work			5	
EMM_011	EMMA ARGOS component shall trigger the image processing task upon reception of new data	EMM A	The scope of the work			4	
EMM_012	EMMA ARGOS image processing component shall trigger events and sent to EMMA component when the images analysed contain problems according to the ML models	EMM A	The scope of the work			5	
EMM_013	EMMA shall receive periodically a selected set of SCADA signals for grid assets and substations	EMM A	Functional and data requirements			5	
EMM_014	EMMA ARGOS component shall identify when new	EMM A	The scope of			4	



D2.3 - Requirements and Detailed Architecture Design

	images or videos have been uploaded and then trigger the image processing process		the product				
EMM_015	EMMA shall feature a web interface to present the maintenance results and KPIS	EMM A	The scope of the work			3	
EMM_016	EMMA signals processing component shall trigger events and store relevant data when the analysis of the signals indicates about problems according to the ML models	EMM A	The scope of the product			5	
EMM_017	EMMA signal processing component ML models must support identifying active and future problems in the substation assets	EMM A	The scope of the product			5	
EMM_018	EMMA ARGOS image processing component ML models must support identifying active and future problems in the	EMM A	The scope of the product			5	



D2.3 - Requirements and Detailed Architecture Design

	substation assets and overhead lines						
EMM_019	EMMA component shall generate a ranked list of interventions prioritized according to its criticality	EMM A	The scope of the product			5	
EMM_020	EMMA GIMAN component shall schedule the workforce duties according to the information received from EMMA	EMM A	Functional and data requirements			4	
EMM_021	EMMA GIMAN component shall generate workforce activities routing to carry out the duties in the most optimal way	EMM A	The scope of the product			4	
EMM_022	Pilot site must deploy metering devices.	EMM A	Operational requirements	Metering devices are required for monitoring purposes. UC26 MV/LV physical substation security relies on metering equipment installation.	Data from the desired points is available.	5	
EMM_023	Pilot sites must identify critical nodes of the grid	EMM A	Operational requirements	EMMA workforce allocation tool must know the critical nodes of the grid, which are the ones whose security must be preserved the most		5	



D2.3 - Requirements and Detailed Architecture Design

EMM_024	Grid operator must configure in EMMA GIMAN the details of personnel involved in incident management.	EMM A	Operational requirements	To be able to assign mitigation tasks to force workers, EMMA GIMAN needs to know the information about the details of personnel, including skills related to grid events solving.		5	
EMM_025	Maintenance UAV could be controlled in remote	EMM A	Legal requirements			5	
EMM_026	EMMA ARGOS ML models should identify problems linked to the presence of forest near the overhead lines according to the images	EMM A	The scope of the product	To identify forest on the images and trigger alarms	images with such problems are tagged and alarms are triggered	4	
EMM_027	EMMA ARGOS ML models should identify physical (structural or mechanical) problems on tower/poles, conductors and insulators based on the images	EMM A	The scope of the product	To identify physical problems and trigger alarms	alarms are triggered	4	
EMM_028	EMMA ARGOS ML models should identify electrical problems on the conductors and insulators based on the images	EMM A	The scope of the product	To identify electrical problems in	images with such problems are tagged and alarms are triggered	4	



D2.3 - Requirements and Detailed Architecture Design

EMM_029	EMMA DYML component shall import data from DGA analysis	EMM A	The scope of the product	To be able to process data from Gas chromatography transformer oil analyser		5	
EMM_030	EMMA DYML component shall support OPC-UA protocol to gather SCADA measurements	EMM A	The scope of the product	To be able to receive SCADA measurements		4	
EMM_031	EMMA ETER shall be able to import grid topology in CIM format	EMM A	The scope of the product			2	
EMM_032	EMMA ETER component shall import historical substation feeder data	EMM A	The scope of the product	To be able to analyse the consumption of the whole feeder		2	
EMM_033	EMMA ETER component shall be able to identify abnormal or suspicious behaviours of supply points based on data	EMM A	The scope of the product			4	
EMM_034	EMMA GIMAN component should feature a web GUI	EMM A	Usability and humanity requirements			3	
EMM_035	EMMA ETER component should feature a web GUI	EMM A	Usability and humanity			4	



D2.3 - Requirements and Detailed Architecture Design

			requirements				
EMM_036	EMMA must contain a communication platform to provide the following services: 1) All participants can upload and download files 2) files are kept for a certain period of time 3) A conference call can be started	EMMA	Functional and data requirements	This communication platform is required for instance for the exchange of files related to the distribution of costs of corrective actions between the TSOs and RCCs involved	All required functionalities are provided	5	
EMM_037	EMMA shall contain a tool to calculate the cost sharing related to remedial actions with cross-border impact between the TSOs involved	EMMA	Functional and data requirements	EMMA must contain cost sharing tool to provide the following: - Can download RA cost files and PTDF matrices from the EMMA communication platform - The operator can set cost sharing rules between the involved TSOs - Calculation of cost sharing between	All required functionalities are provided	5	
EMM_038	EMMA product must contain outage planning optimization tool (EMMA OP)	EMMA	Functional and data requirements	EMMA product will improve the maintenance coordination and planning through outage planning optimization	All required functionalities are provided	5	EMMA OP tool must be capable to: 1) import outage periods proposals of network elements 2) import grid models for the relevant planning period 3) optimize outage periods of network elements. This requirement correlates



D2.3 - Requirements and Detailed Architecture Design

							with task 6.4 (Maintenance coordination and planning)
EMM_ 039	EMMA product must contain an application to transfer topology file	EMM A	Function al and data requirem ents	EMMA product should improve maintenance coordination and planning by automatization of topology file creation after outage planning process is finished	All required functionalities are provided	5	EMMA TTA must be designed to: 1) Import detailed data for planned switching on network elements (off/on), description of switching state change 2) Import default topology file (no planned outages included) 3) Include planned switching in the topology file 4) Export topology file 5) Create reports for selected dates on all network elements which topology status differs from the default topology file
EMM_ 040	EMMA product must contain dedicated script created in DigSILENT environment (DigSILENT Programming Language) to perform calculations related to transient stability.	EMM A	Function al and data requirem ents	EMMA TSC Script shall be used to calculate critical fault clearing time i.e. to check transient stability of the synchronous generators	All required functionalities are provided	5	EMMA TSC Script must be designed to: 1) enable operator to set script options 2) Calculate maximum periods during which the transient stability of the synchronous generation operation after a fault is preserved (rotor angle



D2.3 - Requirements and Detailed Architecture Design

							stability) 3) Export results in txt file
EMM_041	EMMA product must contain application to perform calculations related to power quality	EMMA	Functional and data requirements	EMMA should provide a tool to calculate and monitor power quality parameters in connection points to the grid, such as flickers, higher harmonics and asymmetries) in compliance simulation and real-time compliance monitoring	All required functionalities are provided	5	EMMA PQEL application must be designed to: 1) Import file representing selected grid model 2) Import file with emission levels (of flickers, higher harmonics and asymmetries) measurements 3) Import file with calculated emission levels 4) Calculate emission levels for the selected node 5) Compare measured and calculated emission levels 6) Calculate grid equivalent parameters (such as R/X, Z _d , Z _i , Z _o , Sk''...) for the selected node 7) Create and export file with calculation results
EMM_042	EMMA product must contain an application to transfer Dynamic Line Rating limits into IGMs and SCADA/EMS system	EMMA	Functional and data requirements	In order to use additional transmission capacity it is needed to transfer Dynamic Line Rating limits from DLR server into IGMs and SCADA/EMS system	All required functionalities are provided	5	EMMA DLR Application must be designed to: 1) Read selected analogue values (DLR sensors values) from SCADA 2) Write selected analogue values into SCADA limits 3) Read limit values from CSV file 4) Write values of



D2.3 - Requirements and Detailed Architecture Design

							the forecast current limits to .EQ file 5) Write values form CSV file to SCADA limits
EMM_043	test	EMM A	Performance requirements	this is a test		0	
EMM_044	Surveillance equipment installed in HV/MV substation must provide 24h live streaming image to EMMA ARGOS	EMM A	Functional and data requirements	Image must be constantly available in ETRA EMMA ARGOS module, in order for the tool to perform image analysis		5	Surveillance equipment procured, must support image live streaming, so that the image can be forwarded to EMMA ARGOS
EMM_045	EMMA PQEL script should be created within the PowerFactory DIgSILENT programming environment in the appropriate programming language.	EMM A	Functional and data requirements	This requirement is needed for UC15 Automation of calculation of emission levels of electricity quality parameters	All required functionalities are provided	5	
EMM_046	After running the EMMA PQEL script, a dialog box opens in which the operator selects which scenario will be executed.	EMM A	Functional and data requirements	This requirement is needed for UC15 Automation of calculation of emission levels of electricity quality parameters	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

EMM_047	The EMMA PQEL operator must have capability to make changes to the planned levels for the Compliance simulation scenario and the Equivalent grid parameters calculation scenario.	EMM A	Functional and data requirements	This requirement is needed for UC15 Automation of calculation of emission levels of electricity quality parameters	All required functionalities are provided	5	
EMM_048	In the case of the Compliance simulation scenario, the EMMA PQEL operator can: 1) Define a path to the simulation network model; 2) Mark the nodes for which emission values are calculated; 3) Define the path to the folder where the output file is saved.	EMM A	Functional and data requirements	This requirement is needed for UC15 Automation of calculation of emission levels of electricity quality parameters	All required functionalities are provided	5	
EMM_049	For the Compliance monitoring scenario, the EMMA PQEL operator can: 1) Define the path to the file with emission limits & measured data 2) Mark the nodes for which the comparison is made 3) Define the	EMM A	Functional and data requirements	This requirement is needed for UC15 Automation of calculation of emission levels of electricity quality parameters	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	path to the folder where the output file is stored.						
EMM_050	For the Equivalent grid parameters calculation scenario, the EMMA PQEL operator can: 1) Define the path to the simulation grid model; 2) Mark the nodes for which parameters are calculated; 3) Define the path to the folder where the output file is stored.	EMM A	Functional and data requirements	This requirement is needed for UC15 Automation of calculation of emission levels of electricity quality parameters	All required functionalities are provided	5	
EMM_051	After defining the input parameters through .SetSelect objects within DigSILENT framework, the EMMA PQEL script needs to perform in Compliance simulation scenario operations provided in the requirements comments section.	EMM A	Functional and data requirements	This requirement is needed for UC15 Automation of calculation of emission levels of electricity quality parameters	All required functionalities are provided	5	a. Load the input data - the simulation model of the grid and the labels of the nodes for which the calculation are made; b. Runs the power flow calculation; c. Runs the harmonic power flow calculation, if the power flow calculation has converged; d. Creates an output file containing the following data: i. The title that refers to the performed



D2.3 - Requirements and Detailed Architecture Design

							calculation of emission values; ii. The label of the node for which the calculation was performed; iii. The estimators of the emission value; iv. Information on whether the calculated emission value is within the permitted limits.
--	--	--	--	--	--	--	---



D2.3 - Requirements and Detailed Architecture Design

EMM_052	After defining the input parameters through .SetSelect objects within DIgSILENT framework, the EMMA PQEL script needs to perform in Compliance monitoring scenario the operations provided in the requirement comments section.	EMM A	Functional and data requirements	This requirement is needed for UC15 Automation of calculation of emission levels of electricity quality parameters	All required functionalities are provided	5	<ol style="list-style-type: none">1. Using the previously entered (defined) parameter values as well as the associated set (.SetSelect object), the script should do the following:<ol style="list-style-type: none">a. Loads input data - a file with emission limits and measured data for selected nodes;b. For selected nodes compares emission limits with measured data;c. Creates an output file containing the following data for scenario 2:<ol style="list-style-type: none">i. The title that refers to the performed calculation of emission values;ii. The label of the node for which the calculation was performed;iii. The estimators of the emission value;iv. Information on whether the calculated emission value is within the permitted limits.
---------	---	-------	----------------------------------	--	---	---	---



D2.3 - Requirements and Detailed Architecture Design

EMM_053	After defining the input parameters through .SetSelect objects in the DlgSILENT framework, the EMMA PQEL script in the Equivalent grid parameters calculation scenario executes the operation given in the requirement comments section.	EMM A	Functional and data requirements	This requirement is needed for UC15 Automation of calculation of emission levels of electricity quality parameters	All required functionalities are provided	5	a. Loads the input data - the simulation model of the grid and the labels of the nodes for which the calculation are made; b. Runs the power flow calculation; c. Runs the harmonic power flow calculation, if the power flow calculation has converged; d. Creates an output file containing the following data: - Title related to the performed parameter calculation; - The label of the node for which the calculation was performed; - Calculated parameters.
EMM_054	The EMMA TSC script needs to be created within the PowerFactory DlgSILENT programming environment.	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	
EMM_055	Upon entering the EMMA TSC script, a menu opens so that the operator can run a	EMM A	Functional and data	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	calculation related to a fault which is: 1) switched off by a circuit-breaker 2) of transient type.		requirements				
EMM_056	The EMMA TSC script should have a configurable set of input data (parameters) with the default values provided in the requirement comments section	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	a. Simulation start time (typically: $t_{start} = -0,1s$ – absolute time) b. Total simulation time (typically: $t_{sim} = 2s$ – simulation duration) c. Minimum fault clearing time (typically: $t_{min} = 0,05s$ – minimum time duration of a fault) d. Maximum fault clearing time (typically: $t_{max} = 1s$ – maximum time duration of a fault) e. Accuracy time – „time error“ of a fault clearing time (typically $t_{step} = 0.01s$). This defines a „critical clearing time“ result accuracy.
EMM_057	Before opening the EMMA TSC script, the operator must have the ability to: 1) create a "set" of type .SetSelect object 2) fill the set with elements	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	3) assign the set to the script.						
EMM_058	The EMMA TSC script allows the operator to define initial conditions in the network.	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	
EMM_059	The EMMA TSC script allows the operator to select synchronous machines to be observed in the calculations by creating an "OutOfStep" set of variables (the value of the variable must be selected for each generator).	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	
EMM_060	When starting a new calculation, the EMMA TSC script a) clears the output window of previous results b) reset the previously calculated critical fault time values for all network nodes	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	
EMM_061	The EMMA TSC script calculates the critical fault time for each of the buses from the defined set.	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

EMM_062	The EMMA TSC script internally stores the result of the calculation to one of the variables belonging to the bus structure.	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	
EMM_063	The EMMA TSC script displays calculation results in the output window and stores the calculation results inside the "dpl1" buses variable (pTerm:dpl1).	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	
EMM_064	The EMMA TSC script automatically or manually after completion of the calculation creates an output file with the results in ".txt" format and stores the file in the predefined folder.	EMM A	Functional and data requirements	This requirement is needed for UC14 Automation of transient stability calculations	All required functionalities are provided	5	
EMM_065	EMMA DLR Application must be capable to read analogue values and quality flags of DLR limits and quality of DLR system calculation from SCADA/EMS.	EMM A	Functional and data requirements	This requirement is needed for UC31 DLR integration with IGMs and SCADA/EMS	All required functionalities are provided	5	
EMM_066	EMMA DLR Application must be capable to read real-time and forecasted limits and	EMM A	Functional and data	This requirement is needed for UC31 DLR integration with IGMs and SCADA/EMS	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	quality of DLR system calculation from CSV file.		requirements				
EMM_067	EMMA DLR Application must be capable to write values into SCADA limits for each line with DLR sensor.	EMMA	Functional and data requirements	This requirement is needed for UC31 DLR integration with IGMs and SCADA/EMS	All required functionalities are provided	5	
EMM_068	EMMA DLR Application must be capable to write forecasted limits into OPL file.	EMMA	Functional and data requirements	This requirement is needed for UC31 DLR integration with IGMs and SCADA/EMS	All required functionalities are provided	5	
EMM_069	EMMA TTA shall read an input file containing network element type, network element designation, period, time and type of switching (off/on), description of switching state change	EMMA	Functional and data requirements	This requirement is needed for UC17 Outage coordination and automated creation of topology files for Individual Grid Models	All required functionalities are provided	5	
EMM_070	EMMA TTA shall update the default topology file for the selected date/hour according to the approved planned outages.	EMMA	Functional and data requirements	This requirement is needed for UC17 Outage coordination and automated creation of topology files for Individual Grid Models	All required functionalities are provided	5	Examples: 1) If a line is to be disconnected, this line is disconnected at both ends in the grid model 2) If a transformer is to be disconnected, this transformer is disconnected at both ends in the grid model 3) if a line bay is to be



D2.3 - Requirements and Detailed Architecture Design

							disconnected, this line in disconnected at that end and the unavailability of one bus-bar is appropriately simulated in this substation in the grid model 4) if a transformer bay is to be disconnected, this transformer is disconnected at both ends and the unavailability of one bus-bar is appropriately simulated in this switchyard in the grid model 5) if a bus-bar is to be disconnected, all feeders are appropriately simulated in the grid model as being connected to other bus-bars(s) 6) If a coupling bay is to be disconnected, this bay is disconnected in the grid model etc.
EMM_071	EMMA TTA shall export the topology file to the predefined server (grid model server)	EMM A	Functional and data	This requirement is needed for UC17 Outage coordination and automated creation of	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

			requirements	topology files for Individual Grid Models			
EMM_072	The topology report shall list all network elements whose topology status differs from the topology in the default topology file	EMM A	Functional and data requirements	This requirement is needed for UC17 Outage coordination and automated creation of topology files for Individual Grid Models	All required functionalities are provided	5	
EMM_073	The list of elements that are subject to planned outages must contain: network element type, network element designation, disconnection period, time and type of switching, and description of switching state change (continuous/daily)	EMM A	Functional and data requirements	This requirement is needed for UC17 Outage coordination and automated creation of topology files for Individual Grid Models	All required functionalities are provided	5	
EMM_074	EMMA TTA shall create a default topology file in .csv format	EMM A	Functional and data requirements	This requirement is needed for UC17 Outage coordination and automated creation of topology files for Individual Grid Models	All required functionalities are provided	5	
EMM_075	EMMA TTA shall create an updated topology file in TOP file (format used by eTNA power	EMM A	Functional and data requirements	This requirement is needed for UC17 Outage coordination and automated creation of	All required functionalities are provided	5	



D2.3 – Requirements and Detailed Architecture Design

	flow calculation software)			topology files for Individual Grid Models			
EMM_076	EMMA TTA shall create a topology report file in .xls or .pdf format	EMM A	Functional and data requirements	This requirement is needed for UC17 Outage coordination and automated creation of topology files for Individual Grid Models	All required functionalities are provided	5	
EMM_077	If RA has a positive effect on XNEC unloading and the price of RA is positive (TSO activating the RA pays to balancing entity) then EMMA RA CSS will distribute RA.TSO costs between CNT.TSO and XNEC.TSO equally.	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	XNEC – network element affected by the constraint CNT.TSO – TSO in which Control Area is contingency (CNT) XNEC.TSO – TSO in which Control Area is XNEC RA.TSO – TSO activating remedial action (RA)
EMM_078	If RA has positive effect on XNEC unloading and RA price is negative (balancing entity pays to TSO activating RA) then EMMA RA CSS will distribute equally RA.TSO income between RA.TSO, CNT.TSO and XNEC.TSO.	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	XNEC – network element affected by the constraint CNT.TSO – TSO in which Control Area is contingency (CNT) XNEC.TSO – TSO in which Control Area is XNEC RA.TSO – TSO activating remedial action (RA)

D2.3 – Requirements and Detailed Architecture Design

EMM_079	If RA has negative effect on XNEC unloading and RA price is negative then EMMA RA CSS will distribute equally RA.TSO income between CNT.TSO and XNEC.TSO	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	XNEC – network element affected by the constraint CNT.TSO – TSO in which Control Area is contingency (CNT) XNEC.TSO – TSO in which Control Area is XNEC RA.TSO – TSO activating remedial action (RA)
EMM_080	If RA has negative effect on XNEC unloading and RA price is positive (TSO activating RA pays to balancing entity) then EMMA RA CSS will not distribute any costs between involved TSOs (CNT.TSO, XNEC.TSO, RA.TSO).	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	This case should be very rare as unwanted effect of regional RA optimization. XNEC – network element affected by the constraint CNT.TSO – TSO in which Control Area is contingency (CNT) XNEC.TSO – TSO in which Control Area is XNEC RA.TSO – TSO activating remedial action (RA)
EMM_081	If there is a constraint without contingency, RA has positive effect on XNEC unloading and RA price is positive (TSO activating RA pays to balancing entity)	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	XNEC – network element affected by the constraint XNEC.TSO – TSO in which Control Area is XNEC RA.TSO – TSO activating remedial action (RA)

D2.3 – Requirements and Detailed Architecture Design

	then EMMA RA CSS will distribute all RA.TSO costs to XNEC.TSO.						
EMM_082	If there is a constraint without contingency, RA has positive effect on XNEC unloading and RA price is negative (balancing entity pays to TSO activating RA) then EMMA RA CSS will distribute RA.TSO income equally between RA.TSO and XNEC.TSO	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	XNEC – network element affected by the constraint XNEC.TSO – TSO in which Control Area is XNEC RA.TSO – TSO activating remedial action (RA)
EMM_083	If there is a constraint without contingency, RA has negative effect on XNEC unloading and RA price is negative (balancing entity pays to TSO activating RA) then EMMA RA CSS will distribute all RA.TSO income to XNEC.TSO.	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	XNEC – network element affected by the constraint XNEC.TSO – TSO in which Control Area is XNEC RA.TSO – TSO activating remedial action (RA)
EMM_084	If there is a constraint without contingency, RA has negative effect on XNEC unloading and RA price positive (TSO activating RA pays to balancing entity) then	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	This case should be very rare as unwanted effect of regional RA optimization. XNEC – network element affected by the constraint



D2.3 - Requirements and Detailed Architecture Design

	then EMMA RA CSS will not distribute any costs between involved TSOs (XNEC.TSO, RA.TSO).						XNEC.TSO – TSO in which Control Area is XNEC RA.TSO – TSO activating remedial action (RA)
EMM_085	For each RA applied in one market interval, RA costs EMMA RA CSS will distribute proportionally to all XNECs that are positively affected by an RA (unloading). This way pairs RA-XNEC are created.	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	XNEC – network element affected by the constraint RA – remedial action
EMM_086	After EMM_085 requirement is applied, RA costs in one market interval previously allocated to specific XNEC is furthermore decomposed for each CNT proportionally to the percentage of overload caused by contingencies (included base case constraints).	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	Base case constraint is treated equally to constraint due to contingency. This way triplets RA-CNT-XNEC are created. CNT – contingency XNEC – network element affected by the constraint RA – remedial action
EMM_087	After EMM_086 requirement is applied, for each RA-CNT-XNEC triplet, EMM_077 -	EMM A	Functional and data	This requirement is needed for UC13 Cost-sharing of remedial actions with	All required functionalities are provided	5	CNT – contingency XNEC – network element affected by the



D2.3 – Requirements and Detailed Architecture Design

	EMM_084 requirement is applied by EMMA RA CSS. This way costs are allocated to all involved TSOs.		requirements	cross-border impact in West Balkan region			constraint RA – remedial action
EMM_088	After EMM_087 requirement is applied, EMMA RA CSS will sum all costs/incomes for each TSOs.	EMM_A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_089	RAs costs must be submitted by TSO that activated RAs in its Control Area, in an excel file or similar format, with the costs indicated for each market interval during the day, date and costs. Costs must be expressed in euros.	EMM_A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_090	Common Grid Model must be in CGMES or ucte format	EMM_A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_091	EMMA RA CSS must be capable to import PTDF file, RA costs file and base case flows file (all in excel format).	EMM_A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	



D2.3 – Requirements and Detailed Architecture Design

EMM_092	EMMA RA CSS must be capable to create report in .txt, .csv, .doc, .xsl or other widely used format.	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_093	Cost-sharing report is created on daily basis with the granulation equal to the basic market interval.	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	Cost-sharing report must present all input values (RA costs, PTDF value for RAs impact on network elements with constraint, all contingencies, all overloads in % on every affected network element due to a contingency), all RA-CNET-CNT triplets, all TSOs correlated with RAs, CXNECs and CNTs and allocated cost to all involved TSOs for each RA-XNEC-CNT triplet. Next, report must present total costs/incomes allocated to all involved TSOs for each market interval during a day, and cost/incomes sum on a daily level. CNT – contingency XNEC – network element affected by the



D2.3 - Requirements and Detailed Architecture Design

							constraint RA – remedial action
EMM_ 094	EMMA RA CSS shall have 3 modules: 1) Cost sharing calculation module, 2) database modules (RAs, CNTs and XNECs) and 3) Cost sharing calculation parameters setting module.	EMM A	Function al and data requirem ents	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	CNT – contingency XNEC – network element affected by the constraint RA – remedial action
EMM_ 095	EMMA RA CSS main form must have command buttons to direct to each module and navigation command buttons	EMM A	Look and feel requirem ents	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_ 096	'EMMA RA CSS - Cost-sharing calculation / Date and time' form must have fields to enter date and market time interval and navigation buttons	EMM A	Look and feel requirem ents	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_ 097	'RA CSS - Cost-sharing calculation / Information on RAs' form must have fields to enter RA node label, RA direction, RA cost, command button for	EMM A	Look and feel requirem ents	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	RA – remedial action



D2.3 - Requirements and Detailed Architecture Design

	new RA and navigation buttons						
EMM_098	'EMMA RA CSS - Cost-sharing calculation / Information on CNTs and XNECs' form must have fields to enter CNT label, XNEC label, XNEC overload percentage for CNT, command buttons for new CNTs and XNECs and navigation buttons.	EMM A	Look and feel requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	CNT – contingency XNEC – network element affected by the constraint
EMM_099	'EMMA RA CSS - Cost-sharing calculation / Base Case flows import' form must have command button for base case flows file import from the predefined folder	EMM A	Look and feel requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_100	'EMMA RA CSS - Cost-sharing calculation / PTDF matrix import' form must have command button for PTDF file import from predefined folder	EMM A	Look and feel requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	



D2.3 – Requirements and Detailed Architecture Design

EMM_101	'EMMA RA CSS - Cost-sharing calculation / Results' form must have fields to display, date and market time interval and RA cost sharing calculation results	EMM A	Look and feel requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_102	'EMMA RA CSS - RAs, CNTs and XNECs database' form must have command button to open RAs, CNTs and XNECs databases	EMM A	Look and feel requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	CNT – contingency XNEC – network element affected by the constraint RA – remedial action
EMM_103	EMMA RA CSS - RA database must contain data on RA ID, activating TSO and RA label (generation or demand node)	EMM A	Look and feel requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_104	EMMA RA CSS - CNTs & XNECs database must contain the following data on network elements representing CNTs & XNECs: ID, label, starting node, ending node, TSO operating starting node and TSO operating ending node	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	CNT – contingency XNEC – network element affected by the constraint



D2.3 - Requirements and Detailed Architecture Design

EMM_105	EMMA RA CSS - TSOs database must contain the following data on participating TSOs: ID and TSO name	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_106	EMMA RA CSS - Cost-sharing calculation parameters settings database must contain data on TSO activating RA, TSO operating CNT (both nodes), TSO operating XNEC (both nodes), RA cost/impact quadrant and cost sharing factors between TSOs	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	CNT – contingency XNEC – network element affected by the constraint RA – remedial action
EMM_107	'EMMA RA CSS - Cost-sharing calculation sensitivity' form must have a field to enter PTDF sensitivity threshold.	EMM A	Look and feel requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_108	EMMA RA CSS must be capable to read, delete, create and update data stored in RA, TSOs and CNTs & XNECs databases	EMM A	Functional and data requirements	This requirement is needed for UC13 Cost-sharing of remedial actions with cross-border impact in West Balkan region	All required functionalities are provided	5	
EMM_109	EMMA OP tool must create UAP file, export this file to server, and	EMM A	Functional and data	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	import the manually reconfigured UAP file.		requirements				
EMM_110	EMMA OP tool must create Gantt charts showing the period of network elements planned outages with the following granularity: a) the whole year by hours, b) the whole year by days	EMMA	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	
EMM_111	EMMA OP tool Gantt charts will contain horizontal and vertical sliders to allow good visibility of outage periods. The parts of the chart that contain the date/time and network element label will be fixed on the screen.	EMMA	Look and feel requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	4	



D2.3 – Requirements and Detailed Architecture Design

EMM_112	EMMA OP tool must have automatic and manual mode for performing OPI assessment.	EMM A	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	Based on information from Gantt chart, OP admin prepares input data (CGMs, CON lists and MON lists) which will be used for upcoming Outage Planning Incompatibility (OPI) assessment. OPI assessment represents security analysis on reference model in which proposed outages are applied. This security analysis is performed using modified network model (base case CGM where proposed outages are applied), CON list (contingency list – elements which disconnection will be simulated during OPI assessment) and MON list (monitoring list – elements which will be monitored in order to detect overload after simulation of contingency).
---------	---	-------	----------------------------------	---	---	---	--



D2.3 - Requirements and Detailed Architecture Design

EMM_113	EMMA OP tool should control eTNA offline instance using API.	EMM A	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	OPR (Outage Planning Processor, module of OP tool in charge for communication with other modules and for processing outage planning requests) should be able to communicate with eTNA instance via API – it should be able to send commands to eTNA for importing needed files as well as for performing calculations needed for the optimization of outage planning requests.
EMM_114	EMMA OP tool will store OPI results in a database and display them in appropriate manner	EMM A	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	
EMM_115	EMMA OP tool should calculate certain indicators based on OPI results	EMM A	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	KPI1 and KPI2 are defined in the EMMA OP tool technical specification
EMM_116	EMMA OP tool administrator must have supervisor access and will be able to	EMM A	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	change all locations for file import/export.						
EMM_117	EMMA OP tool must import EIC vs CIM ID cross-reference table periodically.	EMM A	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	EIC vs CIM ID cross-reference table will be updated externally and then imported to the OPR module by OP tool operator periodically.
EMM_118	EMMA OP tool must allow the operator to delete OPC CON files on a dedicated server.	EMM A	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	Since there will be many OPC CON files generated for performing the security analysis, there is a need for deletion of these files after certain amount of time when they are not needed anymore.
EMM_119	EMMA OP tool must export the UAP file in XML format.	EMM A	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	
EMM_120	EMMA OP tool must allow OP operator to manually create initial UAP files for specific periods (yearly, quarterly, weekly).	EMM A	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	When deadline for delivery of outages list is reached, the initial UAP file is delivered based on the manual action of the OP admin (not based on time trigger).
EMM_121	EMMA OP tool must limit in automatic mode, the number of	EMM A	Functional and data	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	elements which can change status (ON and OFF) should be chosen in a way that eTNA calculations are executed in a reasonable time		requirements				
EMM_122	EMMA OP tool must have access to CGM, CON and MON files for each hour for which the calculations are performed. If that is not the case, the user should be informed with the appropriate message.	EMMA	Functional and data requirements	This requirement is needed for UC8 Outage planning optimization	All required functionalities are provided	5	In order for eTNA to perform the security analysis, it needs the access to CGM, CON and MON files.
GEN_001	All products GUIs should present results in English language	General requirements	Usability and humanity requirements	GUI must be understandable by a broad audience, including other partners in the consortium and the EC	GUI presents results in english	4	English is not required to be the only language supported nor the default one
GEN_001	All products GUIs should present results in English language	General requirements	Usability and humanity requirements	GUI must be understandable by a broad audience, including other partners in the consortium and the EC	GUI presents results in english	4	English is not required to be the only language supported nor the default one
GEN_001	All products GUIs should present results in English language	General requirements	Usability and humanity requirements	GUI must be understandable by a broad audience, including other partners in the consortium and the EC	GUI presents results in english	4	English is not required to be the only language supported nor the default one



D2.3 - Requirements and Detailed Architecture Design

GEN_002	EMMA should consider the legislative constraints regarding the limited presence of drones near critical infrastructure	General requirements	Legal requirements	There is not a common approach in national legislation to allow the presence of flying objects near critical infrastructure	Propose changes in legislation for effective application of the EMMA product	3	
GEN_004	Bidirectional communication between DSO and involved energy stakeholders is established. Supported protocols mainly MQTT/AMQP (via RabbitMQ broker)	General requirements	Functional and data requirements	Bidirectional communication helps DSO efficiently manage its network	Appropriate hardware/software allowing bidirectional communication is in place.	5	
GEN_005	Adequate measuring equipment is installed for proper monitoring of the grid	General requirements	Operational requirements	More data available from the DSO with high time granularity is available, contributing to the accuracy of the tools		5	
GEN_006	Historical data from smart meters, sensors, metering devices etc. should be available.	General requirements	Functional and data requirements	Availability of historical metering data for simple analytics and visualization	Availability of all required metering data	5	
GEN_007	Metering data by all involved metering devices (AMI, SCADA, storage systems, etc.) should be anonymised	General requirements	Legal requirements	Metering data should be anonymised for privacy purposes	Availability of having a reliable way to anonymize metering data	5	



D2.3 - Requirements and Detailed Architecture Design

GEN_008	The tools developed should be compatible with different operating systems (Windows, Linux, MacOS, etc.).	General requirements	Functional and data requirements	Tools should be accessible by all end-users		5	
GEN_009	Server/virtual machine technical requirements for tools support must be known as soon as possible.	General requirements	Operational requirements	Knowing early enough the technical requirements will help to avoid extra delays in equipment procurement if needed for hosting purposes.		4	
GEN_010	R2D2 will represent alerts from different products	General requirements	The scope of the product			5	R2D2 will represent alerts from different products to manage cybersecurity incidents
GEN_011	A communication channel between DSO - TSO must be existent	General requirements	Functional and data requirements	For purposes of UC37 realization, a communication channel between System and Network Operators must exist		5	For simulation purposes of UC37, information regarding a potential cascading effect must be sent as an alert to from the network towards the system operator (or reverse) via phone, mail, etc.
IRI_001	IRIS application should be available and accessible to end-users	IRIS	Security requirements		The application is accessible over Internet or private network	1	



D2.3 - Requirements and Detailed Architecture Design

IRI_002	When the user log into IRIS application, IRIS application should get the information who is connected and his affected organization/company and roles in the application to apply the correct rights to functionalities	IRIS	Security requirements		The user is recognized and the correct rights to functionalities inside the application is applied	1	May use OIDC/oAuth2 protocole token and Keycloak for creating and managing user account, user roles and organization
IRI_003	The ICL tools shall list conditions when electricity load cannot be met by supply	IRIS	The scope of the work	To identify system conditions where the involuntary loss of load will happen	When the listed conditions happen, involuntary loss of load > 0	5	
IRI_004	IRIS solution shall use standards in the different components (CIM models, OPC format, etc.)	IRIS	Naming conventions and definitions	Ensure interoperability and modularity of the solution	Standards are shared between components	5	Standards to be used in the different modules of the IRIS Solutions, including : - CIM Standard / possibly CGMES standard / other for network computation - OPC format standard - to be extended to DSO ?
IRI_007	IRIS should ensure interoperability between shared / redundant components	IRIS	Functional and data requirements	Allow inter operability from different technology providers		3	Common modules (Load Flow Engine, optimizers, etc.) shall be available in different instantiation (IMP Load Flow, ILC LF, etc.). Same for other features.



D2.3 - Requirements and Detailed Architecture Design

IRI_008	IRIS DSO "Flexibility system" should operate as protocol communication gateway supporting different standard communication protocols like IEC 60870-5-104, MQTT, ICCP/TASE.2	IRIS	The scope of the product			5	
IRI_009	IRIS DSO "Flexibility system" must be able to receive data from multiple source types	IRIS	Operational requirements			5	
IRI_010	IRIS DSO "Flexibility system" should contain a database to store the received and processed data	IRIS	The scope of the product			5	
IRI_011	IRIS DSO "Flexibility system" database should be scalable	IRIS	Performance requirements			4	
IRI_012	IRIS DSO "Flexibility system" should automatically trigger commands/alerts based on rules/algorithms	IRIS	Operational requirements			5	
IRI_013	IRIS DSO "Flexibility system" system should send identified	IRIS	Usability and humanity			5	



D2.3 - Requirements and Detailed Architecture Design

	commands/alarms to different destinations based on a configuration		requirements				
IRI_014	IRIS DSO "Flexibility system" should have the Web GUI	IRIS	Usability and humanity requirements			5	
IRI_015	IRIS DSO "Flexibility system" GUI access should be secure.	IRIS	The scope of the product			5	
IRI_016	IRIS must provide phasors angle difference monitoring	IRIS	Functional and data requirements	IRIS product must be capable to receive data from PMUs, calculate angle difference between two observed points and generates an alarm when this angle is larger than critical value or a lack of adequate measurements of any PMU is detected	All required functionalities are provided	5	
IRI_017	The IRIS product must contain Emergency and Restoration – Over-frequency protection module (OFPM)	IRIS	Functional and data requirements	OFPM is a system designed to simulate missing limited frequency sensitive mode - over-frequency (LFSM-O) controllers in generators according to the relevant EU regulation (NC ER).	All required functionalities are provided	5	The IRIS product shall have the following functionalities: 1) Reads relevant SCADA measurements 2) Calculates various thresholds and over-frequency settings 3) Sends over-frequency protection settings to



D2.3 - Requirements and Detailed Architecture Design

							protection devices 4) Receives confirmation signal from protection devices 5) Sends generators set-points to SCADA/AGC 6) Sends disconnect signal to selected generators
IRI_018	The IRIS product must contain Emergency and Restoration – System Split module (ER-SSM)	IRIS	Functional and data requirements	The ER SSM is a module designed to assist RCC and TSO operators to follow all the rules defined in EU regulation (NC ER) and Continental Europe Synchronous Area Operation Agreement during a system split	All required functionalities are provided	5	Emergency & Restoration - System Split module will be designed to: 1) Detect system split 2) Generate warning on needed action (regarding Frequency Restoration Controllers operation mode, manual Frequency Restoration and Replacement Process status, Frequency Leader nomination...)3) Receive confirmation on performed actions 4) Share other needed information (such as appointment of the Resynchronization Leader, info on upcoming/executed resynchronization, info on selected Frequency Leader after resynchronization...) 5)



D2.3 - Requirements and Detailed Architecture Design

							Identify and display all directly affected TSOs 6) Calculate which TSO should act as Frequency Leader
IRI_019	The IRIS product must include RES and end-load forecasting tool	IRIS	Functional and data requirements	In order to improve the quality of the individual grid model, it is necessary to separate the prediction of end load and RES at the distribution level	All required functionalities are provided	5	IRIS Forecasting Tool must have the ability to 1) produce RES output depending on the type of production unit (wind, sun) and location and 2) forecast final consumption and 3) aggregate this production/consumption according to the distribution TS connected to the transmission system
IRI_020	IRIS product must contain a communication platform	IRIS	Functional and data requirements	IRIS Communication Platform must provide the following services: 1) Participants can upload / download files 2) Files are kept for a certain period 3) Participants can exchange notifications and acknowledgements 4) A conference call can be started	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

IRI_02 1	IRIS product must contain Remedial Action tool	IRIS	Functional and data requirements	Remedial Action tool must indicate in close to real time possible and optimized RAs	All required functionalities are provided	5	IRIS RA tool must be designed to: 1) Receive information on detected constraints 2) Import a price list of re-dispatching 3) Import grid model 4) Calculate applicable RAs and sort them according to costs 5) Send selected RAs 6) Enable manual confirmation of selected RAs 7) Send control signals to SCADA/EMS system 6) Send alarms to SCADA/EMS with proper messages
IRI_02 2	IRIS product must contain an application to optimize PMU installation points in the transmission network	IRIS	Functional and data requirements	The optimization of PMU installation points means the determination of the minimum number of buses in the system (substations, power facilities etc.) where PMU devices need to be installed in order for the given power system to be fully observable.	All required functionalities are provided	5	IRIS OPP Application must be designed to: 1) Enable operator to enter bus data to create connectivity matrix 2) Enable operator to choose one of the given optimization options 3) Enable operator to enter buses with already installed PMUs 4) Calculate optimal installation points 5) Create a file with calculation results



D2.3 - Requirements and Detailed Architecture Design

IRI_02 3	IRIS DSO "Flexibility system" should contain service for voltage profile and loading calculation	IRIS	Functional and data requirements			5	
IRI_02 4	IRIS DSO "Flexibility system" should detect if voltages and/or loadings are outside the expected limits	IRIS	Functional and data requirements			5	
IRI_02 5	IRIS DSO "Flexibility system" should enable checking of execution of control actions	IRIS	Functional and data requirements			5	
IRI_02 6	IRIS DSO "Flexibility system" should contain DER operation optimization for ancillary services, taking into account voltage profile and loadings	IRIS	Functional and data requirements			5	
IRI_02 7	IRIS DSO "Flexibility system" should contain state estimation functionality	IRIS	Functional and data requirements			5	
IRI_02 8	IRIS DSO "Flexibility system" should contain service for defining restrictions in	IRIS	Functional and data			5	



D2.3 - Requirements and Detailed Architecture Design

	ancillary service control actions to prevent voltage and loadings outside the expected limits		requirements				
IRI_029	IRIS DSO "Flexibility system" should be able to send restriction to all service providers (TSO, Aggregator, Balancing responsible, Consumer, DER)	IRIS	Functional and data requirements			5	
IRI_030	The alarm on critical angle difference between two observed points by PMUs must be in sound form, accompanied by information about the angle difference, and the places where PMUs are installed. It must be ensured that operator can acknowledge the alarm.	IRIS	Functional and data requirements	This requirement is needed for UC22 Monitor phasor angles and if a critical angle is reached apply generation re-dispatching to prevent network instability	All required functionalities are provided	5	
IRI_031	The alarm on lack of adequate measurements of any PMU must be in sound form, accompanied by information about the place where the faulty PMUs is installed. It	IRIS	Functional and data requirements	This requirement is needed for UC22 Monitor phasor angles and if a critical angle is reached apply generation re-dispatching to prevent network instability	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	must be ensured that the operator can acknowledge the alarm.						
IRI_03 2	IRIS OPP application must allow the user to draw a network graph (branches and nodes) using a computer mouse or to enter all network branches in a table with two columns (start and end nodes) defining connectivity matrix.	IRIS	Functional and data requirements	This requirement is needed for UC16 Optimization of PMU installation points	All required functionalities are provided	5	
IRI_03 3	IRIS OPP must allow the user to select the optimization criteria for the selection of the installation points of the PMUs as follows: Basic optimisation, N-1 optimisation, Optimisation with already installed PMUs	IRIS	Functional and data requirements	This requirement is needed for UC16 Optimization of PMU installation points	All required functionalities are provided	5	
IRI_03 4	If the user selects the optimization option with PMUs already installed, IRIS OPP opens a new window where the user can enter the buses where	IRIS	Functional and data requirements	This requirement is needed for UC16 Optimization of PMU installation points	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	PMUs are already installed.						
IRI_035	After starting the calculation for the selected optimization process, IRIS OPP displays in a new window (or popup window) all solutions of the applied optimization.	IRIS	Functional and data requirements	This requirement is needed for UC16 Optimization of PMU installation points	All required functionalities are provided	5	
IRI_036	IRIS OPP must calculate and display with each optimal solution the SORI parameter to describe the quality of optimization solution	IRIS	Functional and data requirements	This requirement is needed for UC16 Optimization of PMU installation points	All required functionalities are provided	5	
IRI_037	IRIS OPP creates an optimization report in .docx or .csv format, which contains all relevant input data and all optimization results, as well as the optimization quality parameter. The report is saved in a predefined folder.	IRIS	Functional and data requirements	This requirement is needed for UC16 Optimization of PMU installation points	All required functionalities are provided	5	
IRI_038	It must be possible to record all communication during a single session for	IRIS	Functional and data	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	system split (all records must be time-stamped) in the E&R - System Split module.		requirements				
IRI_039	The Emergency & Restoration - System Split module communication tool displays must have a header with the inscription System Split throughout the procedure described in steps 1 – 35 and the name of the step currently being executed.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_040	The Emergency & Restoration - System Split module communication tool displays must contain a bar graph of all System Split procedure steps with the currently active step highlighted.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_041	After the system split is detected, the Emergency & Restoration - System Split module communication tool is automatically started	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	at all TSOs and RCC with a corresponding sound alarm.						
IRI_04 2	The RCC must have the ability to manually jump to any step of the system split scenario. In this case, a corresponding message and a sound alarm are generated at all TSOs.	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	
IRI_04 3	Each Emergency & Restoration - System Split module display must contain a message field that is editable for each user and in which all previous messages can be viewed during one procedure.	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	
IRI_04 4	When opening each new Emergency & Restoration - System Split module display, a sound alarm should be activated, which is deactivated by manual action of the operator receiving the information.	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

IRI_04 5	All displays of Emergency & Restoration - System Split module should show the responses of all TSOs/RCCs to the requested actions.	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	
IRI_04 6	When a declaration in Emergency & Restoration - System Split module (agree/disagree) is required, then there should be two declaration check boxes, one for agree (YES) and one for disagree (NO).	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	
IRI_04 7	After acting on some control of Emergency & Restoration - System Split, it is necessary to open a dialog box asking for confirmation of activation/change of control status.	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	
IRI_04 8	When a System Split procedure step requires a response from TSOs/RCC, such displays should have a countdown timer visible to all	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	participants to see how much time is left to respond. Time periods must be configurable (default value is set to 2 min).						
IRI_049	The RCC as the administrator of the System Split procedure must have the ability to communicate instead of TSOs who cannot do so for technical reasons (e.g. to change statuses, make confirmations, etc.)	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	
IRI_050	When all requested parties have performed the actions required in a particular step, the next display is automatically opened). Note: some steps can be shown on the same display, which is defined by other requirements.	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	
IRI_051	At each System Split procedure step, a button for starting the teleconference must be available, in which	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	case the corresponding audio message about the requested teleconference is activated for all participants.						
IRI_05 2	When a system break is detected, a visual and sound warning is created that a system break has been detected. The visual information must contain the number of islands detected, and which TSO is in which island.	IRIS	Functional and data requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	5	
IRI_05 3	One display opens for System Split procedure steps 1 and 2 with appropriate warning on system split detection and contains a separate check box for confirmation by all TSOs.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_05 4	One display opens for System Split procedure steps 3 and 4 with appropriate information on identified affected TSOs warning and	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	



D2.3 - Requirements and Detailed Architecture Design

	contains a separate check box for confirmation by all TSOs.						
IRI_05 5	One display opens for System Split procedure steps 5 and 6 with appropriate warning on required frequency deviation management actions and contains a separate check box for confirmation by all TSOs.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_05 6	System Split procedure display for steps 5 and 6 contains warning on required EAS communication on system state and a separate check box for confirmation by all TSOs.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_05 7	One display opens for steps System Split procedure 7, 8 and 9 with information on Frequency Leader determination results, nominated Frequency Leader and contains a separate check box for	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	



D2.3 - Requirements and Detailed Architecture Design

	confirmation by all TSOs.						
IRI_058	One display opens for steps System Split procedure 10 and 11 with appropriate warning on required frequency deviation management actions and contains a separate check box for confirmation by all TSOs.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_059	One display opens for steps System Split procedure 12 and 13 with appropriate warning on required further frequency deviation management actions and contains a separate check box for confirmation by all TSOs.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_060	One display opens for steps System Split procedure 14, 15 and 16 with appropriate information on ongoing telco with SAM, nominated	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	



D2.3 - Requirements and Detailed Architecture Design

	Resynchronisation Leader and contains a separate check box for confirmation by all TSOs.						
IRI_06 1	The RCC manually enters the name of the TSO designated as the frequency leader in the display for steps System Split procedure 14, 15 and 16	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_06 2	One display opens for System Split procedure steps 17 and 18 with appropriate warning on required Resynchronization Leader announcement on EAS and contains a separate check box for confirmation by the Resynchronization Leader.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_06 3	One display opens for System Split procedure steps 19 and 20 with appropriate warning on upcoming resynchronisation and contains a separate check box for	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	



D2.3 - Requirements and Detailed Architecture Design

	confirmation by all TSOs and RCC.						
IRI_06 4	One display opens for System Split procedure steps 21 and 22 with appropriate warning on executed resynchronisation and contains a separate check box for confirmation by all TSOs and RCC.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_06 5	One display opens for System Split procedure steps 23 and 24 with appropriate warning on cancelation the Resynchronization Leader status on EAS and contains a separate check box for the cancelation confirmation by the Resynchronization Leader.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_06 6	One display opens for System Split procedure steps 25, 26 and 27 with appropriate information on ongoing telco to select	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	



D2.3 - Requirements and Detailed Architecture Design

	Frequency Leader after resynchronisation, nominated Frequency Leader and contains a separate check box for TSO/RCC confirmation.						
IRI_067	The Frequency Leader of the region manually enters the name of the TSO designated as the Frequency Leader after resynchronisation in the display opened for System Split procedure steps 25, 26 and 27.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_068	One display opens for System Split procedure steps 28 and 29 with appropriate warning on confirmation or cancelation of the Frequency Leader status on EAS after resynchronisation.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_069	Display for System Split procedure steps 28 and 29 contains a separate check box for the cancelation confirmation by the Frequency Leader after resynchronisation.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	



D2.3 - Requirements and Detailed Architecture Design

IRI_07 0	One display opens for System Split procedure steps 30 and 31 with appropriate warning on Frequency Deviation Management after Resynchronisation and contains a separate check box for confirmation by all TSOs.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_07 1	One display opens for System Split procedure steps 32 and 33 with appropriate warning on Return of the Frequency Restoration Controller to Normal Operation Mode and contains a separate check box for confirmation by RCC.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_07 2	One display opens for System Split procedure steps 34 and 35 with appropriate warning on Return of the Frequency Restoration Controller to Normal Operation Mode and update of EAS status regarding Frequency	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	



D2.3 - Requirements and Detailed Architecture Design

	Restoration Controller operation mode.						
IRI_07 3	Display for System Split procedure steps 34 & 35 contains a separate check box for confirmation of Frequency Restoration Controller Operation Mode and for Frequency Restoration Controller Operation Mode on EAS, both by all TSOs except the Frequency Leader	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_07 4	One display opens for steps System Split procedure 36 & 37 with appropriate warnings on Return of the Frequency Restoration Controller to Normal Operation Mode and adjustment of system state status on EAS.	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	
IRI_07 5	Display for System Split procedure steps 34&35 contains a separate check box for confirmation of	IRIS	Look and feel requirements	This requirement is needed for UC19 Emergency & Restoration - System Split module	All required functionalities are provided	4	



D2.3 - Requirements and Detailed Architecture Design

	Frequency Restoration Controller Operation Mode and for Frequency Restoration Controller Operation Mode on EAS, both by Frequency Leader.						
IRI_076	IRIS RA tool must be able to receive the list of CA results in .xml format	IRIS	Functional and data requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	5	
IRI_077	IRIS RA tool must be capable to recognize and offer applicable RAs for CA results and alarms from real time violation.	IRIS	Functional and data requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	5	
IRI_078	IRIS RA tool must allow the operator to select applicable RAs using checkboxes.	IRIS	Look and feel requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	4	
IRI_079	The list of applicable RAs in IRIS RA tool must contain name of RAs, priority index, short and detailed description	IRIS	Functional and data requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	5	
IRI_080	IRIS RA tool must have access to the SCADA/EMS power flow database and	IRIS	Functional and data	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	must be able to enter changes in this database according to the applied RAs.		requirements				
IRI_08 1	IRIS RA tool must be designed to provide the end user with a dialog with Yes/No/Cancel buttons for the final decision whether to perform RA or not	IRIS	Look and feel requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	4	
IRI_08 2	IRIS RA tool must have established connection with the SCADA system to execute RAs.	IRIS	Functional and data requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	5	
IRI_08 3	IRIS RA tool must be able to access the list of constrained (overloaded) network elements from SCADA/EMS database.	IRIS	Functional and data requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	5	
IRI_08 4	IRIS RA tool must allow the operator to select the relevant constraints (overloads) from a list using a check box	IRIS	Look and feel requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	4	
IRI_08 5	IRIS RA tool must be able to send signals to SCADA system in order	IRIS	Functional and data	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	5	



D2.3 – Requirements and Detailed Architecture Design

	to change status on European Awareness System platform.		requirements				
IRI_086	IRIS RA tool, in case of real time security violations, must be able to automatically use available RAs according to priority index.	IRIS	Functional and data requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	5	
IRI_087	IRIS RA tool must be able to access SCADA/EMS Contingency Analysis reports.	IRIS	Functional and data requirements	This requirement is needed for UC21 Remedial Actions Automation	All required functionalities are provided	5	
IRI_088	IRIS OFPM must be active if frequency exceeds 50.2 Hz	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	
IRI_089	IRIS OFPM must calculate total needed decrease of active power generation in case of over-frequency Pdec [MW] as follows (for LFSM-O droop of 5%): $P_{dec} = P_{total} \cdot (40 \cdot f - 2008)$	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	- Ptotal – Total active power generation in TSO Control Area [MW] at the moment of the over-frequency appearance - f – frequency [Hz]



D2.3 – Requirements and Detailed Architecture Design

IRI_090	For each generator available for active power decrease, IRIS OFPM must calculate: $P_{dw} = P - P_{min}$. In addition the sum of P_{dw} for all generators shall be calculated – $SUM(P_{dw})$.	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	<ul style="list-style-type: none">- P_{dw} – available generators downward active power reserve- P – generators active power measured at the beginning of the OFPM activation due to over-frequency- P_{min} – generators minimum active power for permanent operation (so called technical minimum)
IRI_091	IRIS OFPM must recalculate total active power decrease, available downward reserves and generators base (set) points in time interval set by OFPM operator.	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	
IRI_092	IRIS OFPM operator must be able to set available downward active power reserve threshold ($P_{threshold}$) and frequency threshold ($f_{threshold}$).	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

IRI_093	IRIS OFPM will firstly activate reduction of active power on generators if $f > 50.2$ Hz and secondly disconnection of the generators if the following condition is met: $SUM(PH_{dw}) + SUM(PT_{dw}) + SUM(PW_{dw}) < P_{threshold}$ or $f > f_{threshold}$	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	<ul style="list-style-type: none">- SUM(PH_{dw}) – available total downward active power for all hydro generators- SUM(PH_{dw}) – available total downward active power for all hydro generators- SUM(PT_{dw}) – available total downward active power for all thermal generators- SUM(PW_{dw}) – available total downward active power for all wind generators
IRI_094	IRIS OFPM will reduce generators active power according to the following priority: Hydro Power Plants, Thermal Power Plants, Wind Parks (according to the Serbian pilot site characteristics).	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	
IRI_095	Based on IRI_090 requirement, IRIS OFPM must calculate SUM(PH _{dw}), SUM(PT _{dw}) and SUM(PW _{dw}). In the event of an outage of a generator that is in this	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	<ul style="list-style-type: none">- SUM(PH_{dw}) – available total downward active power for all hydro generators- SUM(PT_{dw}) – available total downward active power for all thermal generators



D2.3 – Requirements and Detailed Architecture Design

	mechanism, $\text{SUM}(\text{PH}_{\text{dw}}) / \text{SUM}(\text{PT}_{\text{dw}}) / \text{SUM}(\text{PW}_{\text{dw}})$ is reduced by the P_{dw} of this generator.						- $\text{SUM}(\text{PW}_{\text{dw}})$ – available total downward active power for all wind generators
IRI_096	If $\text{P}_{\text{dec}} + \text{SUM}(\text{P}_{\text{var}}) < \text{SUM}(\text{PH}_{\text{dw}})$, for each hydro generator IRIS OFPM must calculate new base point P_{b} as follows: $\text{P}_{\text{b}} = \text{P} - [\text{P}_{\text{dec}} + \text{SUM}(\text{P}_{\text{var}})] \cdot \text{P}_{\text{dw}} / \text{SUM}(\text{PH}_{\text{dw}})$. Thermal and wind generators get a base point equal to their active power when OFPM is activated.	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	<ul style="list-style-type: none">- P – generators active power measured at the beginning of the OFPM activation due to over-frequency- P_{dec} – total needed decrease of active power generation- P_{dw} – available generator downward active power- $\text{SUM}(\text{PH}_{\text{dw}})$ – available total downward active power for all hydro generators- $\text{SUM}(\text{P}_{\text{var}})$ – the algebraic sum of the difference of the generator's active power when activating the OFPM and at later iterations, which includes (for the first iteration it is zero):<ul style="list-style-type: none">• disconnection of the generator due to the



D2.3 - Requirements and Detailed Architecture Design

							<p>second mechanism (remote disconnection)</p> <ul style="list-style-type: none">• unexpected outage of any generator• other changes in the active power of generators that are not in this mechanism• reduction in the production of wind generators due to the weakening of the wind
--	--	--	--	--	--	--	--



D2.3 – Requirements and Detailed Architecture Design

IRI_097	If $\text{SUM}(\text{PH}_{dw}) < \text{P}_{dec} + \text{SUM}(\text{P}_{var}) < \text{SUM}(\text{PH}_{dw}) + \text{SUM}(\text{PT}_{dw})$, for each thermal generator IRIS OFPM must calculate new base point P_b as follows: $P_b = P - [\text{P}_{dec} \text{SUM}(\text{P}_{var}) - \text{SUM}(\text{PH}_{dw})] \cdot \text{P}_{dw} / \text{SUM}(\text{PT}_{dw})$. All hydro generators get P_b equal to their technical minimum.	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	<ul style="list-style-type: none">- P – generators active power measured at the beginning of the OFPM activation due to over-frequency- P_{dec} – total needed decrease of active power generation- $\text{SUM}(\text{PH}_{dw})$ – available total downward active power for all hydro generators- P_{dw} – available generator downward active power- $\text{SUM}(\text{PT}_{dw})$ – available total downward active power for all thermal generators- $\text{SUM}(\text{P}_{var})$ – the algebraic sum of the difference of the generator's active power when activating the OFPM and at later iterations, which includes (for the first iteration it is zero):<ul style="list-style-type: none">• disconnection of the generator due to the second mechanism (remote disconnection)• unexpected outage of
---------	---	------	----------------------------------	--	---	---	--



D2.3 - Requirements and Detailed Architecture Design

							<p>any generator</p> <ul style="list-style-type: none">• other changes in the active power of generators that are not in this mechanism• reduction in the production of wind generators due to the weakening of the wind <p>Wind generators get a base point equal to their active power when OFPM is activated.</p>
--	--	--	--	--	--	--	---



D2.3 – Requirements and Detailed Architecture Design

IRI_098	If $\text{SUM}(\text{PHdw}) + \text{SUM}(\text{PTdw}) < \text{Pdec} + \text{SUM}(\text{Pvar}) < \text{SUM}(\text{PHdw}) + \text{SUM}(\text{PTdw}) + \text{SUM}(\text{PWdw})$, for each wind generator IRIS OFPM must calculate new base point $P_b = P - [\text{Pdec} - \text{SUM}(\text{PHdw}) - \text{SUM}(\text{PTdw})] \cdot \text{Pdw} / \text{SUM}(\text{PWdw})$	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	<ul style="list-style-type: none">- P – generators active power measured at the beginning of the OFPM activation due to over-frequency- Pdec – total needed decrease of active power generation- SUM(PHdw) – available total downward active power for all hydro generators- SUM(PTdw) – available total downward active power for all thermal generators- Pdw – available wind generator downward active power- SUM(PWdw) – available total downward active power for all wind parks- SUM(Pvar) – the algebraic sum of the difference of the generator's active power when activating the OFPM and at later iterations, which includes (for the first iteration it is zero):<ul style="list-style-type: none">• disconnection of the generator due to the
---------	---	------	----------------------------------	--	---	---	--



D2.3 - Requirements and Detailed Architecture Design

							<p>second mechanism (remote disconnection)</p> <ul style="list-style-type: none">• unexpected outage of any generator• other changes in the active power of generators that are not in this mechanism• reduction in the production of wind generators due to the weakening of the wind <p>All hydro and thermal generators get P_b equal to their technical minimum.</p>
--	--	--	--	--	--	--	---



D2.3 – Requirements and Detailed Architecture Design

IRI_099	If $SUM(PH_{dw}) + SUM(PT_{dw}) + SUM(PW_{dw}) < P_{dec} + SUM(P_{var})$, IRIS OFPM must calculate for all generators new base point P_b equal to their technical minimum.	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	<ul style="list-style-type: none">- P – generators active power measured at the beginning of the OFPM activation due to over-frequency- P_{dec} – total needed decrease of active power generation- $SUM(PH_{dw})$ – available total downward active power for all hydro generators- $SUM(PT_{dw})$ – available total downward active power for all thermal generators- $SUM(PW_{dw})$ – available total downward active power for all wind parks- $SUM(P_{var})$ – the algebraic sum of the difference of the generator's active power when activating the OFPM and at later iterations, which includes (for the first iteration it is zero):<ul style="list-style-type: none">• disconnection of the generator due to the second mechanism (remote disconnection)• unexpected outage of
---------	---	------	----------------------------------	--	---	---	---



D2.3 - Requirements and Detailed Architecture Design

							any generator • other changes in the active power of generators that are not in this mechanism • reduction in the production of wind generators due to the weakening of the wind
IRI_100	IRIS OFPM shall communicate generators base point signal through: 1) Thermal power plant and wind park gateway 2) TSO connection facility gateway and GRAS devices installed in hydro power plants	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	
IRI_101	All generators in IRIS OFPM disconnection mechanism, will be sorted in array according to local security criteria and additional criteria set by generator owners according to the following priority: Hydro Power Plants, Thermal Power Plants, Wind Parks.	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	



D2.3 – Requirements and Detailed Architecture Design

IRI_102	IRIS OFPM must calculate disconnection frequency for all generators as follows: $f_{disci} [Hz] = (2008 + SUM(Pvar) + 0,5 \cdot Pi + SUM(P1 \rightarrow i-1))/40$	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	<ul style="list-style-type: none">- f_{disci} – disconnection frequency for generator in position 'i' in the generators array set according to Nov9 requirements- P_i – generators active power in position 'i' in the generators array set according to Nov9 requirements (expressed in % of the total active power of all generators in TSO Control Area)- $SUM(P1 \rightarrow i-1)$ – active power sum of generators from the first until the position 'i-1' in (expressed in % of the total active power of all generators in TSO Control Area).- $SUM(Pvar)$ – the algebraic sum of the difference of the generator's active power when activating the OFPM and at later iterations, which includes (for the first iteration it is zero):<ul style="list-style-type: none">• disconnection of the generator due to the first
---------	---	------	----------------------------------	--	---	---	--



D2.3 - Requirements and Detailed Architecture Design

							mechanism (generators active power decrease) <ul style="list-style-type: none">• unexpected outage of any generator• other changes in the active power of generators that are not in this mechanism• reduction in the production of wind generators due to the weakening of the wind
IRI_103	IRIS OFPM must recalculate disconnection frequency for all generators in time interval set by OFPM operator.	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	
IRI_104	IRIS OFPM must communicate generators disconnection signal to circuit breaker of the generators connection line in TSO connection substation	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	
IRI_105	IRIS OFPM must provide to operator observability of generators participating in active	IRIS	Look and feel requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	4	



D2.3 - Requirements and Detailed Architecture Design

	power generation decrease mechanism and generators disconnection mechanism.						
IRI_106	IRIS OFPM operator must be able to include/exclude generators for one or both mechanism (active power generation decrease mechanism / generators disconnection mechanism) before or during OFPM activation.	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	
IRI_107	When over-frequency higher than 50.2 Hz is detected, IRIS OFPM must generate sound alarm that can be cancelled by operator.	IRIS	Look and feel requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	
IRI_108	When over-frequency is detected, OFPM must generate summary display presenting: 1) actual frequency 2) time relapsed from over-frequency detection 3) calculated total active	IRIS	Look and feel requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	power to be reduced 4) total reduced power after over-frequency detection						
IRI_109	When OFPM active power generation decrease mechanism is activated, OFPM must generate a display presenting all data given in comments section.	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	<ul style="list-style-type: none">- Generators' active power at the moment of over-frequency detection- Calculated set-point by OFPM- Generators' actual active power- Total reduced power after over-frequency detection by OFPM / Active power generation decrease mechanism- Remaining summary active power to be reduced by OFPM / Active power generation decrease mechanism
IRI_110	If IRIS OFPM generators disconnection mechanism is active, OFPM must generate a display presenting: Generators' active power at the moment of over-frequency detection, identification if generator is	IRIS	Look and feel requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	



D2.3 - Requirements and Detailed Architecture Design

	disconnected by OFPM / Generators disconnection mechanism						
IRI_111	IRIS OFPM and SCADA must communicate through IPC (inter-process communication).	IRIS	Functional and data requirements	This requirement is needed for UC12 Emergency & Restoration - Over-frequency protection module	All required functionalities are provided	5	
PRE_001	Relevant changes in data which may affect ML-based components must be detectable	PREC OG	Maintainability and support requirements			3	The product has to include mechanisms to characterize statistically data consumed by ML-based components and to track these properties, so that significant changes are detected and models are re-trained/adjusted.
PRE_002	Web service for signing and verification	PREC OG	Functional and data requirements	There is a need for an interface to sign and verify the data, this is one of the options.	Possible to send POST request to a service to sign or verify data that respectively returns a signature or verification results.	3	Whichever option is needed by the pilot use case.
PRE_003	Command line solution for signing and verification	PREC OG	Functional and data requirements	There is a need for an interface to sign and verify the data, this is one of the options.	Command line interface to sign and verify data locally within the same OS, excluding	3	Whichever option is needed by the pilot use case.



D2.3 - Requirements and Detailed Architecture Design

					any KSI Block chain communication.		
PRE_004	Connections to KSI Gateway	PREC OG	Functional and data requirements	Without it is not possible to operate.	KSI Gateway is accessible for the command line tool or for the web service.	5	
PRE_005	Connections to KSI Block chain	PREC OG	Functional and data requirements	Without it is not possible to operate.	KSI Gateway has access to KSI Block chain to serve signing requests and to fetch calendar database.	5	
PRE_006	Sample data sets for tools available as soon as possible after UC-s are defined and agreed	PREC OG	Functional and data requirements	It is needed but could be tested with random data if need be.	Amount and quality of data sets is sufficient to test the tools functionality	4	
PRE_007	KSI tool detects 100% of changed in signed data during verification.	PREC OG	Functional and data requirements	If it does not provide 100% accuracy then the technology would not be valuable.	Must be tested with corrupted datasets	5	
PRE_008	KSI tool confirms integrity of original files on 100% of cases, when verification function is applied on originally signed data.	PREC OG	Functional and data requirements	If it does not provide 100% accuracy then the technology would not be valuable.	Must be tested with original datasets	5	



D2.3 - Requirements and Detailed Architecture Design

PRE_009	Tokenization tool provides tokens, which verify originality of tokenized data in 100% of cases	PREC OG	Functional and data requirements	If it does not provide 100% accuracy then the technology would not be valuable.	Must be tested with originally tokenized datasets	5	
PRE_010	Model (IGM, CGM) shall be available.	PREC OG	Functional and data requirements	It is needed but could be tested with random data if need be.	Amount and quality of data sets is sufficient to test the tools functionality	4	Similar to GEN_006 - "Historical data from smart meters, sensors, metering devices etc. should be available."
PRE_011	Data format must be agreed to run data registration and integrity validation.	PREC OG	Functional and data requirements	Even the slightest change in data results in validation error.	Integrity validation returns equal results for all parties who run validation on tokenized data.	5	
PRE_012	Tokenized data and its token must be stored in the same or different database, a link between them must be maintained.	PREC OG	Functional and data requirements	If the link between data and its token is not maintained, integrity validation can not be conducted.	Tokenized data can be located using created link, validation returns "OK" when data is validated with the token.	5	

D2.3 - Requirements and Detailed Architecture Design

PRE_013	CARMEN product must be able to comprehend and analyze ICS protocols	PREC OG	Functional and data requirements			5	The minimum list of protocols that PRECOG should understand are: - C37.118 - Modbus - S7Comm - Ethernet/IP - 104 - DNP3 - ICCC - Profinet - Lontalk - OPC/DA - OPC/UA - Other protocols that are in demo sites are mandatory.
PRE_014	PRECOG Supply Chain Assessment Tool must provide management guidelines for EPES to secure supply chain	PREC OG	The scope of the product			2	
PRE_015	PRECOG Supply Chain Assessment Tool must provide guidelines for EPES' vendors to use to secure their supply chain and their product development	PREC OG	The scope of the product			2	
PRE_016	PRECOG Supply Chain Assessment Tool must provide guidelines in HTML and PDF format	PREC OG	Usability and humanity	Usability of the developed module		2	



D2.3 - Requirements and Detailed Architecture Design

			requirements				
PRE_017	PRECOG Supply Chain Assessment Tool shall support a self-assessment for EPES Operator vendors/suppliers to evaluate their current supply chain and development practices	PRECOG	The scope of the product			5	
PRE_018	PRECOG Supply Chain Assessment Tool shall support a self-assessment for EPES Operator to evaluate their own supply chain management practices	PRECOG	The scope of the product			4	
PRE_019	PRECOG Supply Chain Assessment Tool should provide scoring mechanisms to assess and evaluate vendor and EPES practices, providing an overall rating or score.	PRECOG	The scope of the product			5	
PRE_020	PRECOG Supply Chain Assessment Tool should be accessible through standard web browsers and compatible with	PRECOG	Usability and humanity requirements	Usability of the developed module		4	



D2.3 - Requirements and Detailed Architecture Design

	different devices, such as desktops, tablets, and smartphones.						
PRE_021	PRECOG Supply Chain Assessment Tool shall be accessible to registered/authorised users to enforce proper access control on the provided information and the assessment results.	PREC OG	Security requirements	The tool should ensure the security and confidentiality of user data and assessment results.		5	Each user will have their own account.
PRE_022	PRECOG Supply Chain Assessment Tool should generate comprehensive reports summarizing the assessment results for vendors and EPES practices.	PREC OG	Functional and data requirements	The tool should generate reports summarizing the assessment results, including overall scores, individual question responses, and any additional comments or recommendations.		4	
PRE_023	Supply Chain Assessment Toolkit must get access to T5.1 tool to register and validate data and its associated proofs	PREC OG	Functional and data requirements			5	
PRE_024	CARMEN product will automatically detect new devices connected to the network	PREC OG	Functional and data requirements			5	Devices will be detected using passive scanning.



D2.3 - Requirements and Detailed Architecture Design

PRE_025	CARMEN will detect potential threats using pattern detection	PREC OG	Functional and data requirements			5	A ML module will be used to cluster the anomalies.
PRE_026	CARMEN product will detect anomalies based on traffic characterization	PREC OG	Functional and data requirements			5	
PRE_027	CARMEN product will detect anomalies based on control, operation and supervision levels	PREC OG	Functional and data requirements			5	
PRE_028	CARMEN will detect operational alerts from IT/OT devices	PREC OG	Functional and data requirements			5	
PRE_029	PRECOG Supply Chain Assessment Tool should monitor new components communications in an isolated (staging/test) environment and for a specific period of time, to identify suspicious communications	PREC OG	The scope of the product			5	
PRE_030	PRECOG Supply Chain Assessment Toolkit	PREC OG	Functional and			5	



D2.3 - Requirements and Detailed Architecture Design

	should identify suspicious communications utilizing T5.4 Deep Learning Data Analytics Module		data requirements				
PRE_031	PRECOG Supply Chain Assessment Toolkit shall utilise the R2D2 block chain to protect the integrity of the assessment results	PREC OG	Functional and data requirements			5	
PRE_032	PRECOG Supply Chain Assessment Toolkit should maintain a list of evaluated components on the Device Origin and Supply Chain Toolkit available to the EPES community.	PREC OG	Functional and data requirements			5	
PRE_033	PRECOG should assure secure communication between DSO "Flexibility system" and devices	PREC OG	Functional and data requirements			5	
PRE_034	PRECOG should alarm DSO IT security department in case of detected attack	PREC OG	Functional and data requirements			5	

D2.3 - Requirements and Detailed Architecture Design

PRE_035	Validation environment for should be offline.	PREC OG	The scope of the product	In order to minimize data security breach, all environments where internet connection is not necessary should be offline.	All links toward internet are disabled for defined virtual machine.	5	Signing process requires access to KSI Block chain. Publication file is needed for verification. Signatures are extended with publication file that is most recent AFTER the signing time. New publications are released every month on 15'th. From there is a need on monthly basis to update publication file and to extend all signatures that were created within last month. Extended signatures could be validated offline with the use of publications (publications file, physical publications such as in NY Times, twitter tweet, etc.) later on.
PRE_036	Environment will be established using virtual machines.	PREC OG	The scope of the product	Easier deployment and maintenance, better monitoring and configuration of resources, more flexibility.	/	5	
PRE_037	Claudia tool has to be installed in a windows device to detect anomalies to act as EDR	PREC OG	Functional and data requirements			5	Claudia is a tool that can be integrated in Carmen for an additional detection in endpoint terms. Is an optional tool



D2.3 - Requirements and Detailed Architecture Design

							but it improves that anomaly detection and helps the analyst for more findings not in the network but on the devices.
PRE_038	Claudia tool needs dependencies for installation	PREC OG	Functional and data requirements			4	In case that Claudia is installed, it will need some dependencies, such as libraries and connectivity with Carmen.
PRE_039	Carmen needs internet connection to S2 servers	PREC OG	Functional and data requirements			5	Carmen needs internet connection to S2 Grupo Carmen central systems in order to update and feedback the information reported. Also it must be necessary to complete the installation.

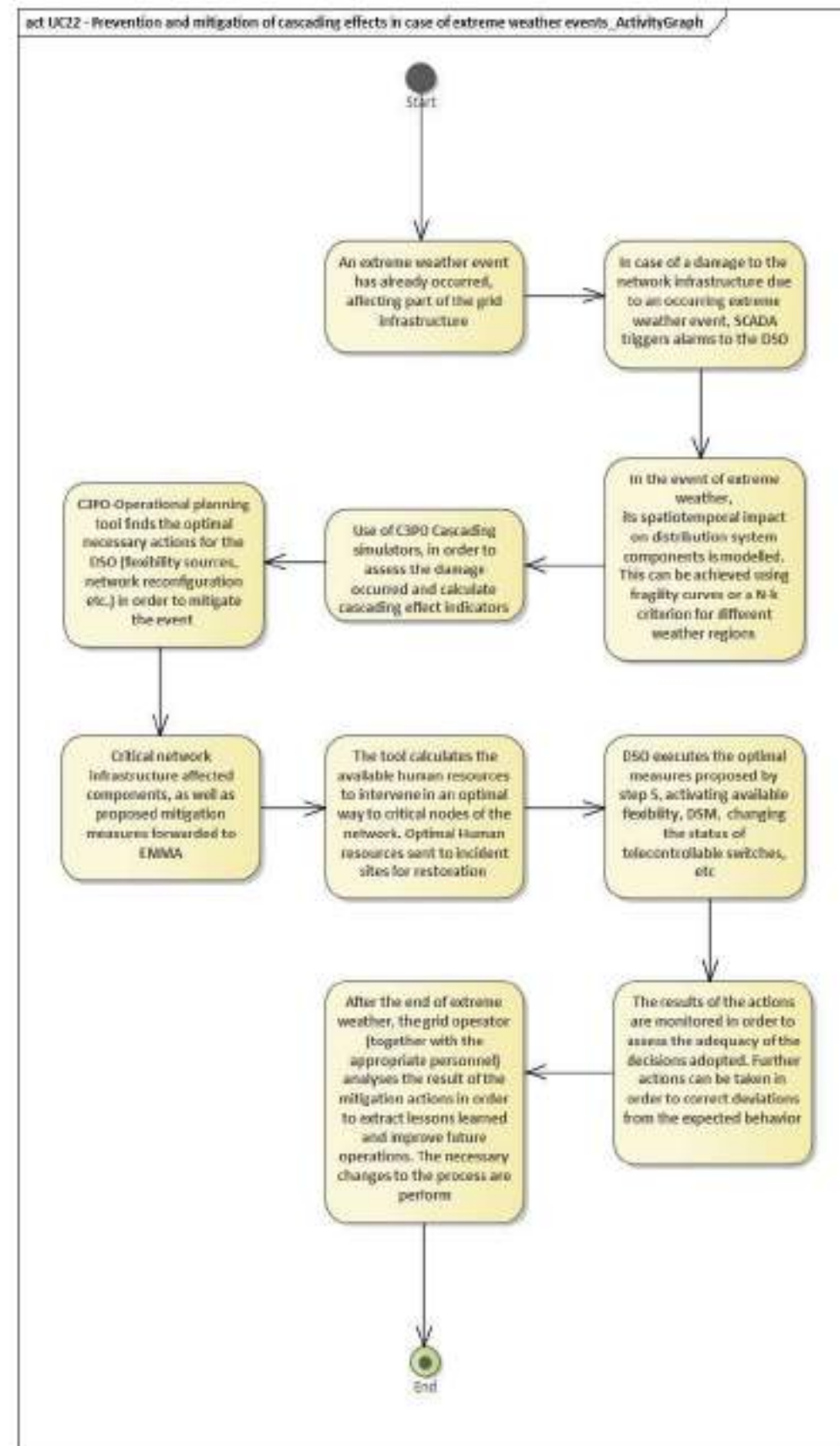


Figure 24 - UC22 Activity Graph

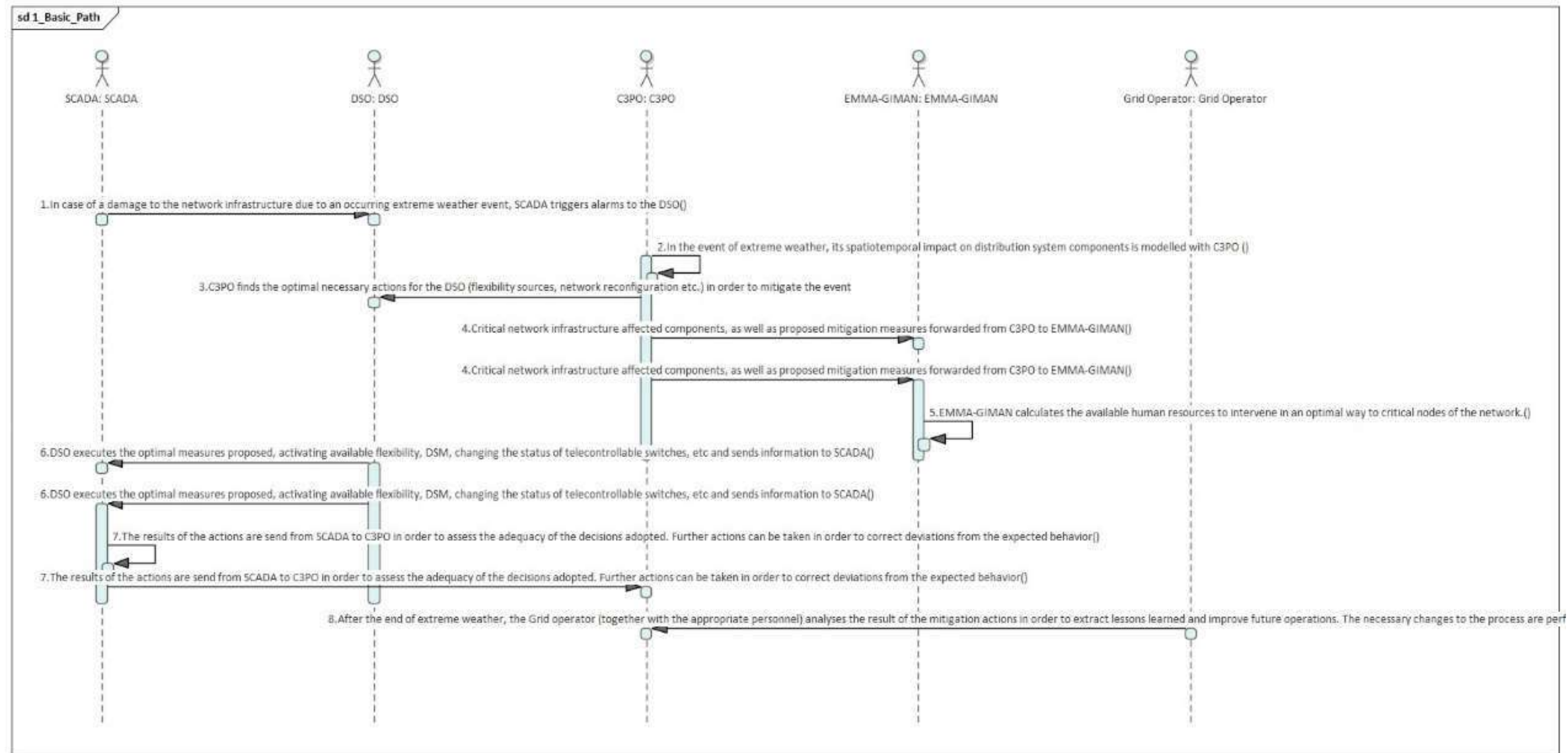


Figure 25 - UC22 Basic Path

UC23 - Cooperative crisis handling in case of cascading event

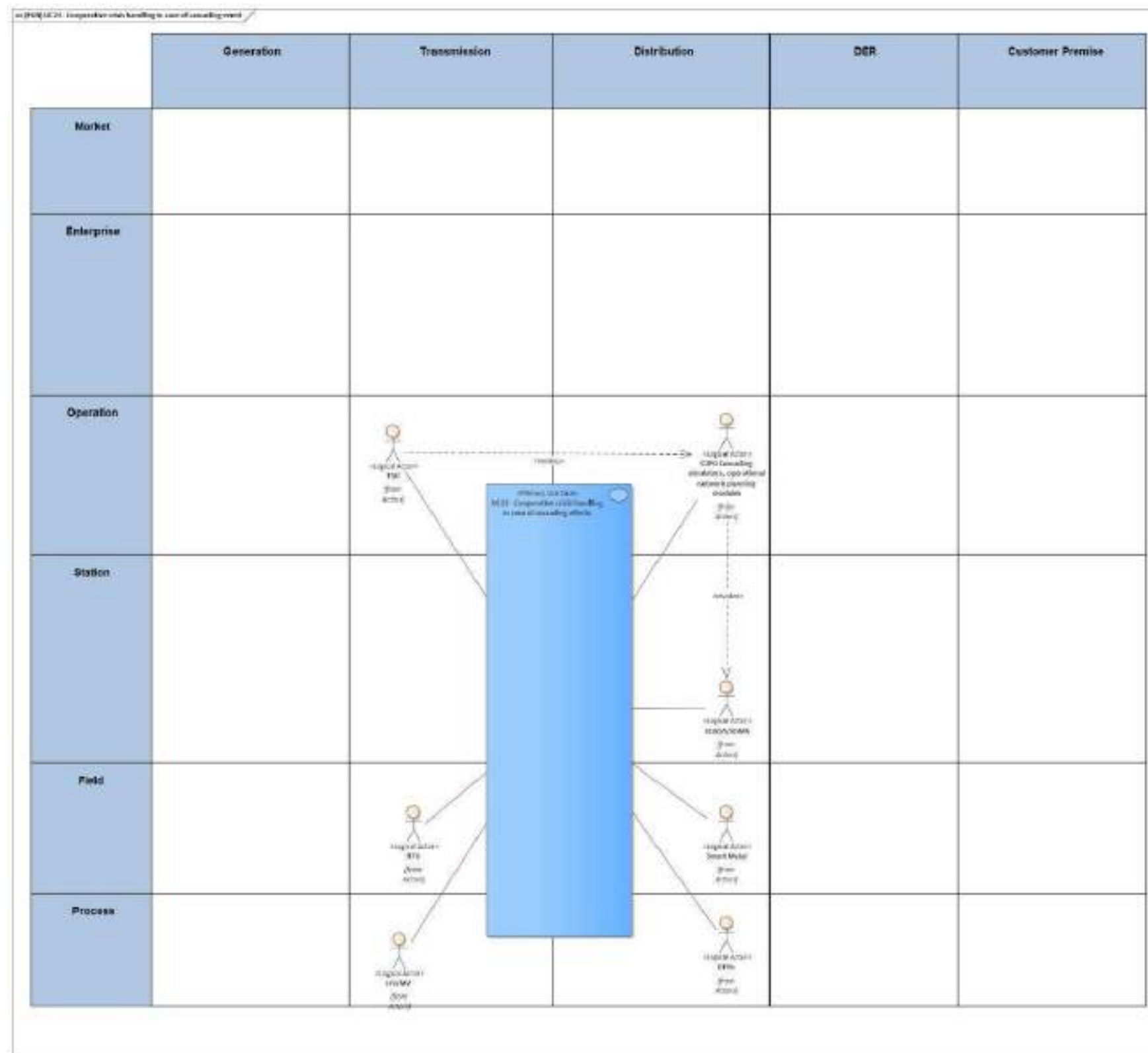


Figure 26 - UC23 Functional layer

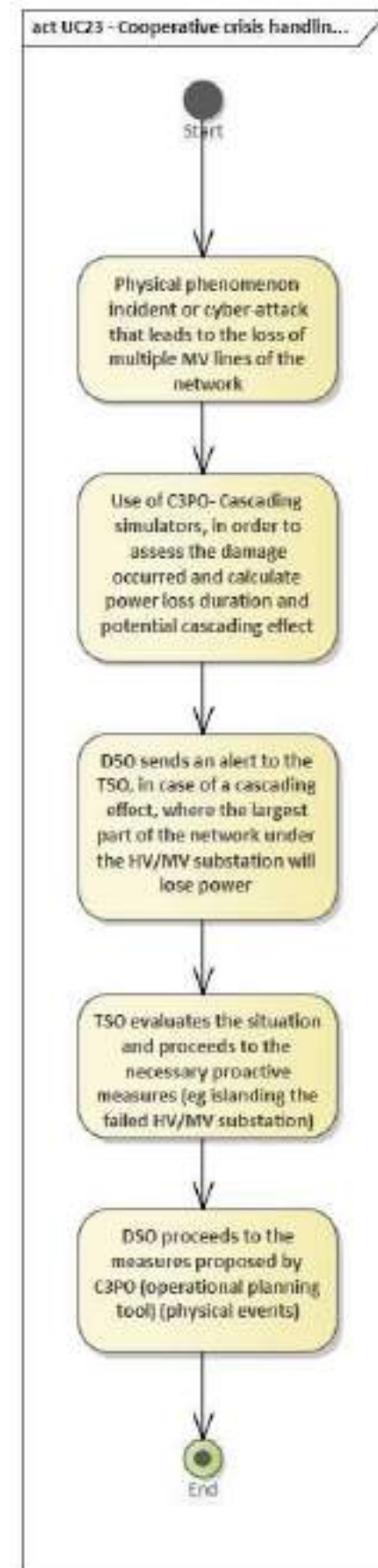


Figure 27 - UC23 Activity Graph

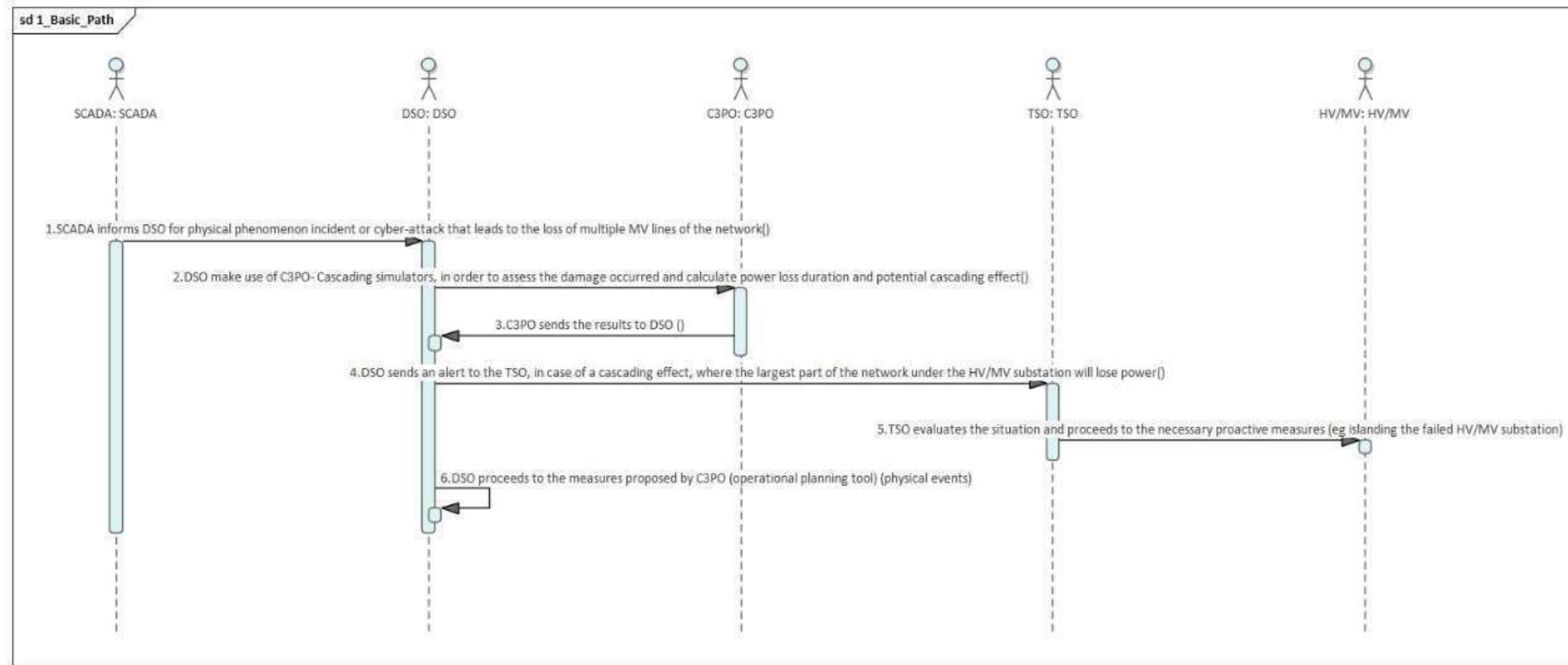


Figure 28 - UC23 Basic Path



UC24 - Cyber Security Risk assessment on EPES infrastructure

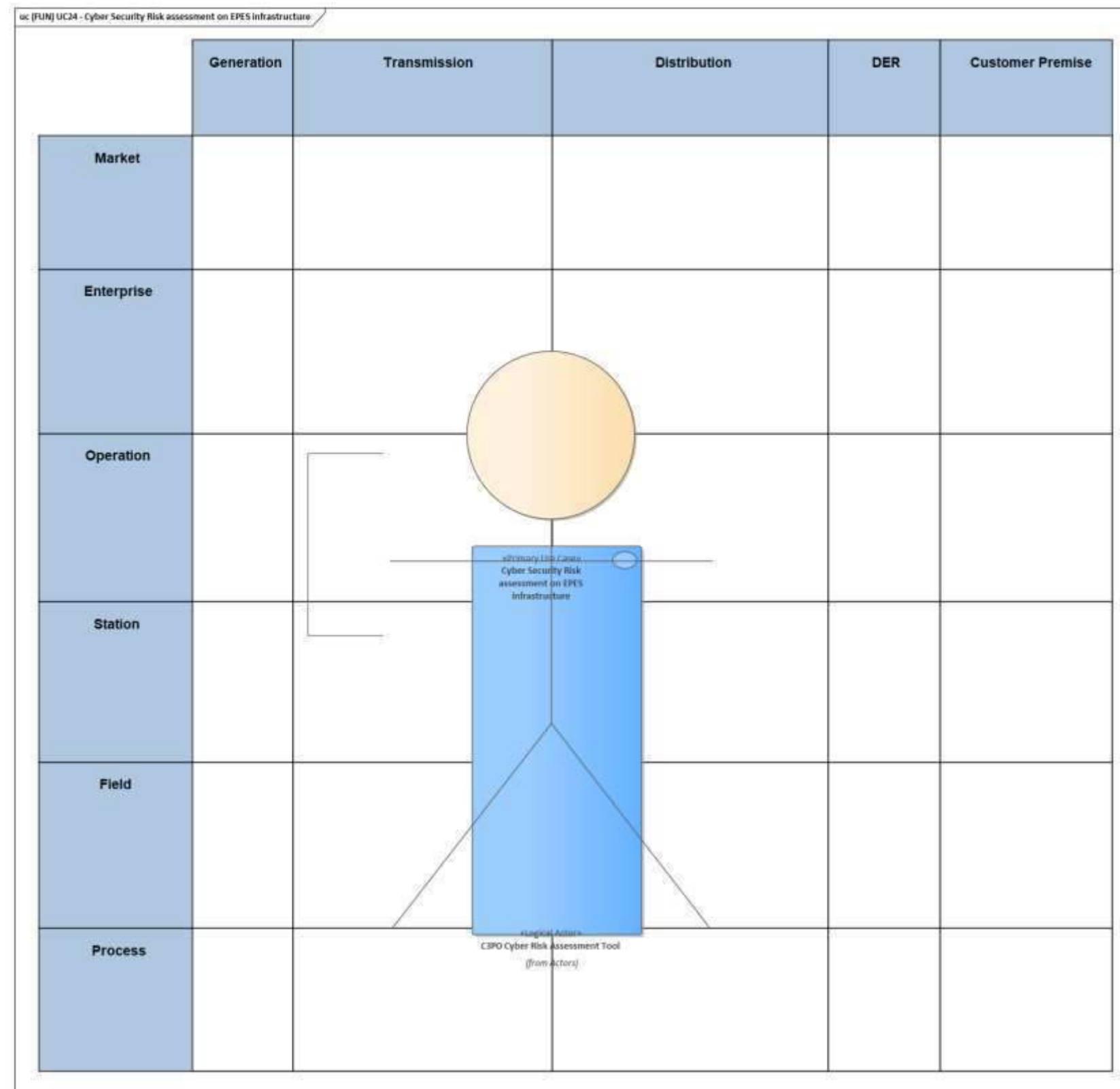


Figure 29 - UC24 Functional Layer

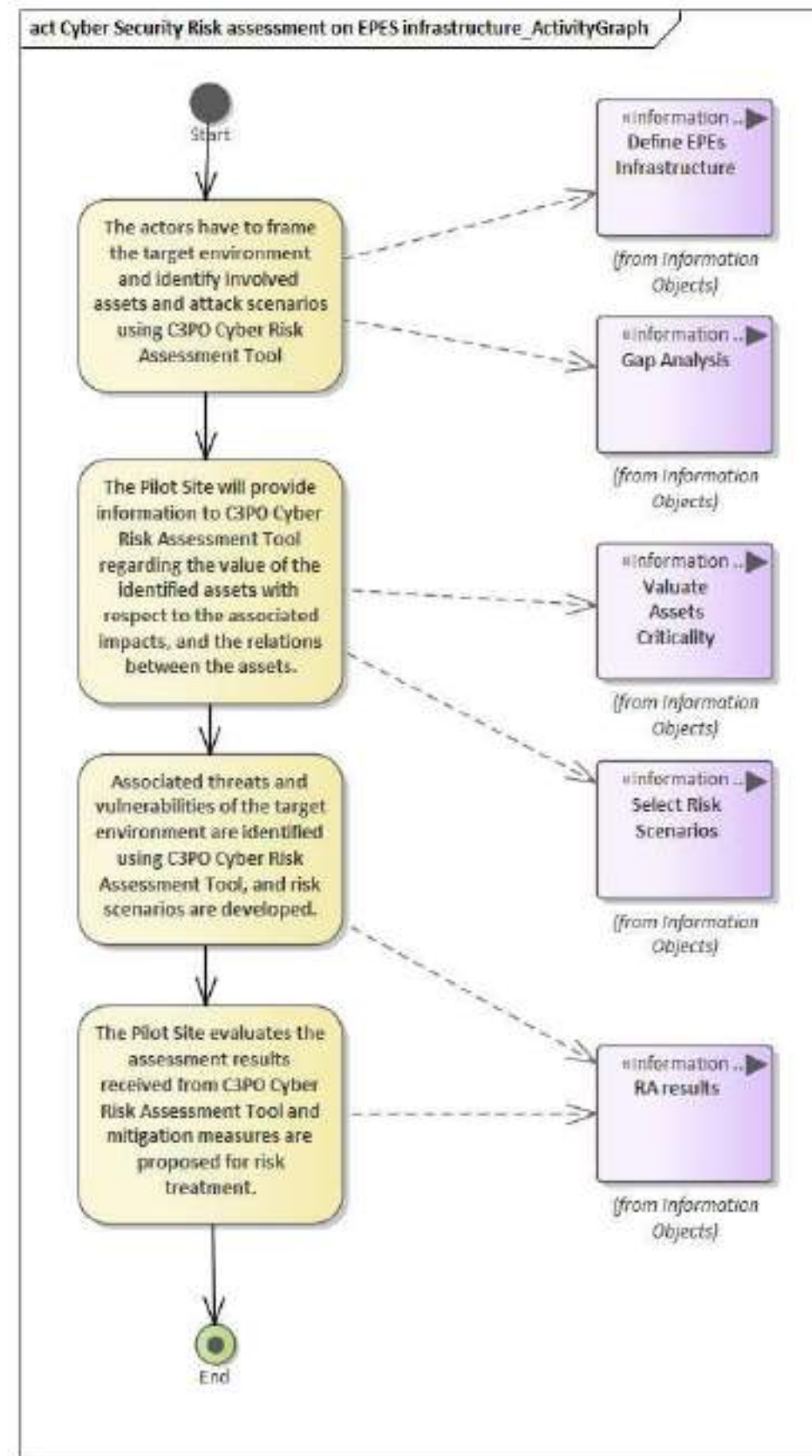


Figure 30 - UC24 Activity Graph

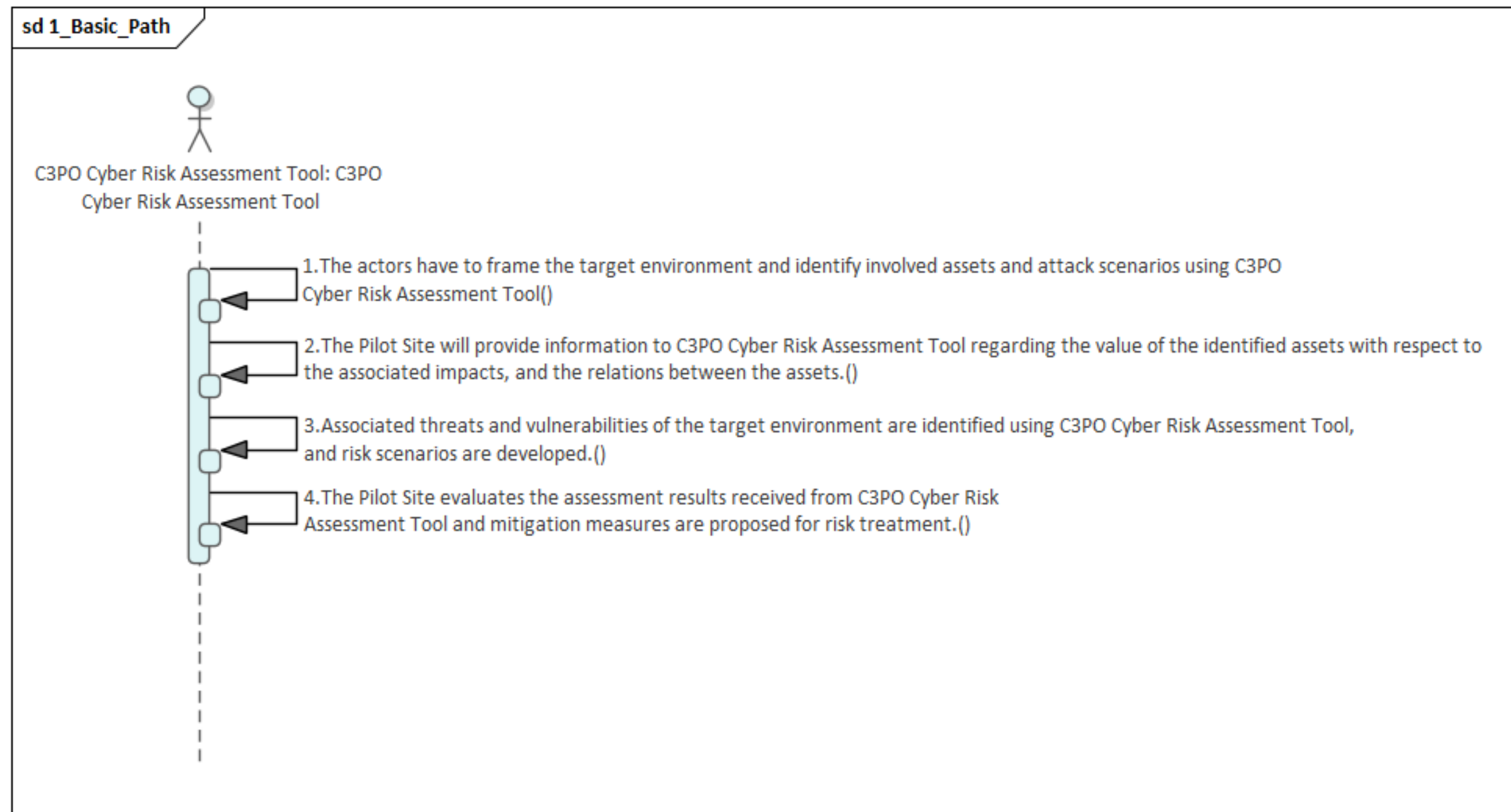


Figure 31 - UC24 Basic Path



UC25 - Dynamic Cyber-Risk Status Evaluation considering existing technical vulnerabilities

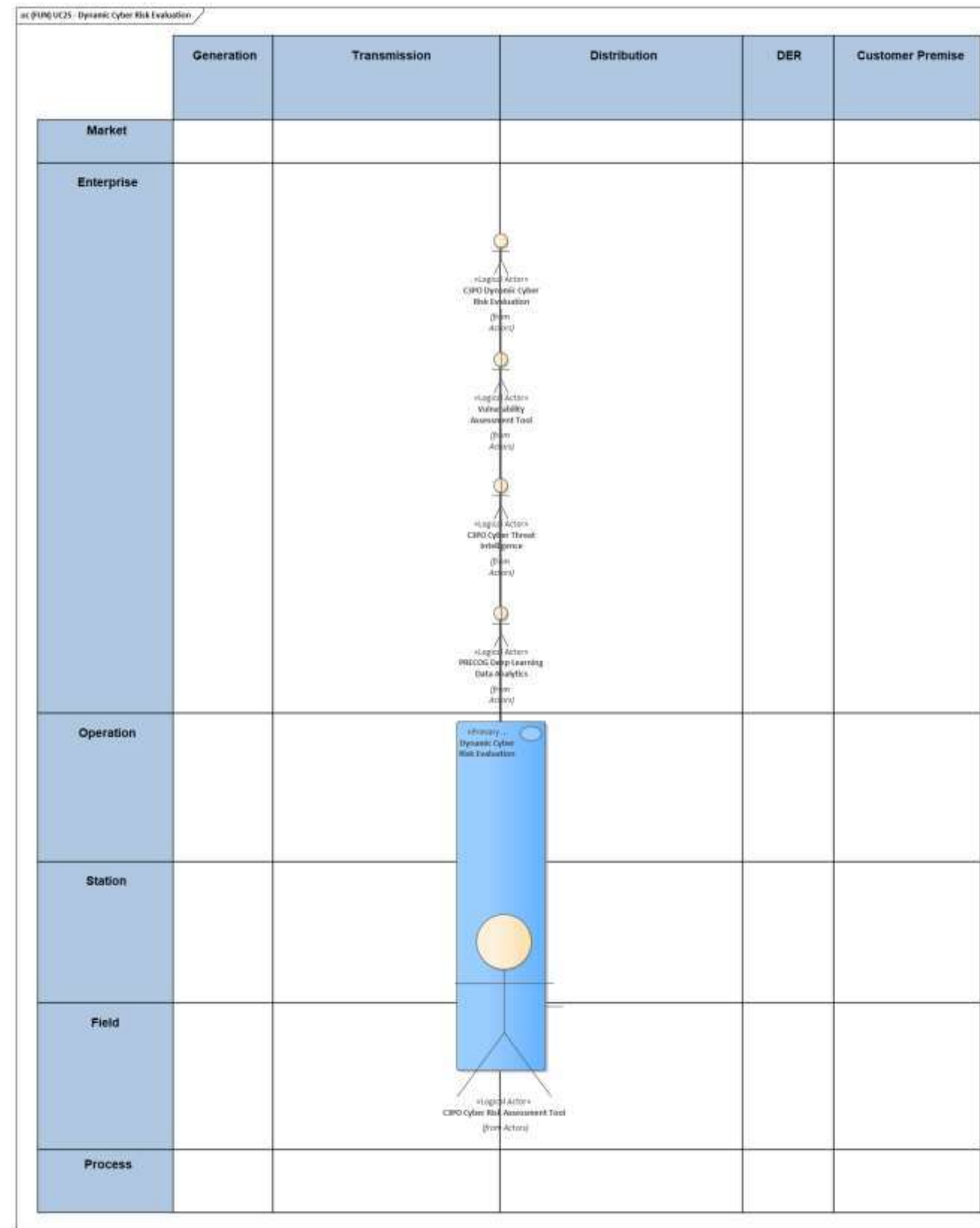


Figure 32 - UC25 Functional Layer

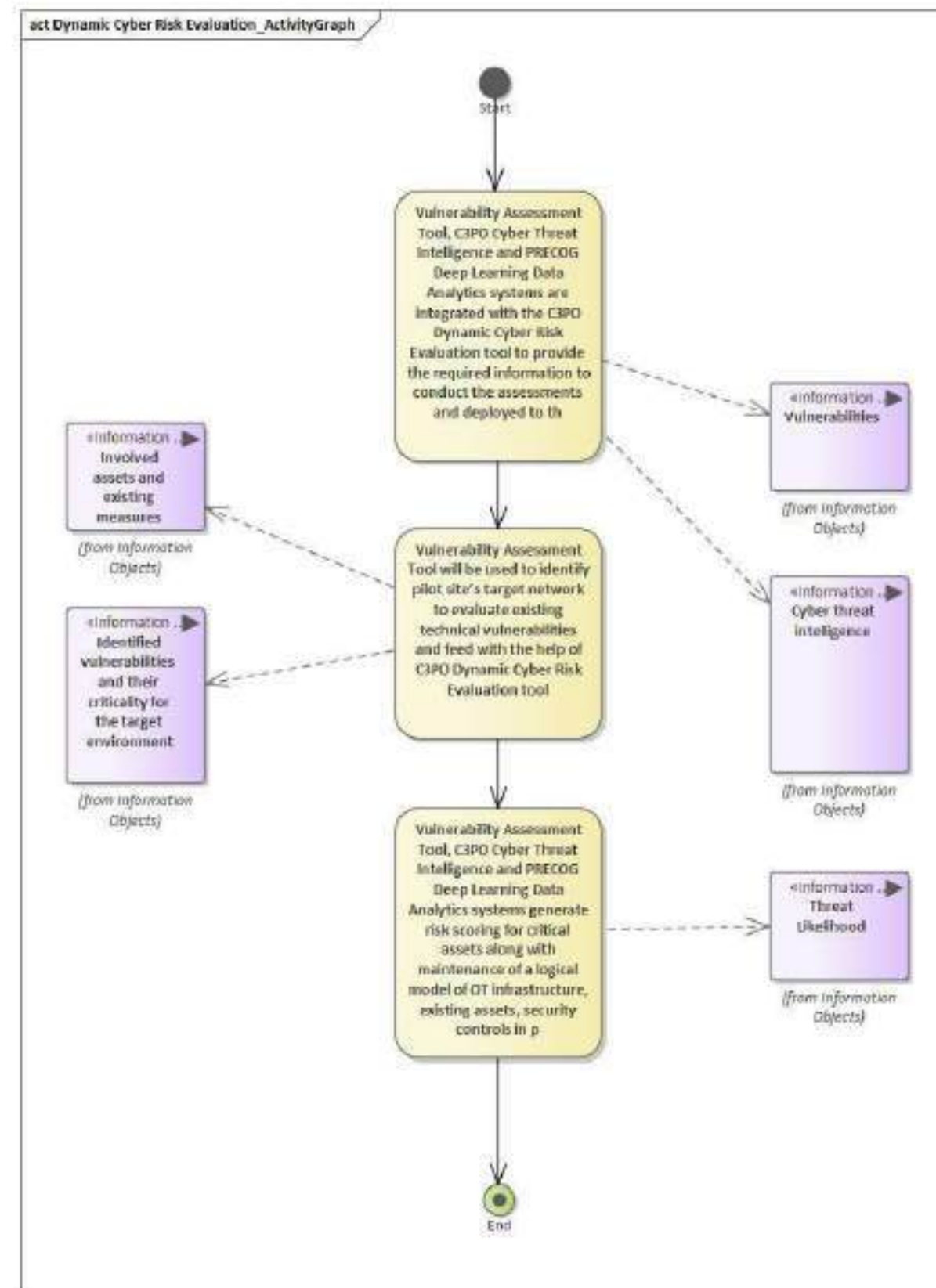


Figure 33 - UC25 Activity Graph

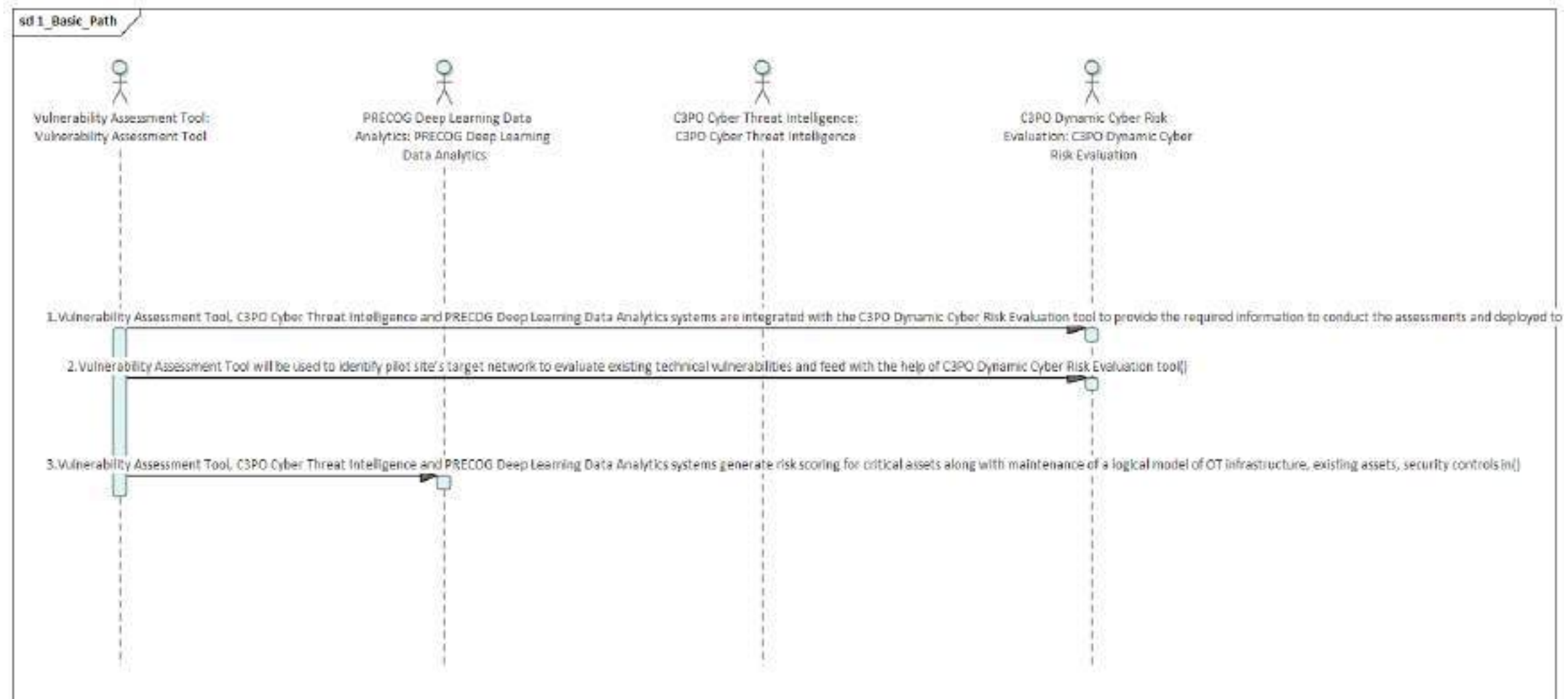


Figure 34 - UC25 Basic Path



UC26 - Cyber Threat Intelligence knowledge collection/sharing with external sources

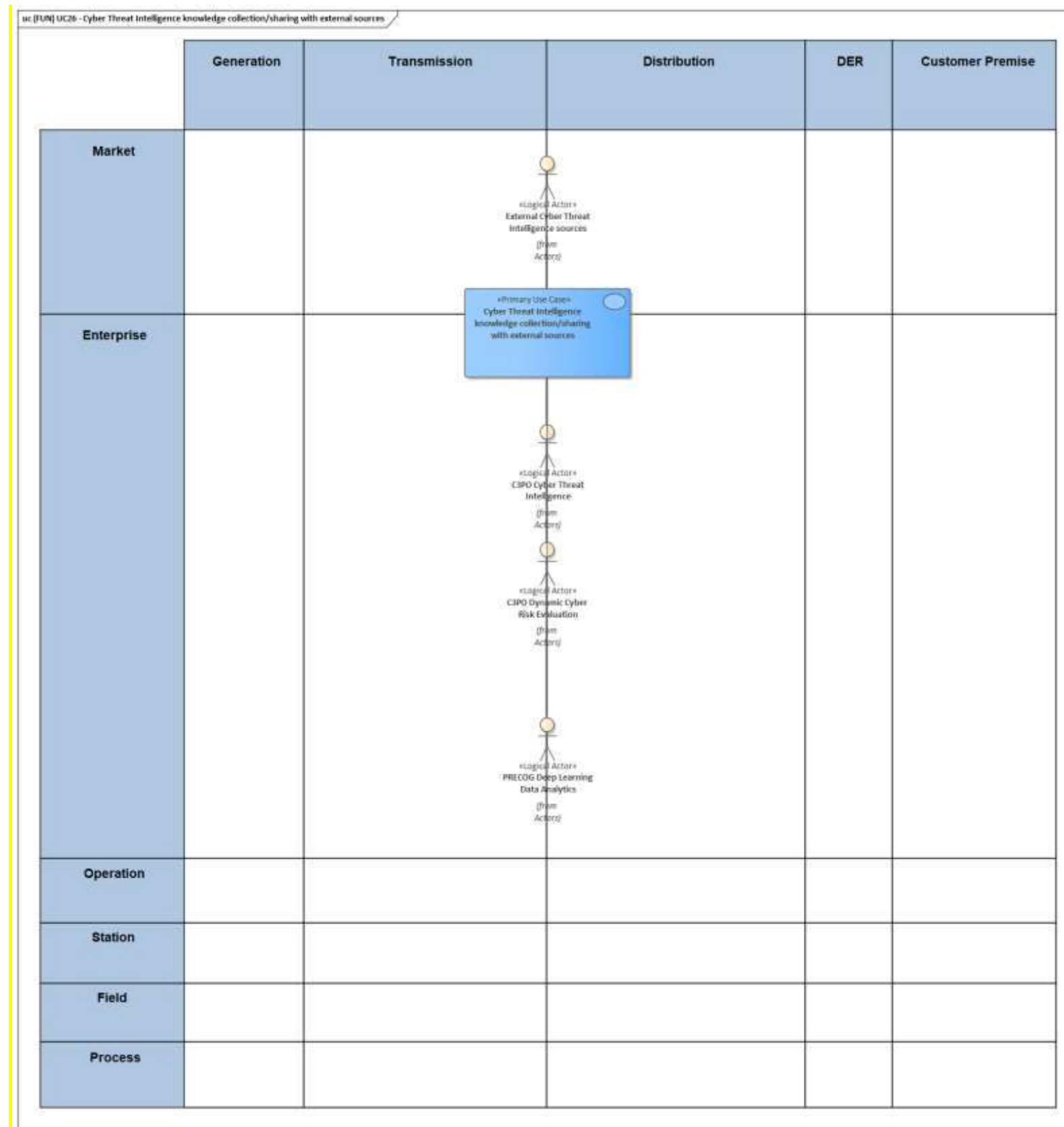


Figure 35 - UC26 Functional Layer

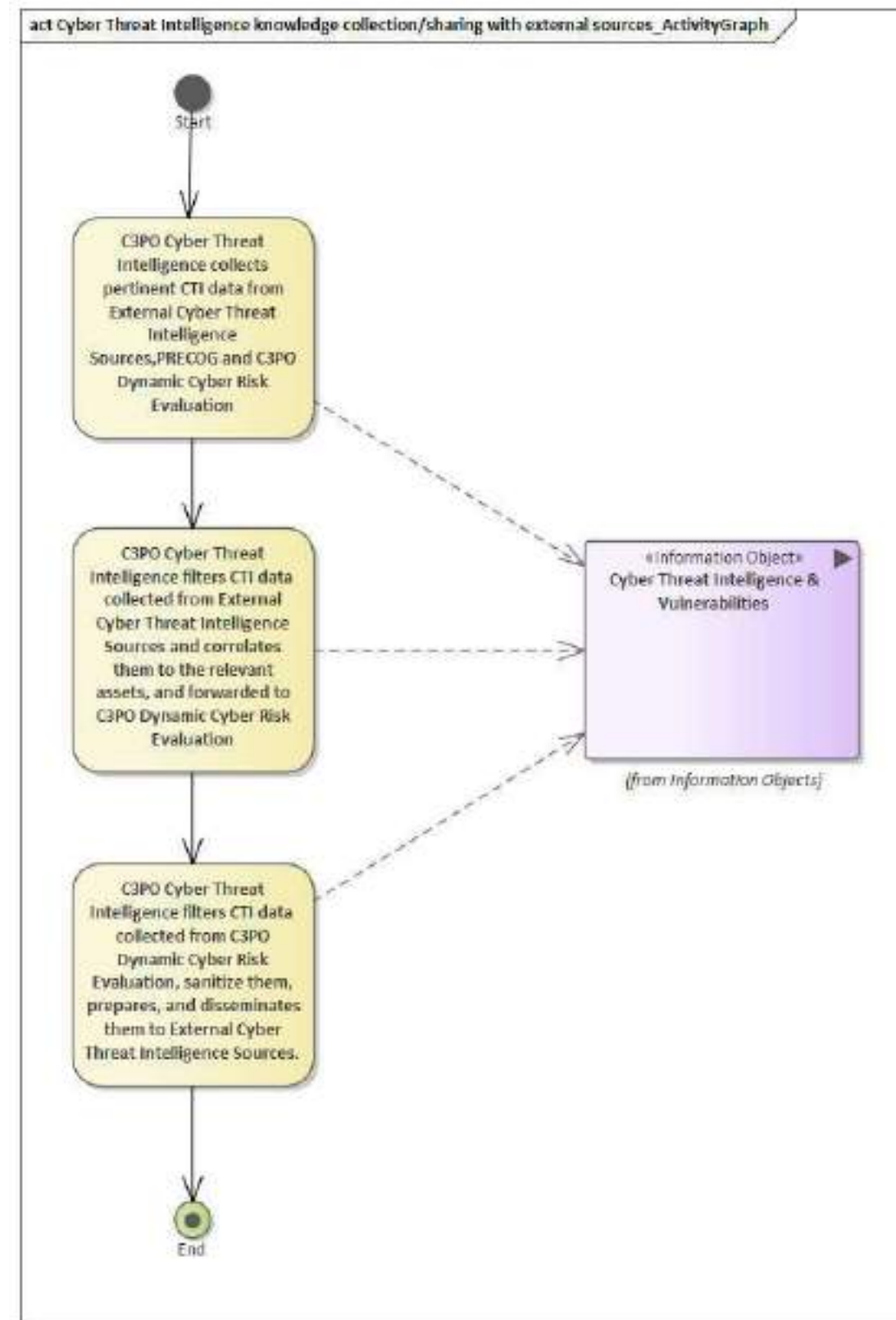


Figure 36 - UC26 Activity Graph

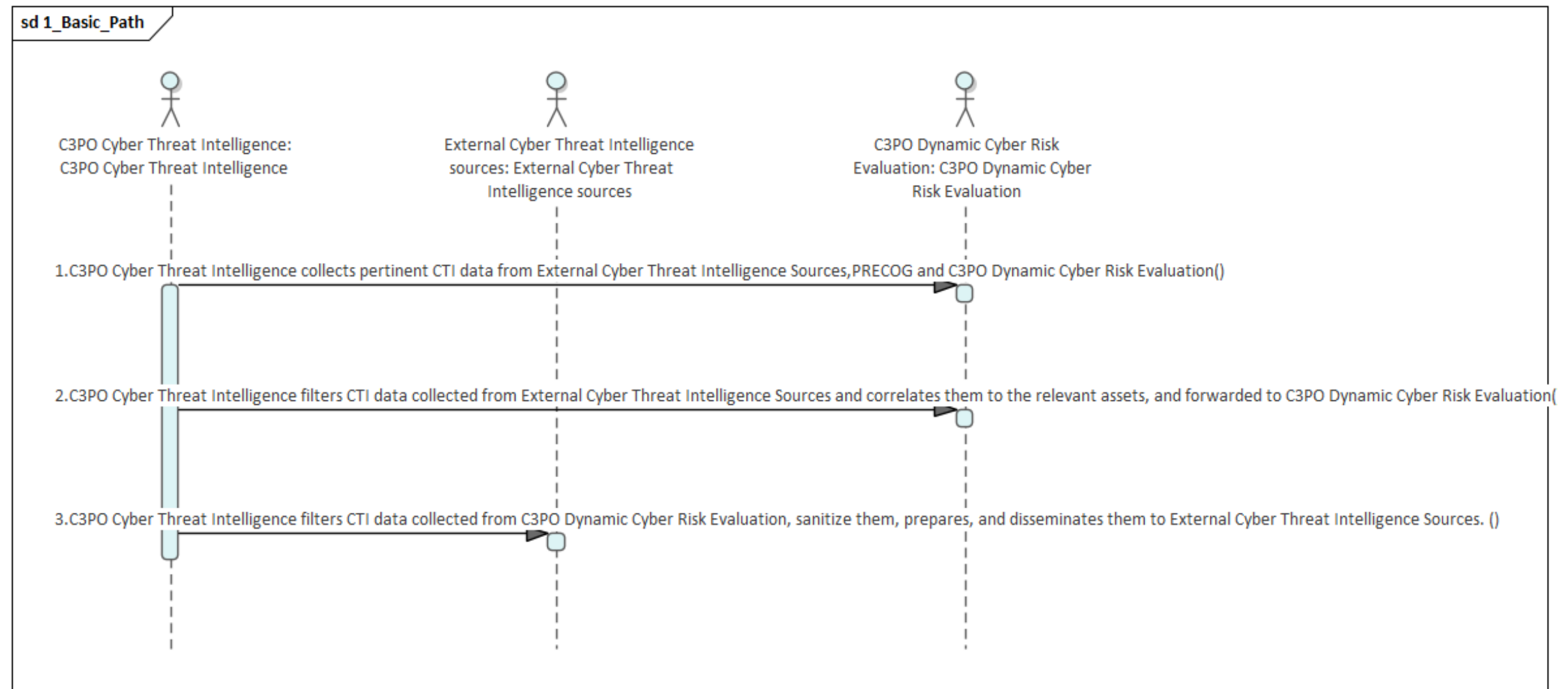


Figure 37 - UC26 Basic Path

UC29 - Event simulator of a progressing wildfire and assessment of its impact on distribution system

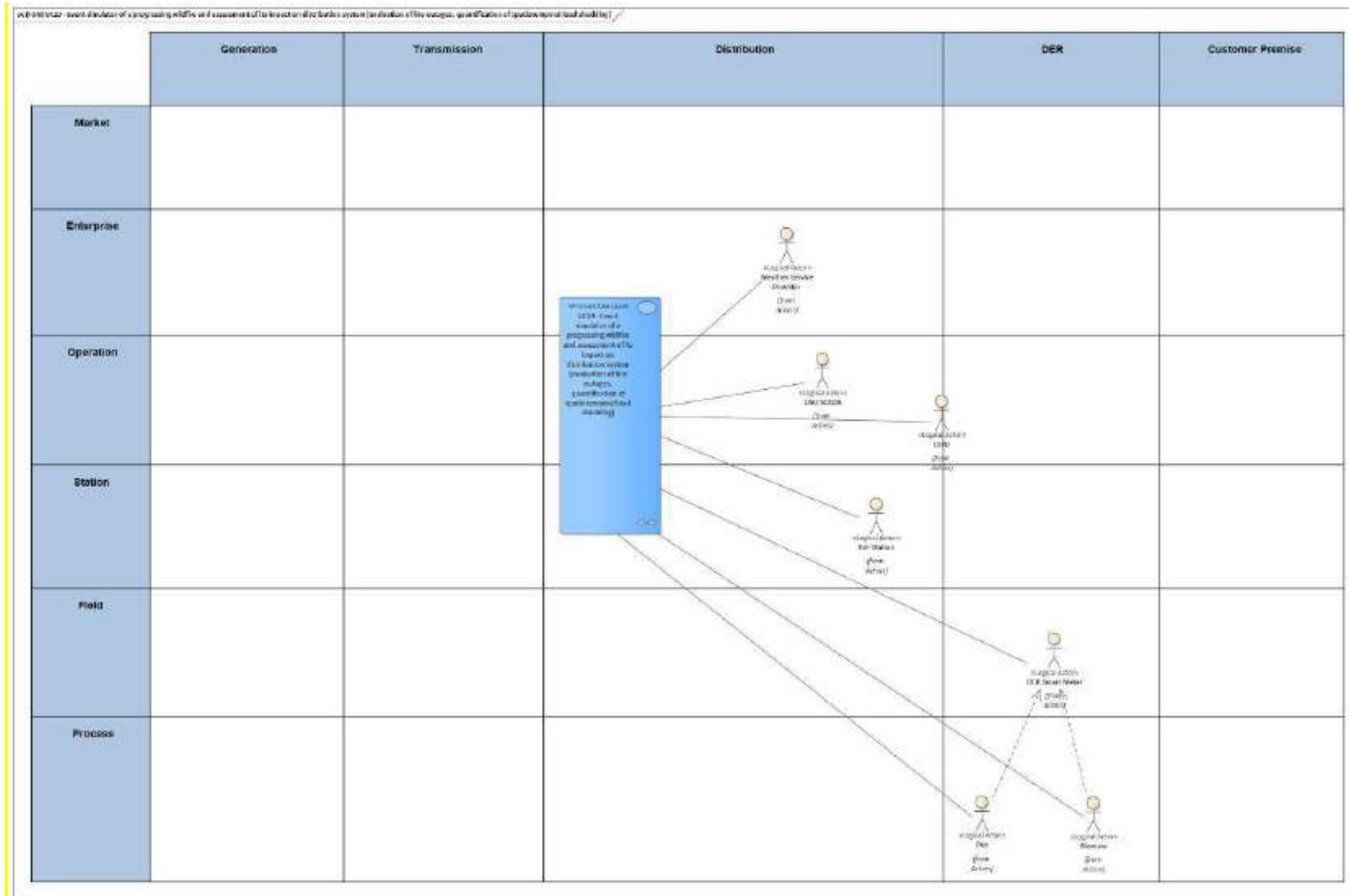


Figure 38 - UC29 Functional Layer

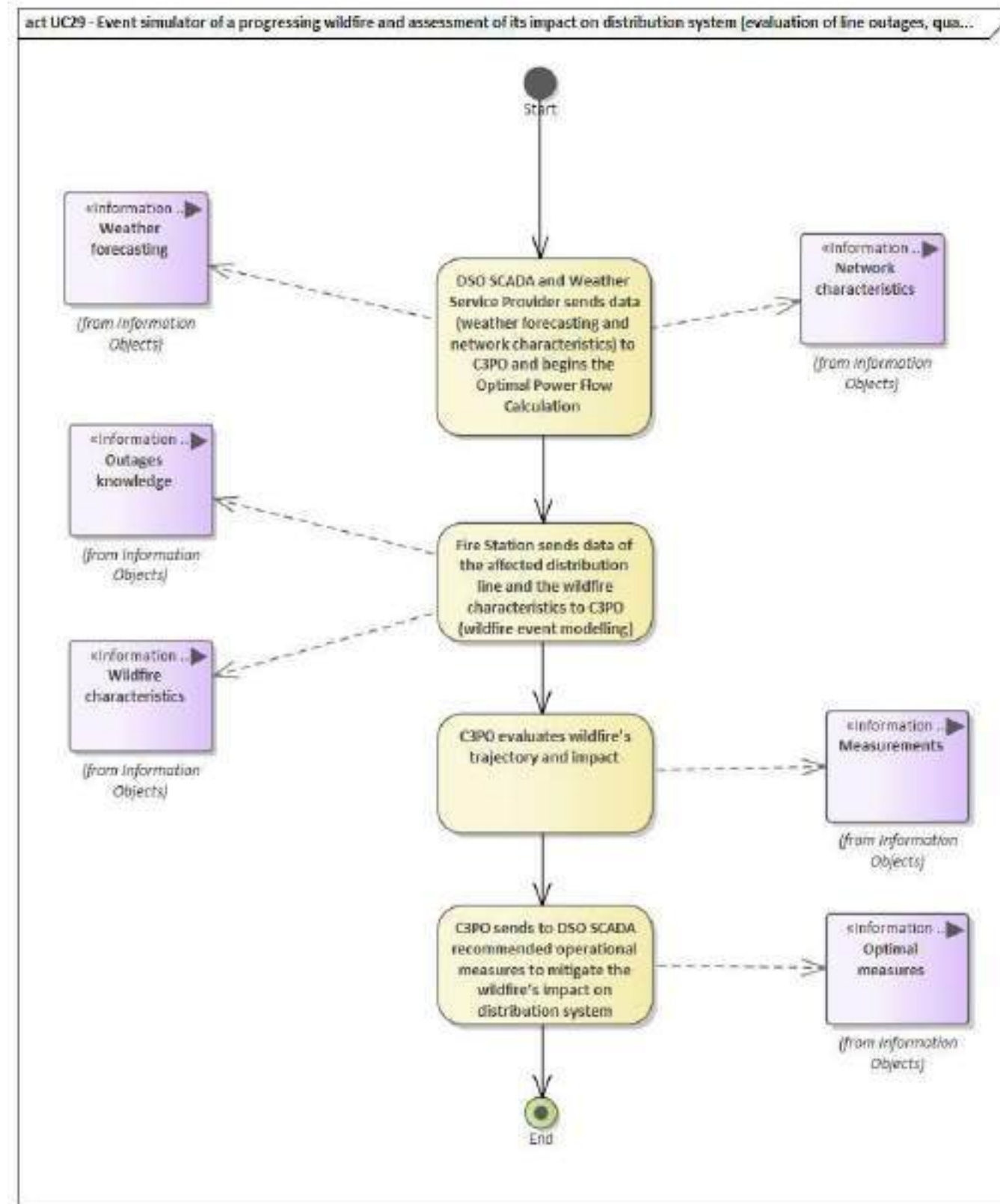


Figure 39 - UC29 Activity Graph

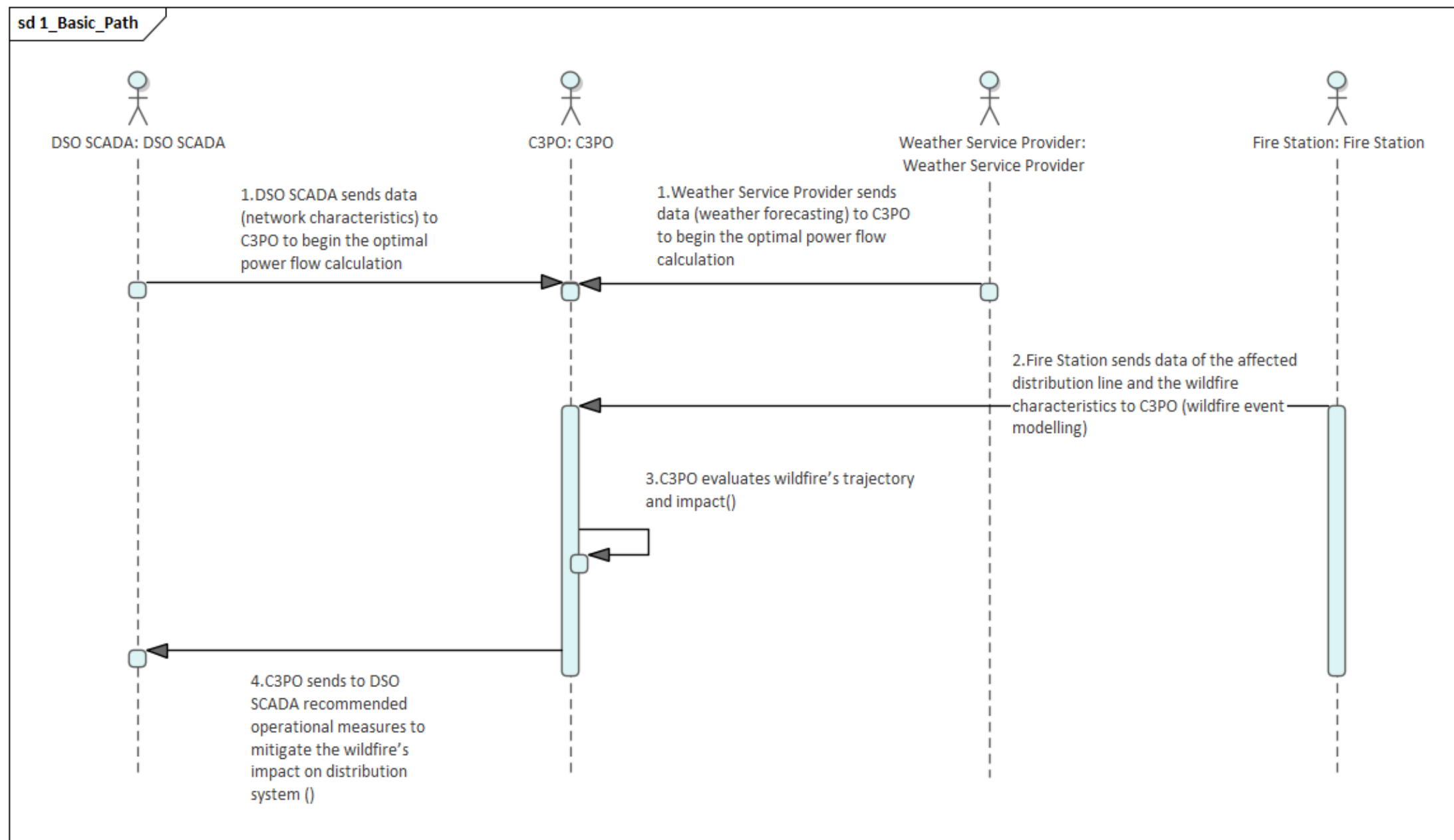


Figure 40 - UC29 Basic Path

UC30 - Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling

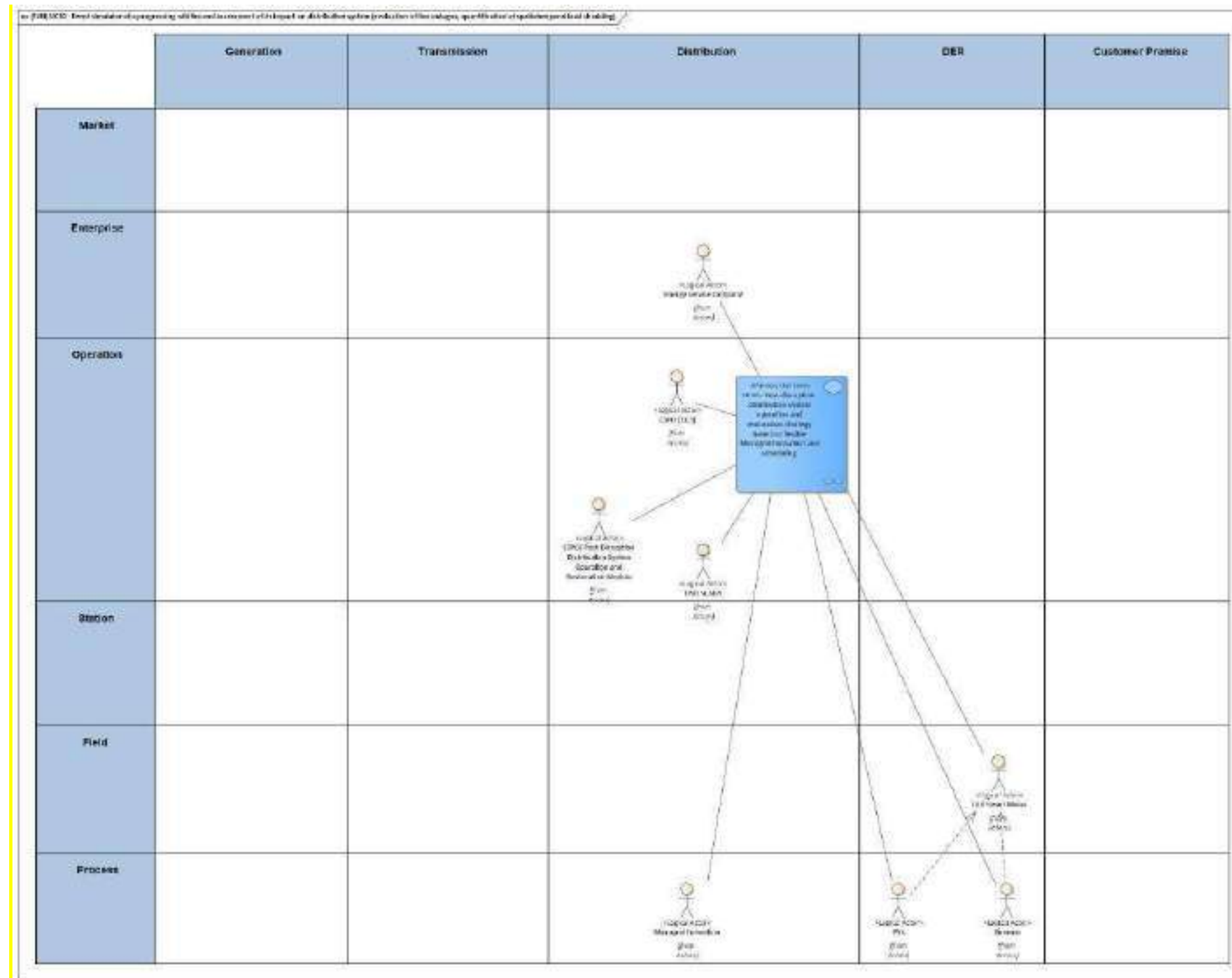


Figure 41 - UC30 Functional Layer

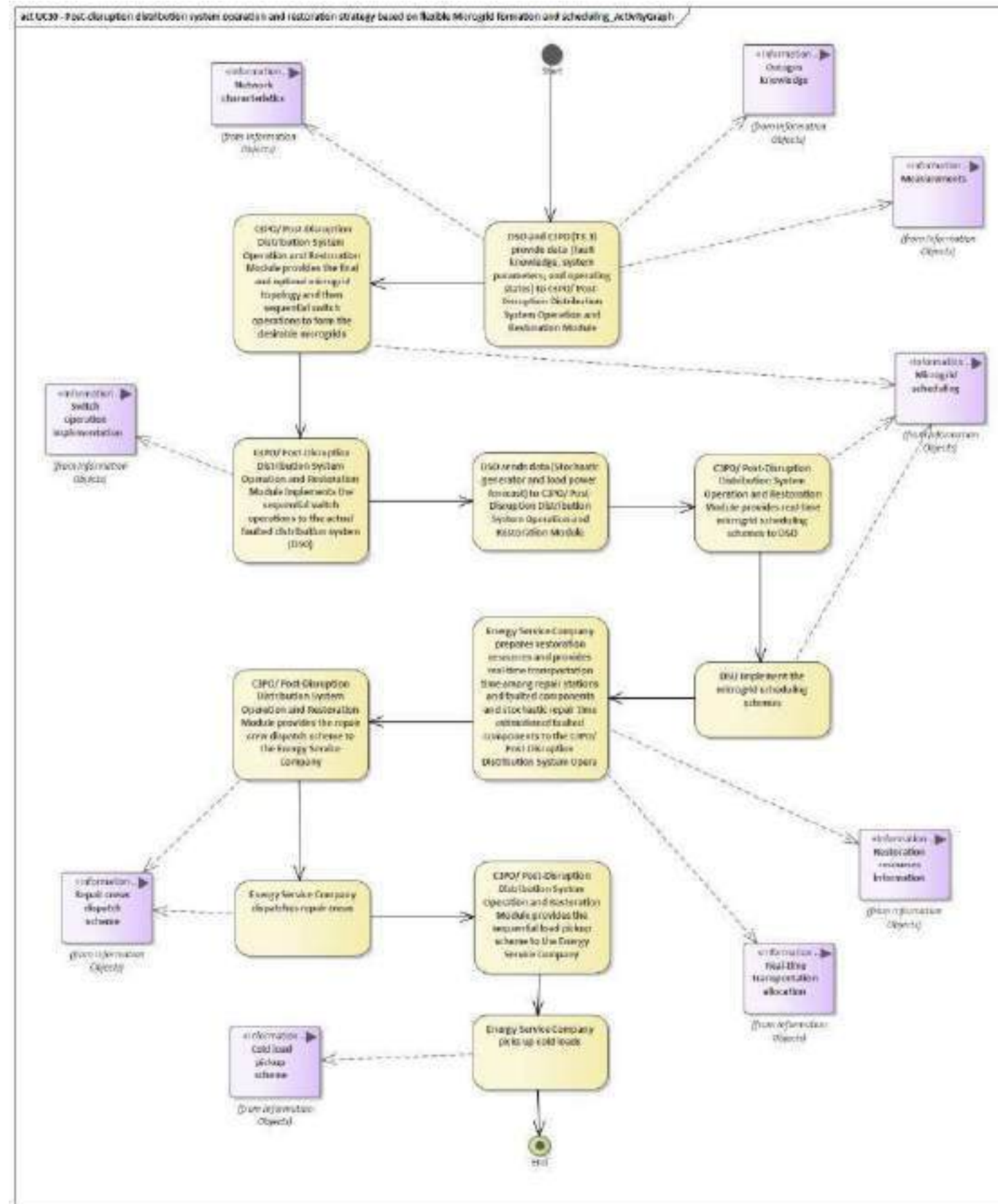


Figure 42 - UC30 Activity Graph

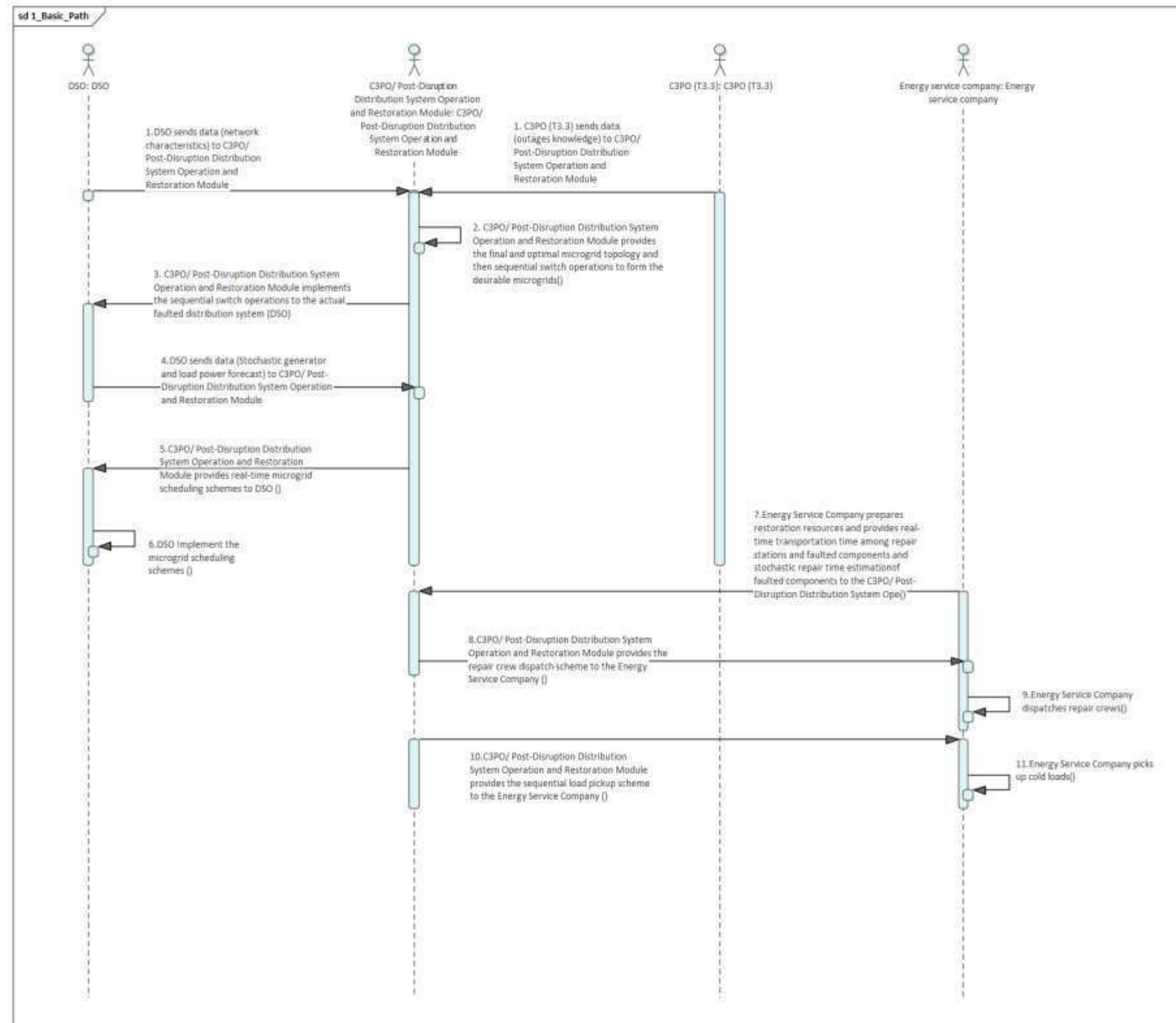


Figure 43 - UC30 Basic Path

UC32 - Planning and operation for a resilient multi-energy microgrid

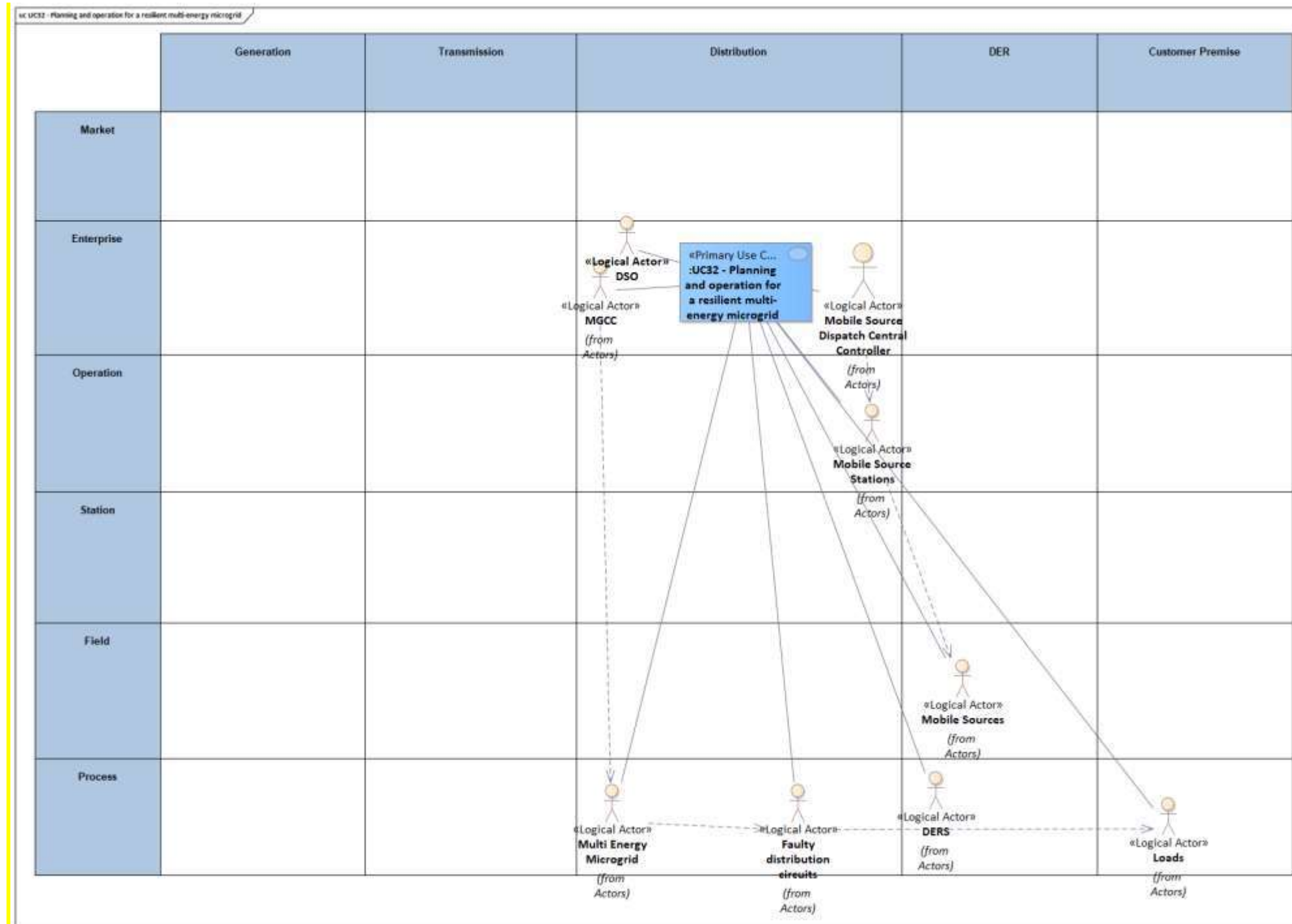


Figure 44 - UC32 Functional Layer

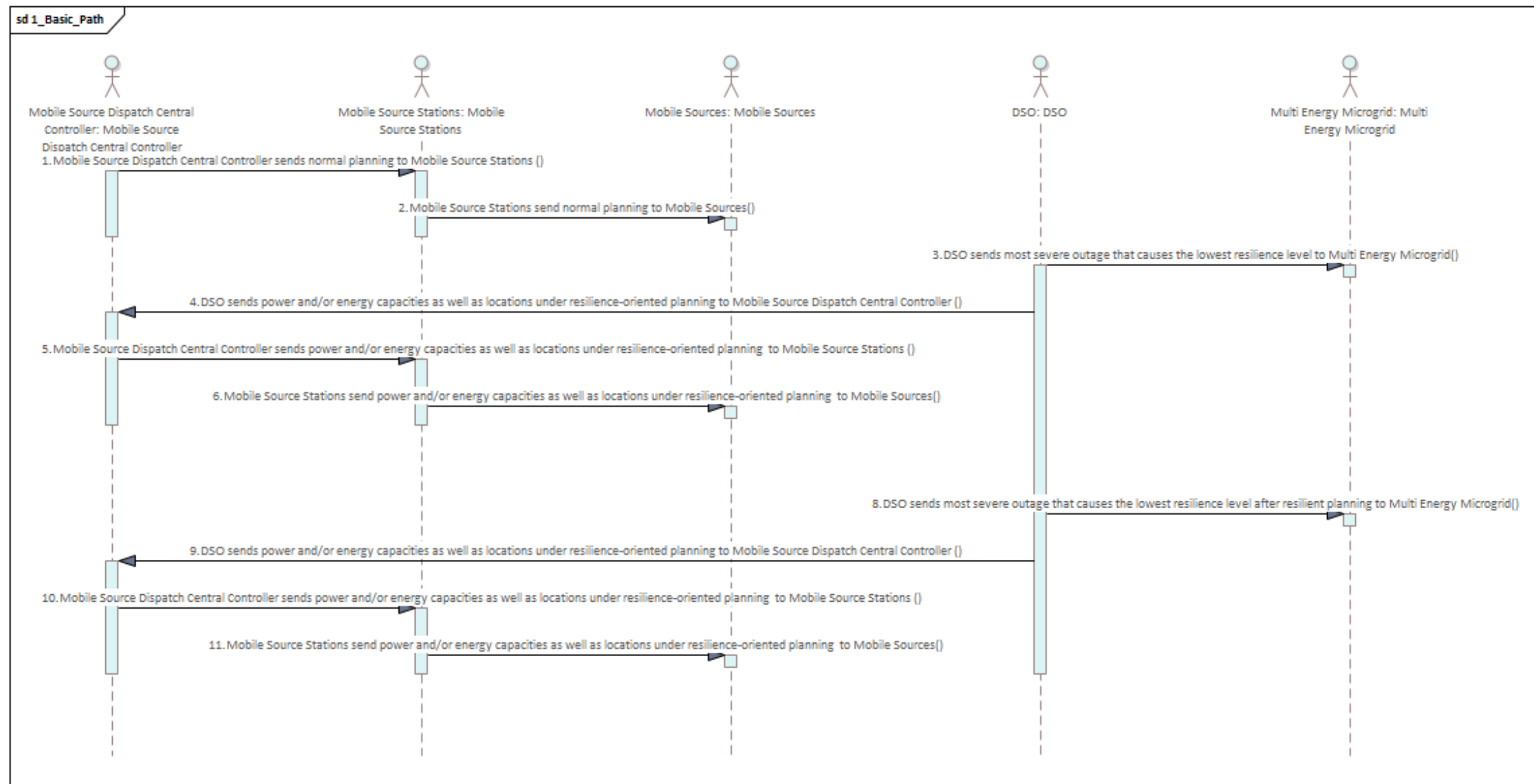


Figure 46 – UC32 Basic Path

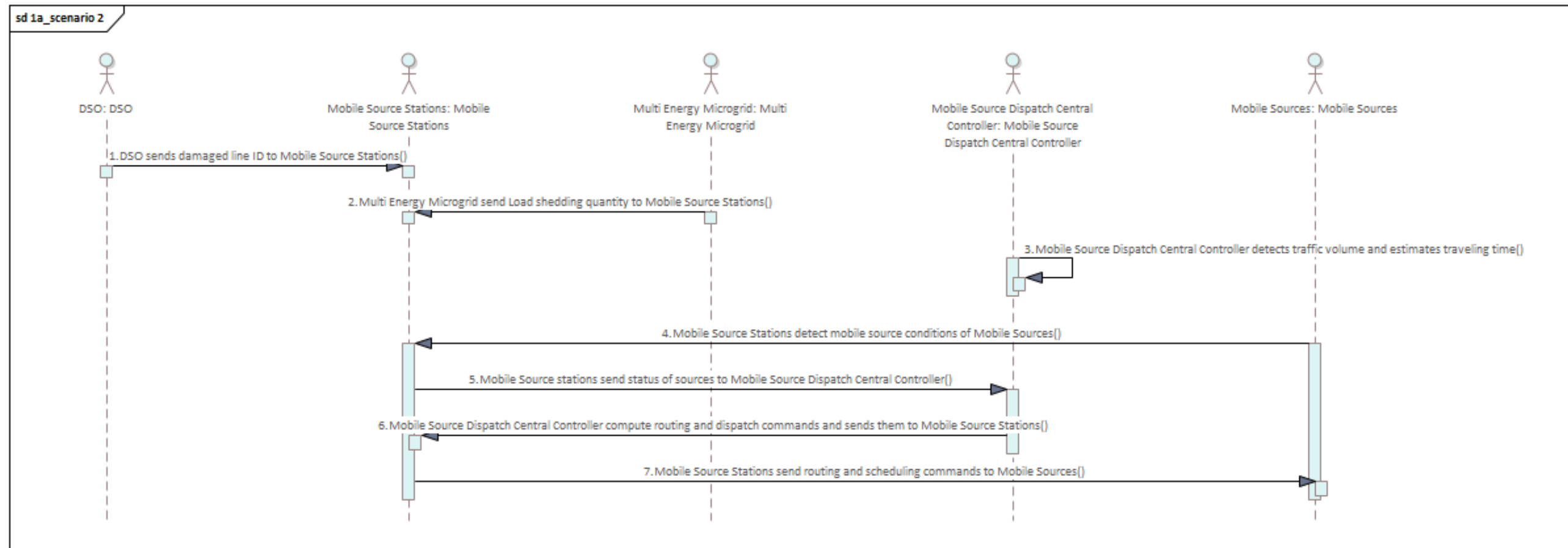


Figure 47 - UC32 Alternative Path

UC39 - OPDE Risk Register

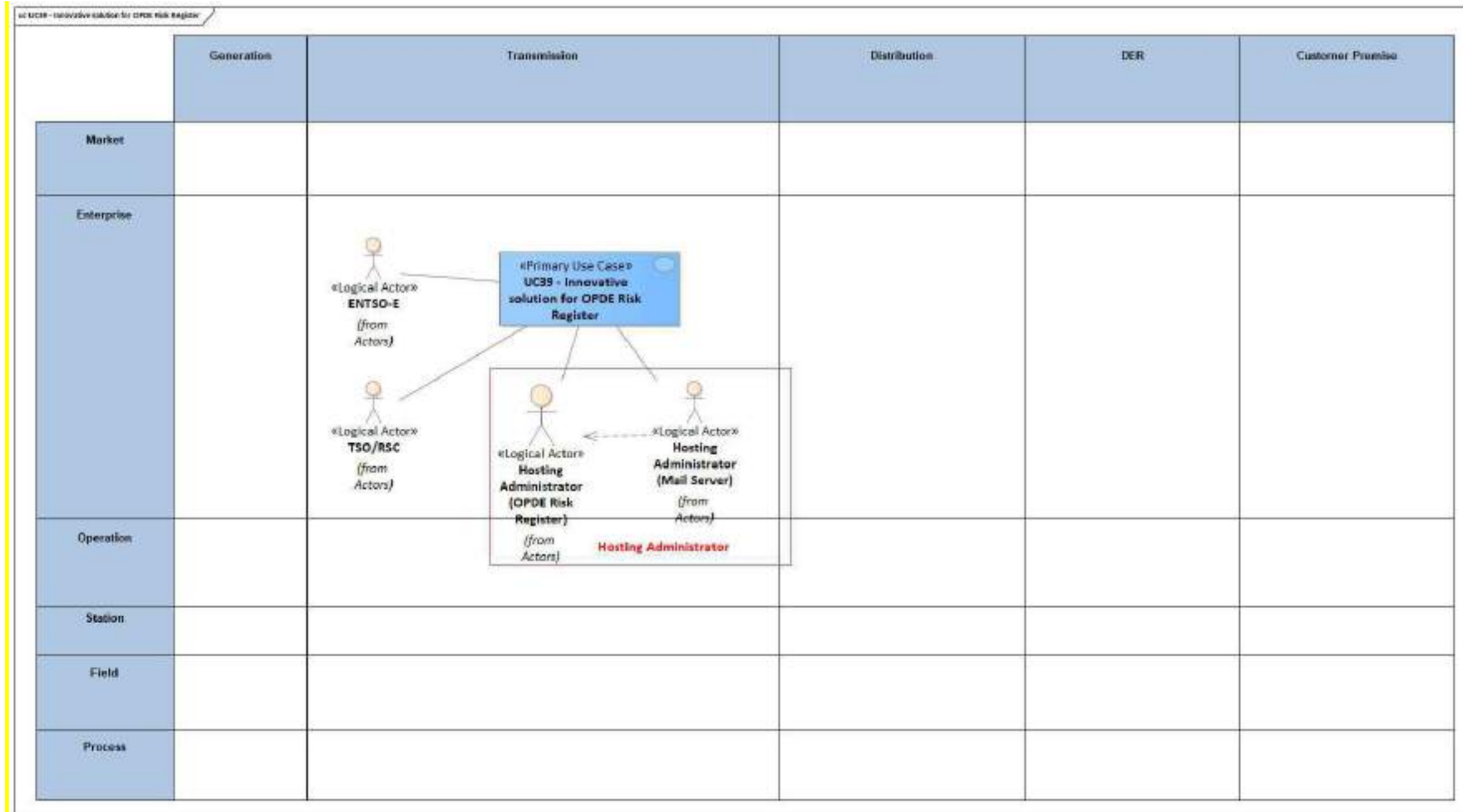


Figure 48 - UC39 Functional layer

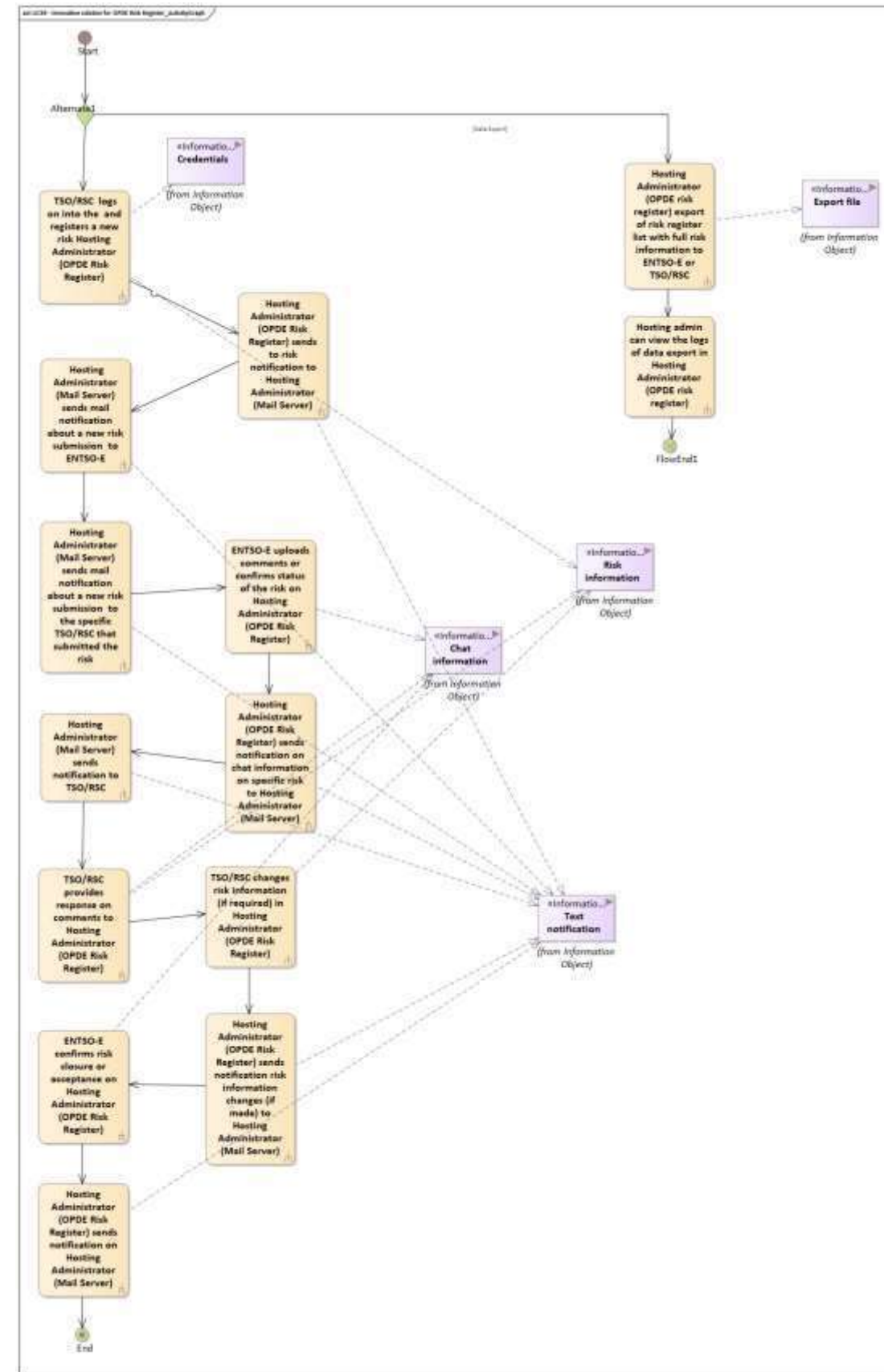


Figure 49 - UC39 Activity Graph

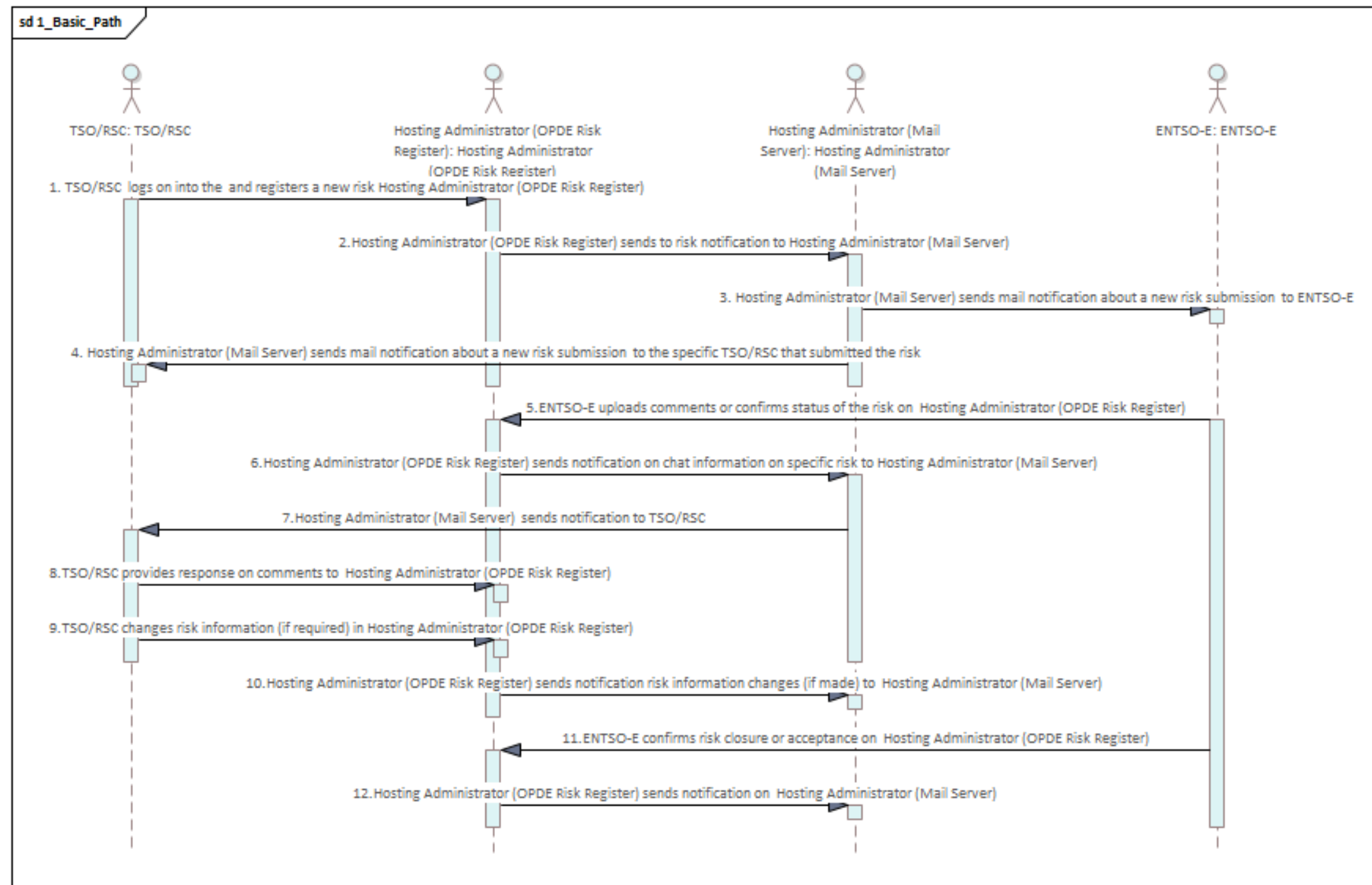


Figure 50 - UC39 Basic Path

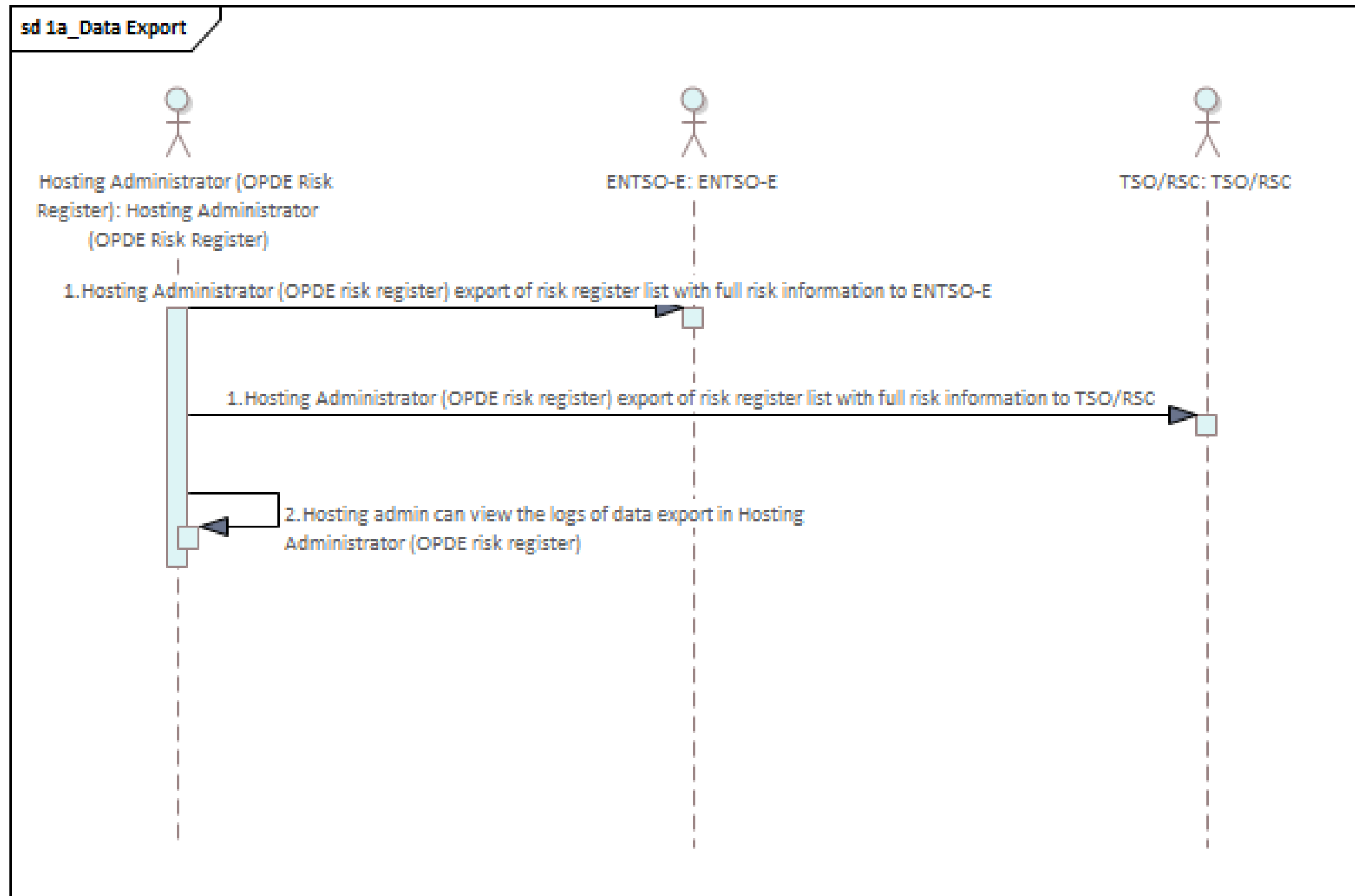


Figure 51 - UC39 Alternative Path

13.1.2 WP4-IRIS

UC07 - Enhancement in DER control and management systems to participate in flexibility procurement schemes for DSO and TSO to improve network operation security

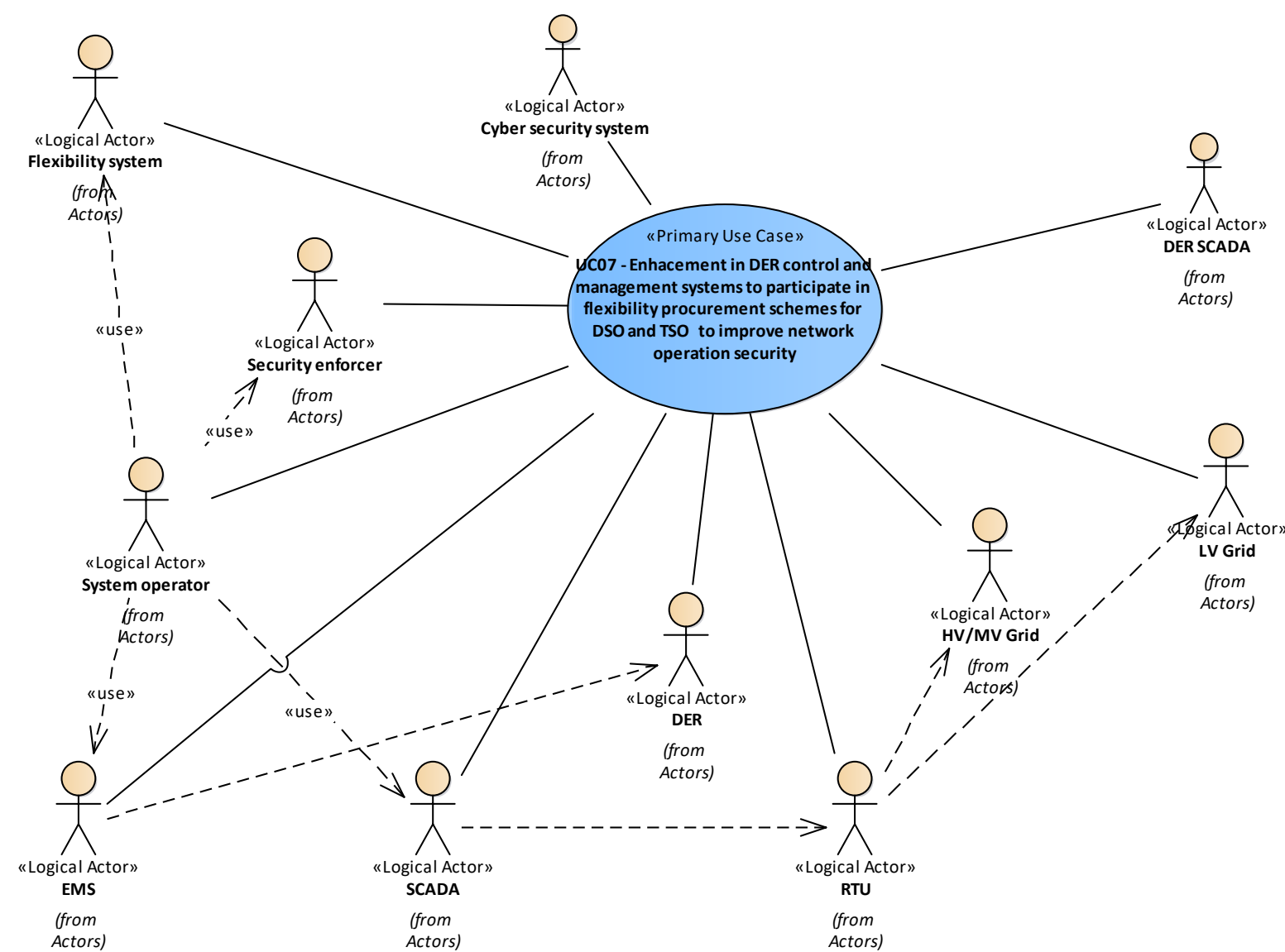


Figure 52 - UC07 Actors Involved

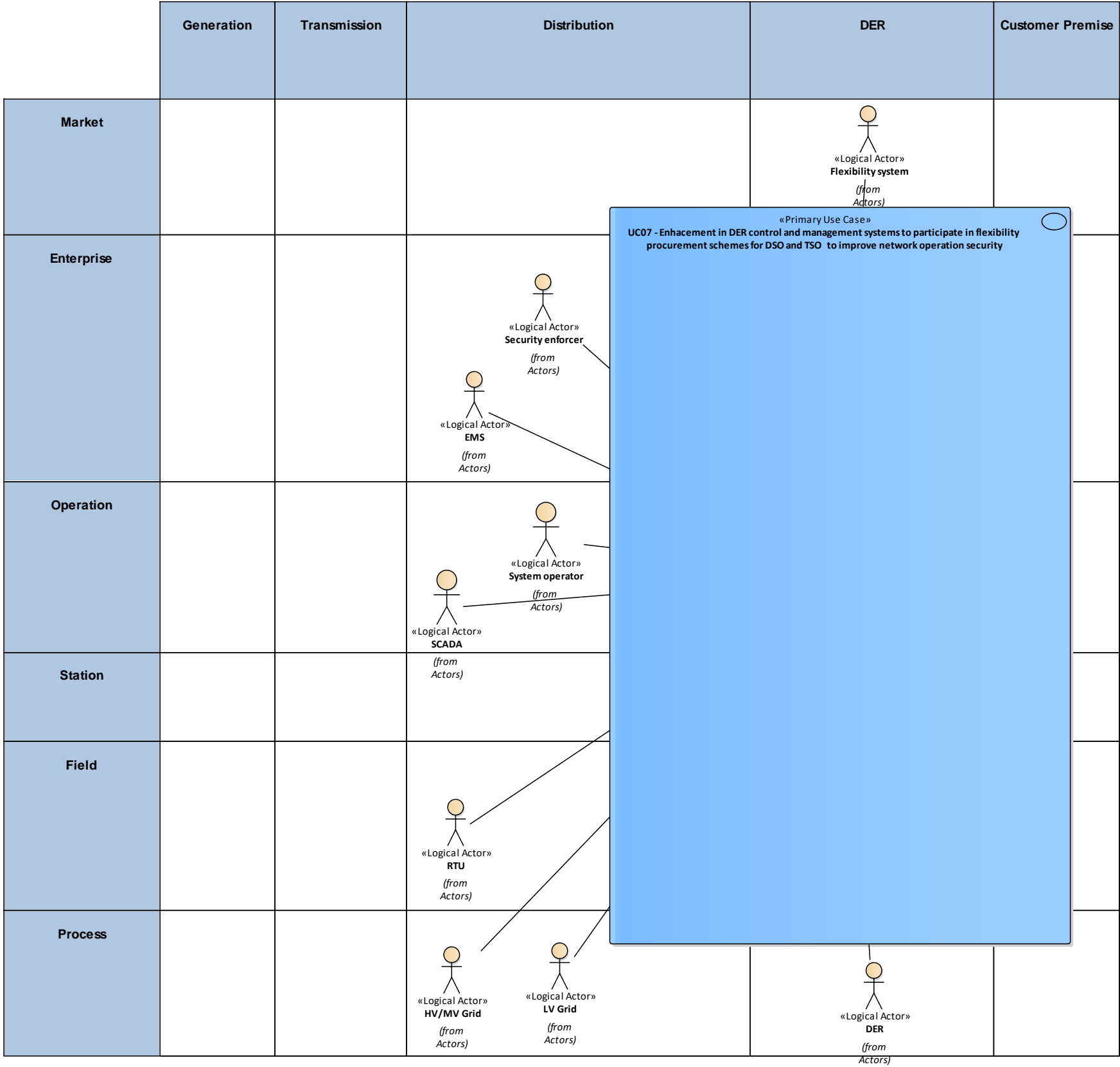


Figure 53 - UC07 Functional Layer

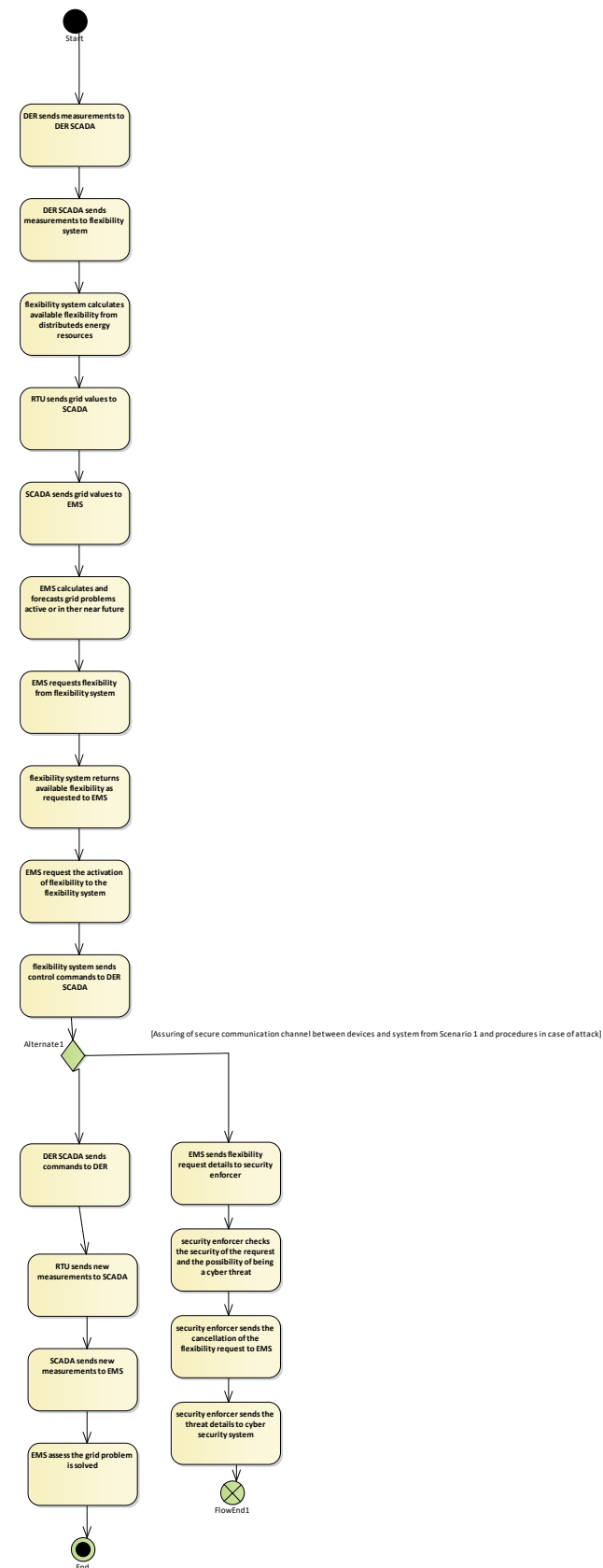


Figure 54 – UC07 Activity Graph

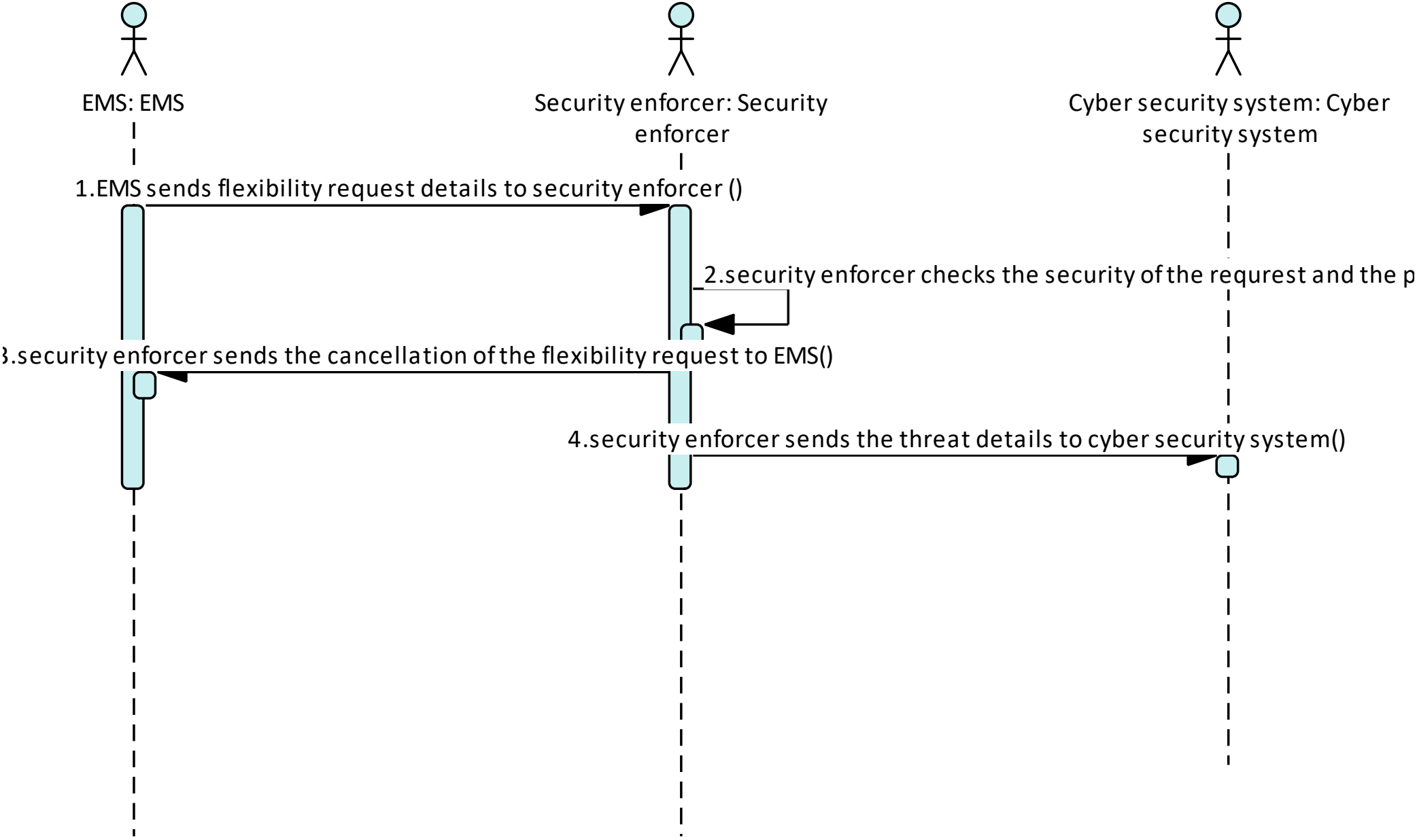


Figure 55 - UC07 Scenario 1

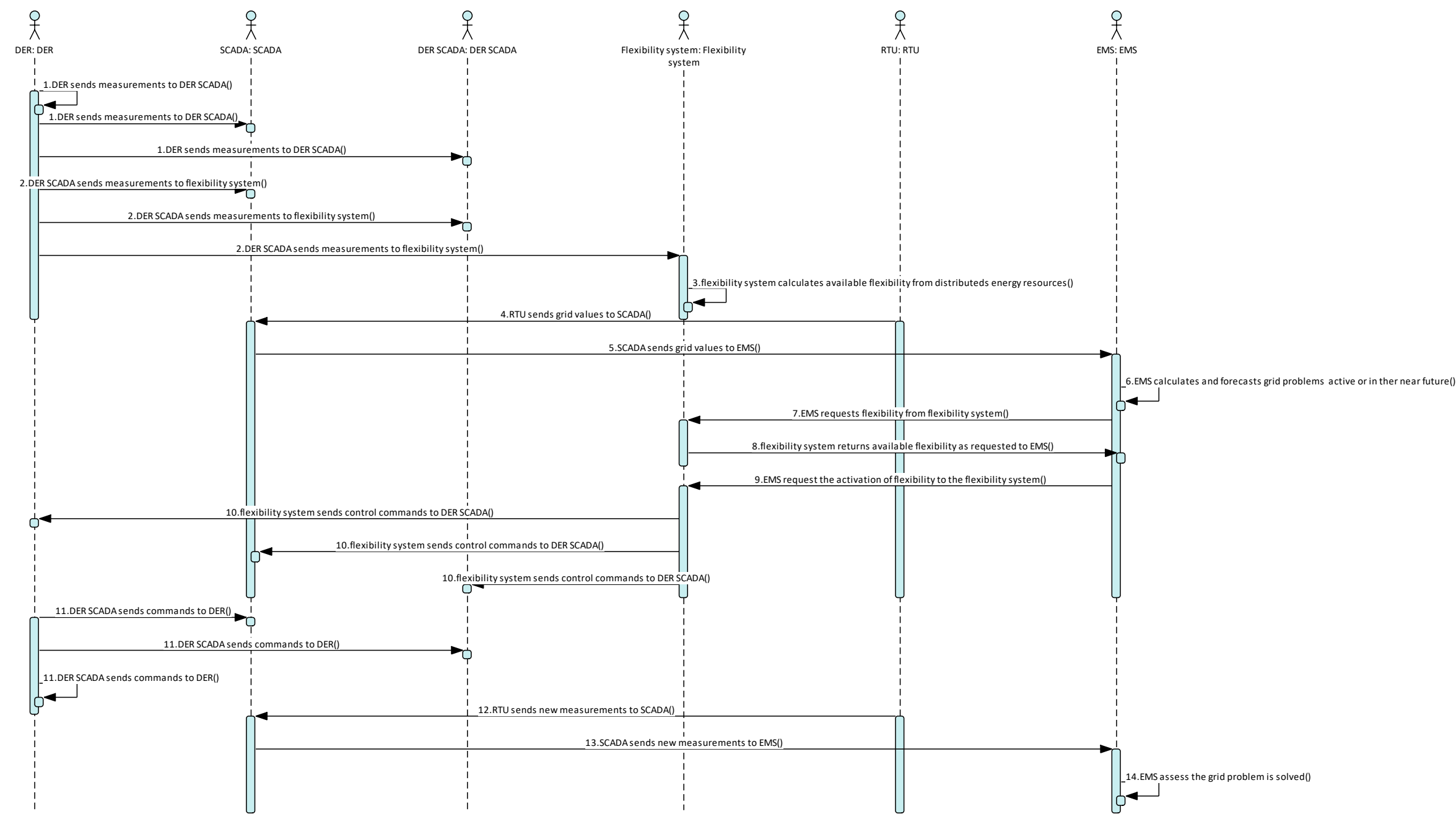


Figure 56 - UC07 Basic Path

UC10 - Improving of LV network observability based on billing metering system by means of secure interface with SCADA-ADMS system

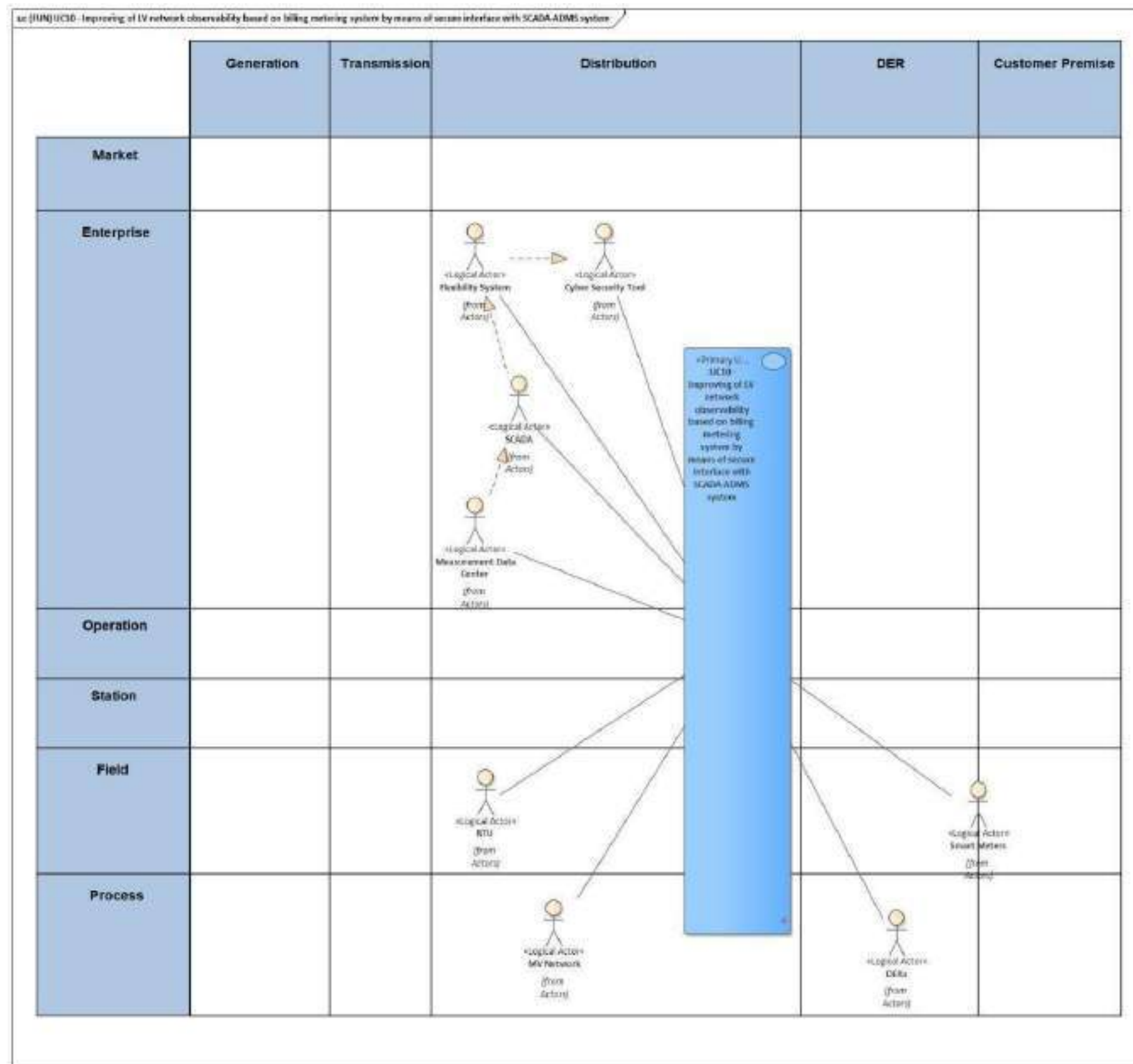


Figure 57 - UC10 Functional Layer

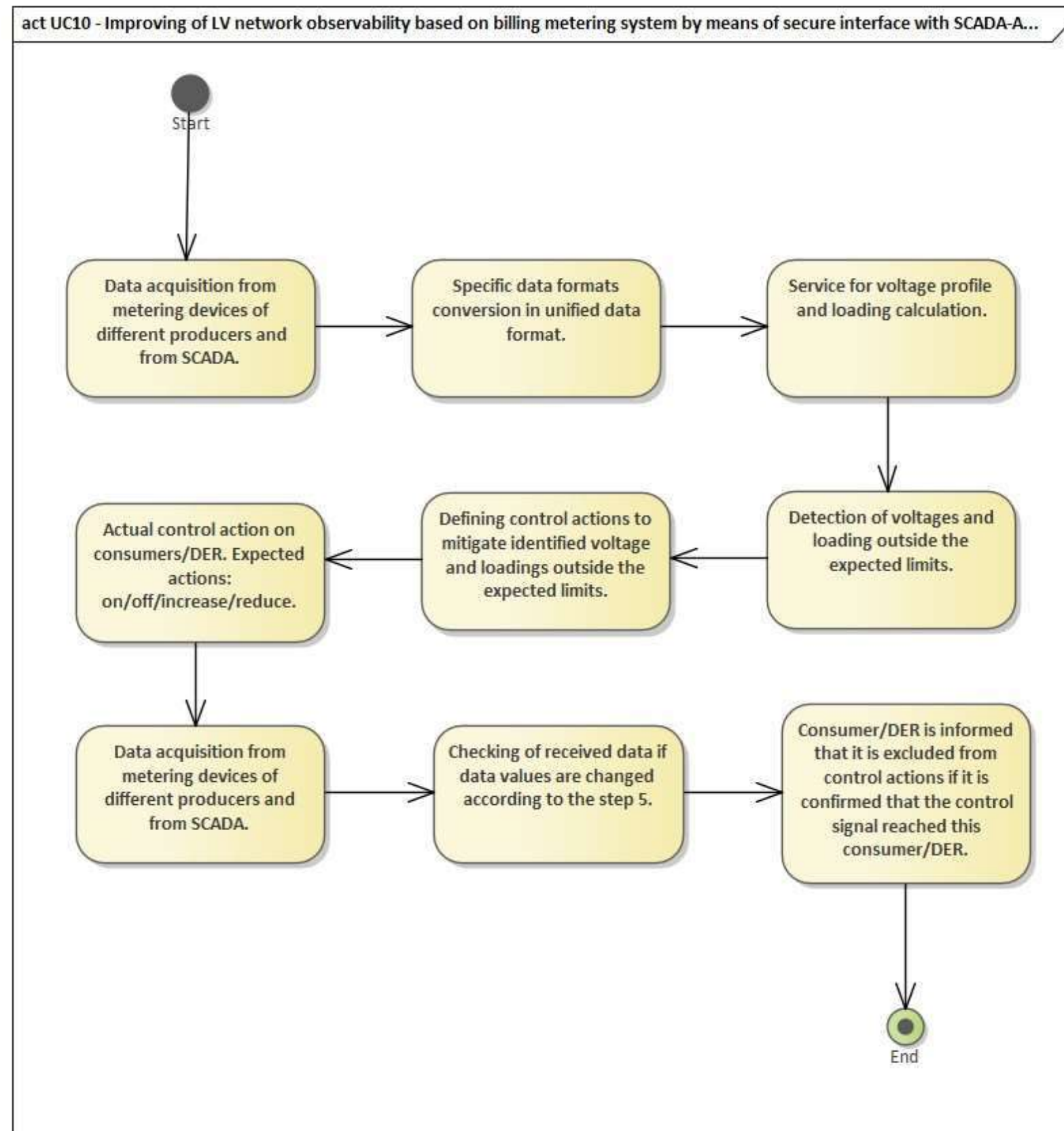


Figure 58 - UC10 Basic Path

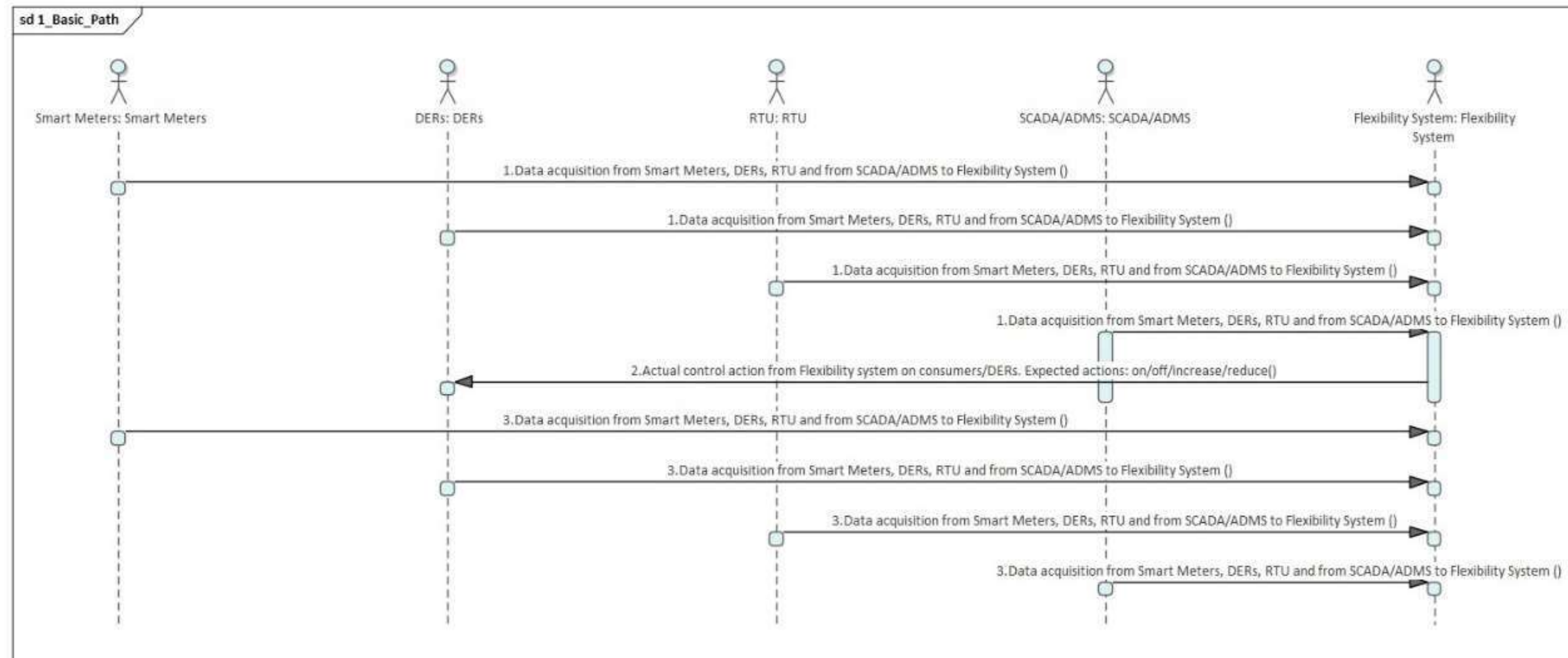


Figure 59 - UC10 Sequence Diagram



UC11 - DSO - TSO congestion and power quality coordination in application of system services

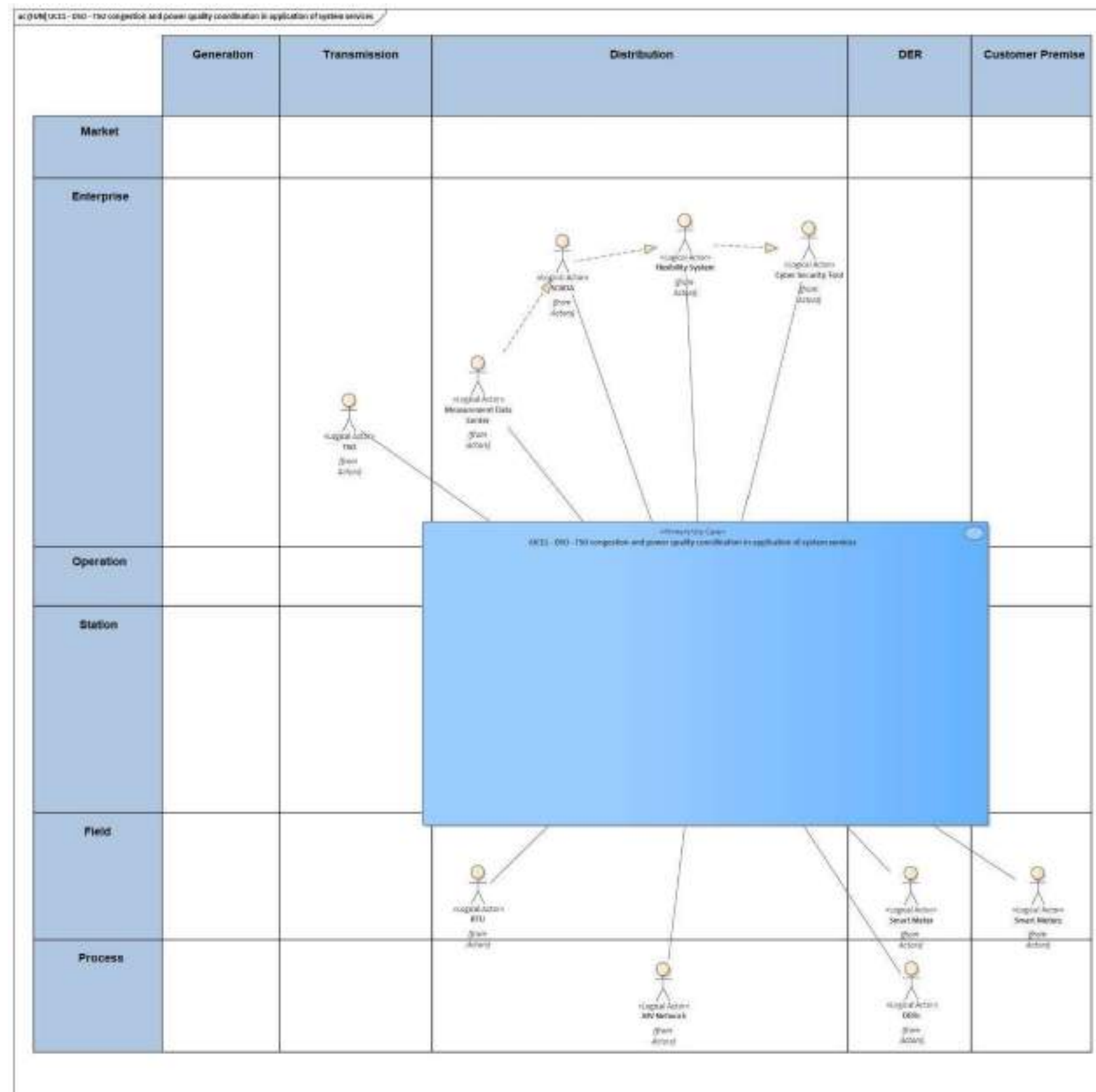


Figure 60 - UC11 Functional Layer

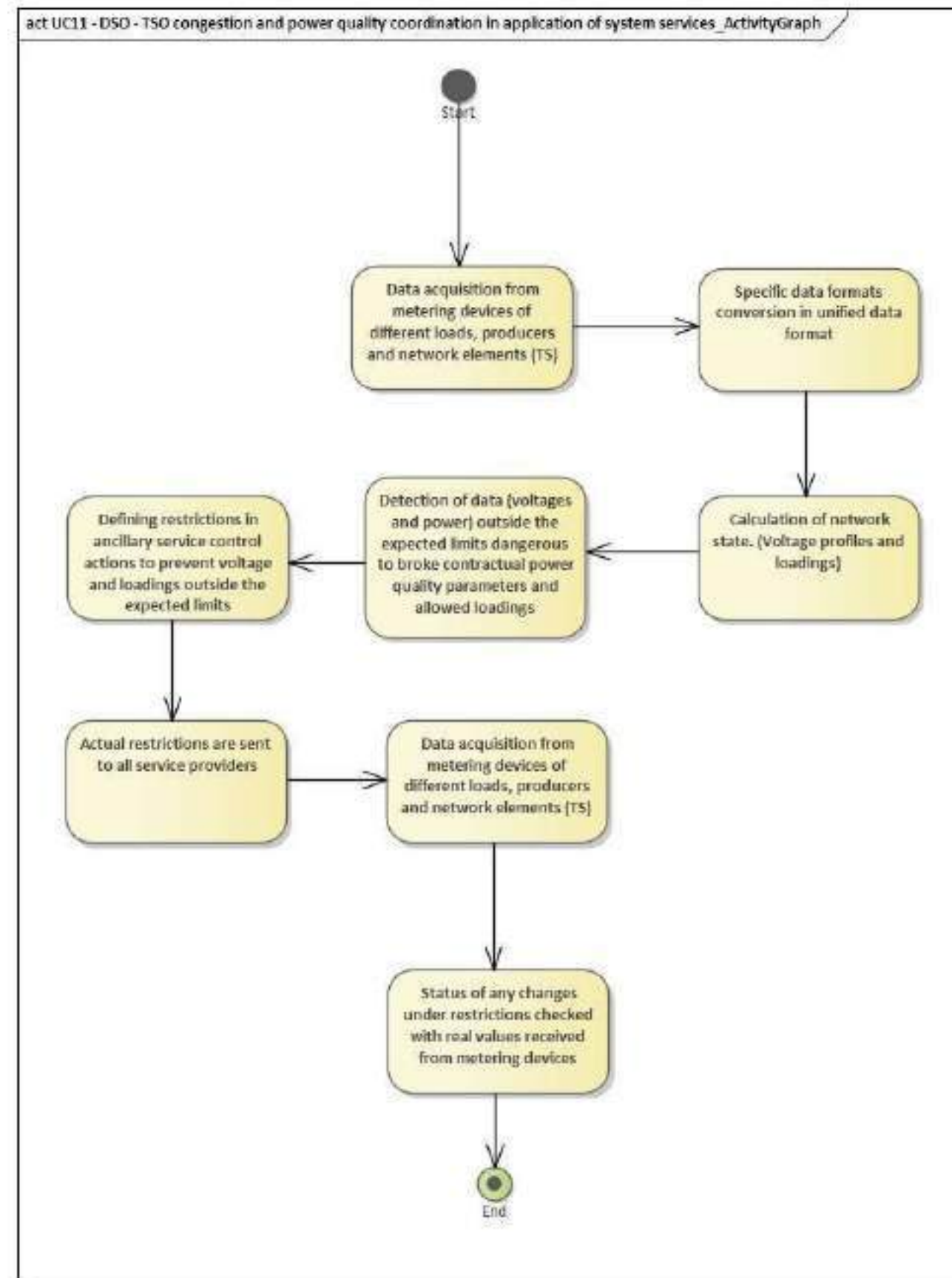


Figure 61 – UC11 Activity Graph

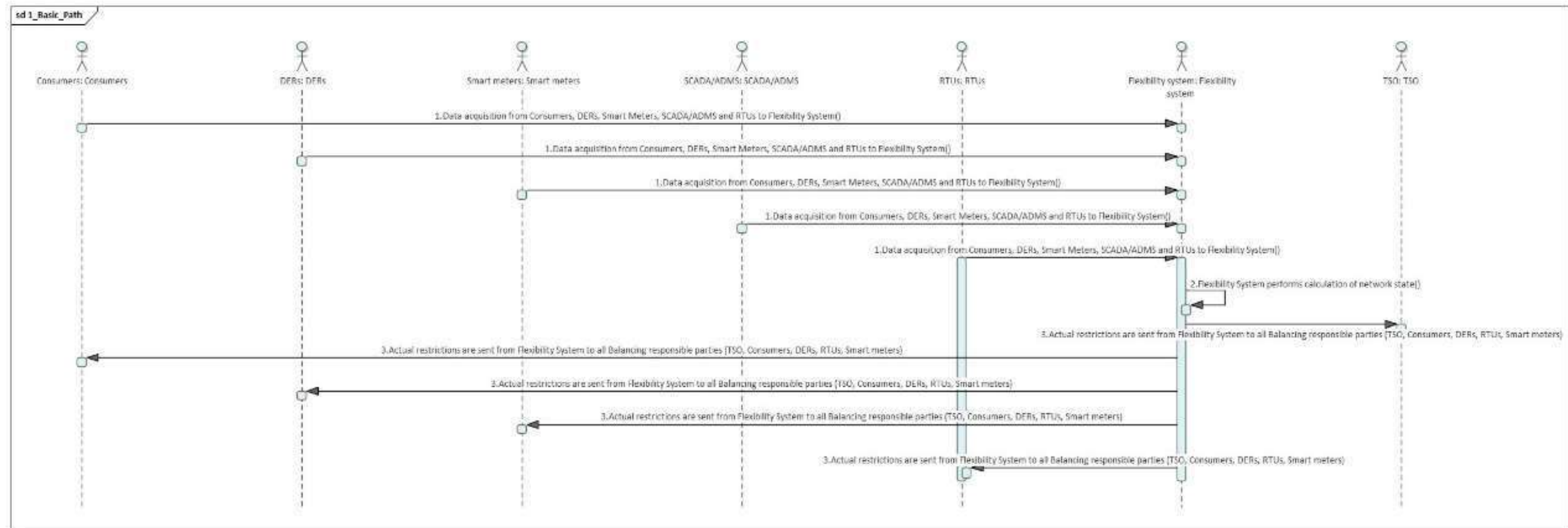


Figure 62 - UC11 Sequence Diagram



UC12 – Emergency & Restoration – Over-Frequency Protection Module

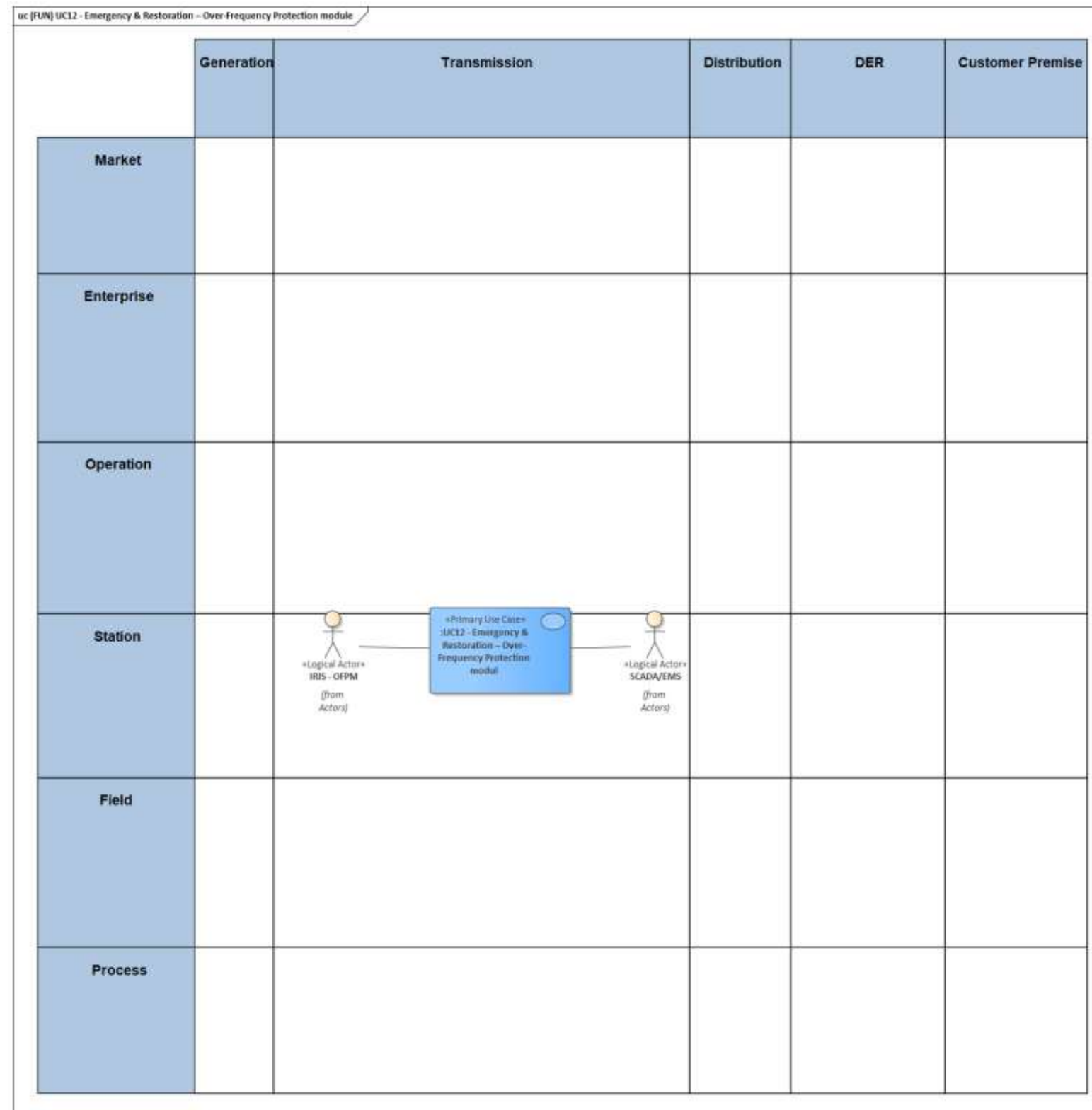


Figure 63 – UC12 Functional Layer

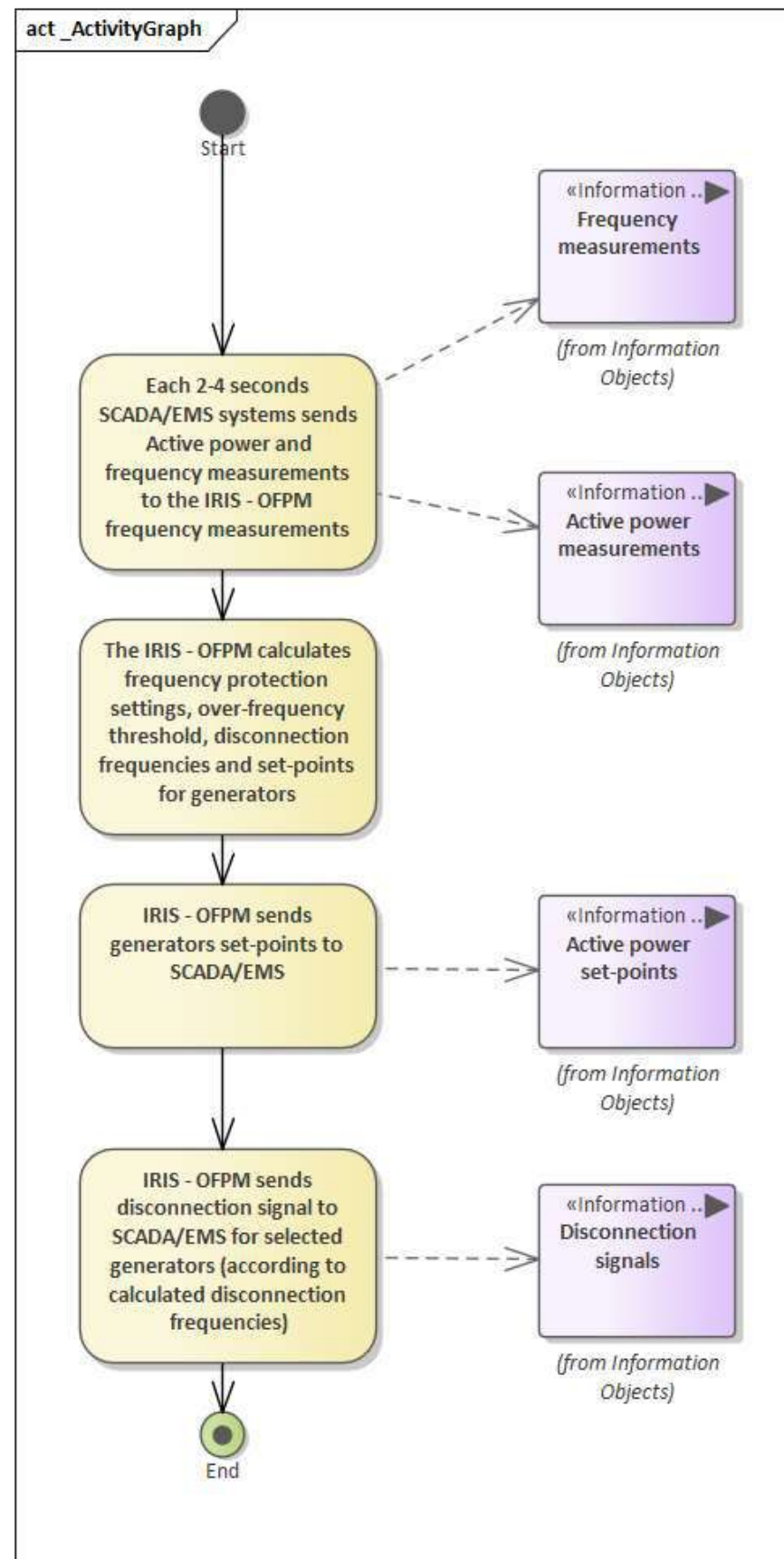


Figure 64 - UC12 Activity Graph

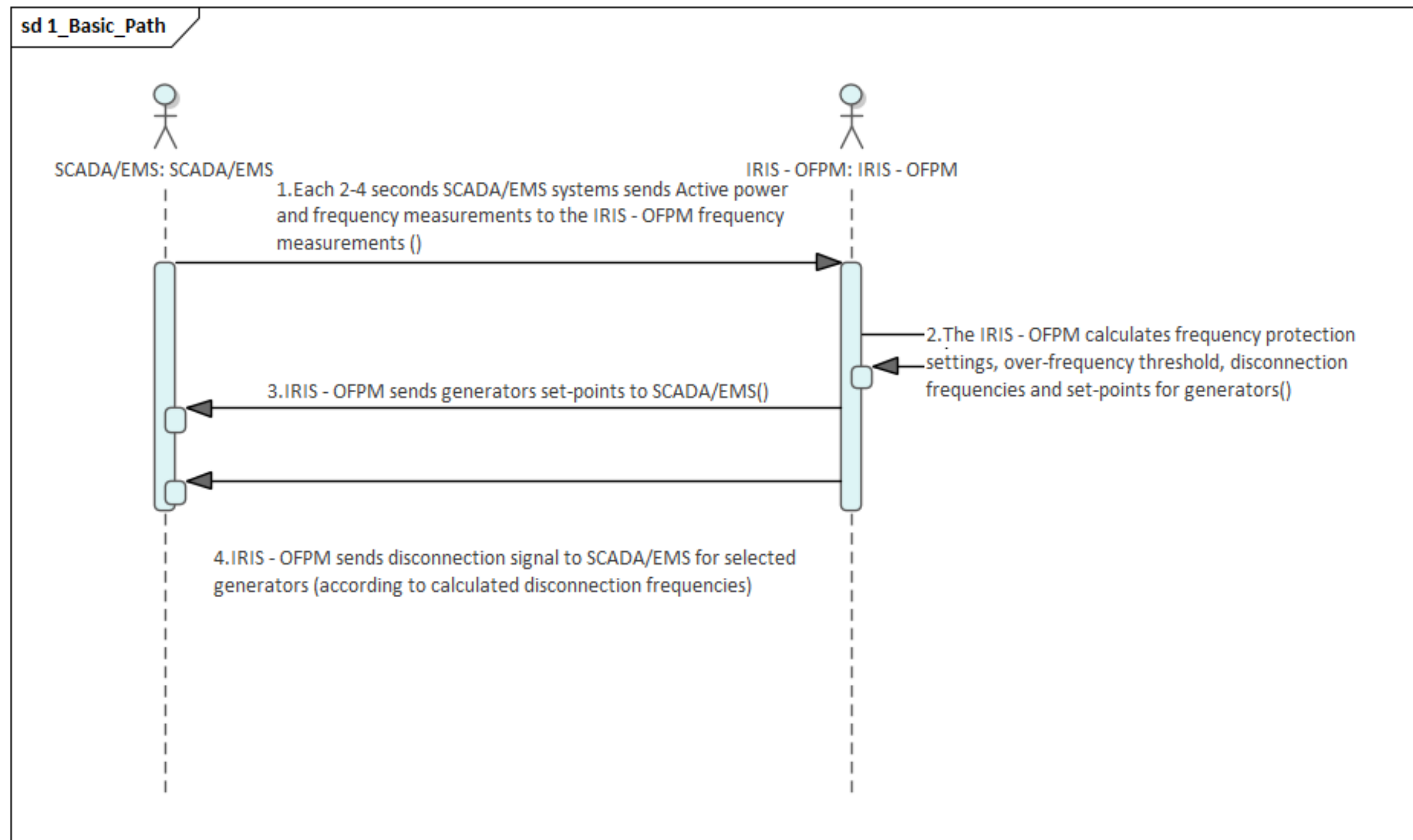


Figure 65 - UC12 Basic Path

UC15 - DSO-TSO cooperation in Individual Grid Model creation

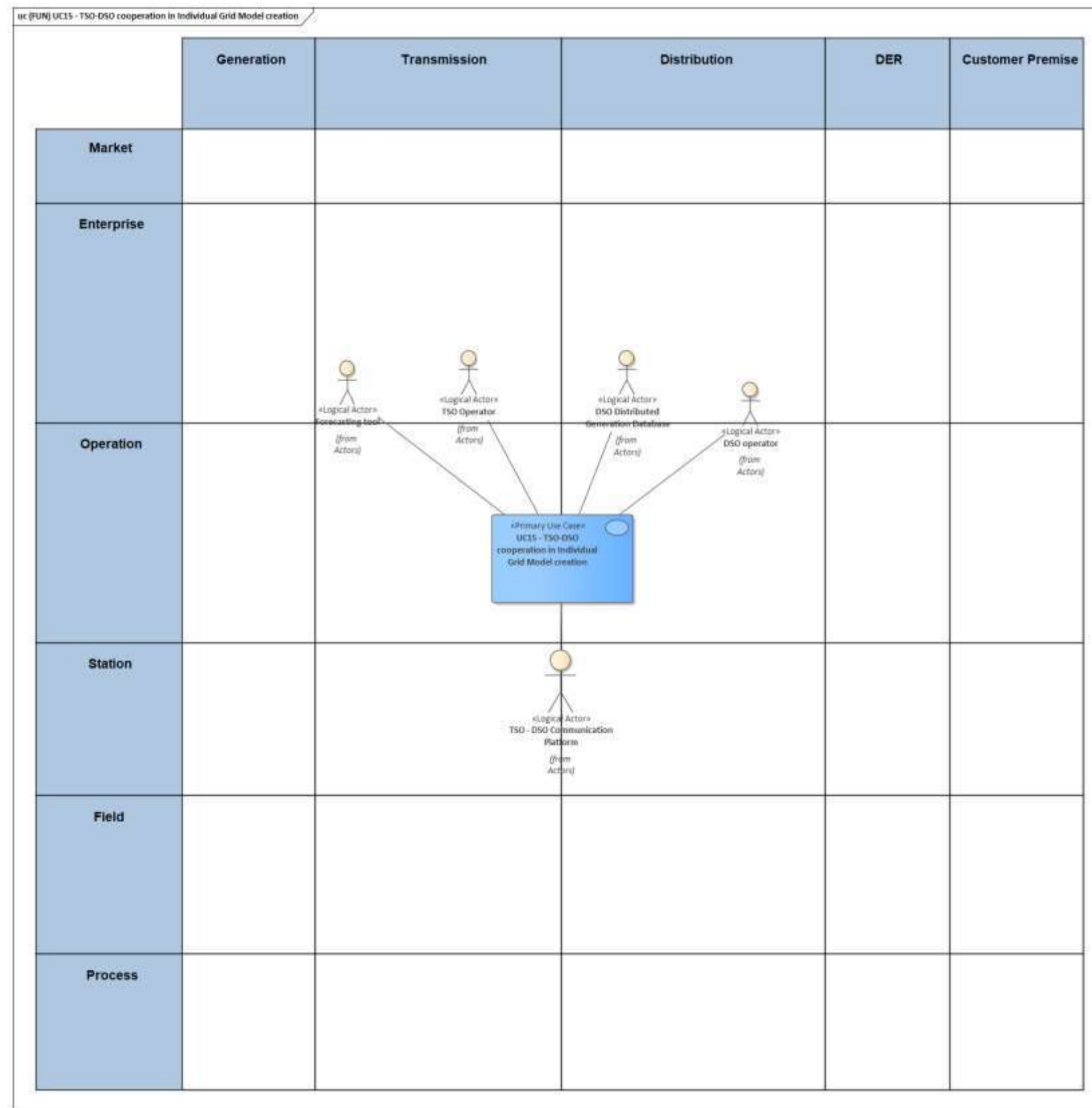


Figure 66 - UC15 Functional Layer

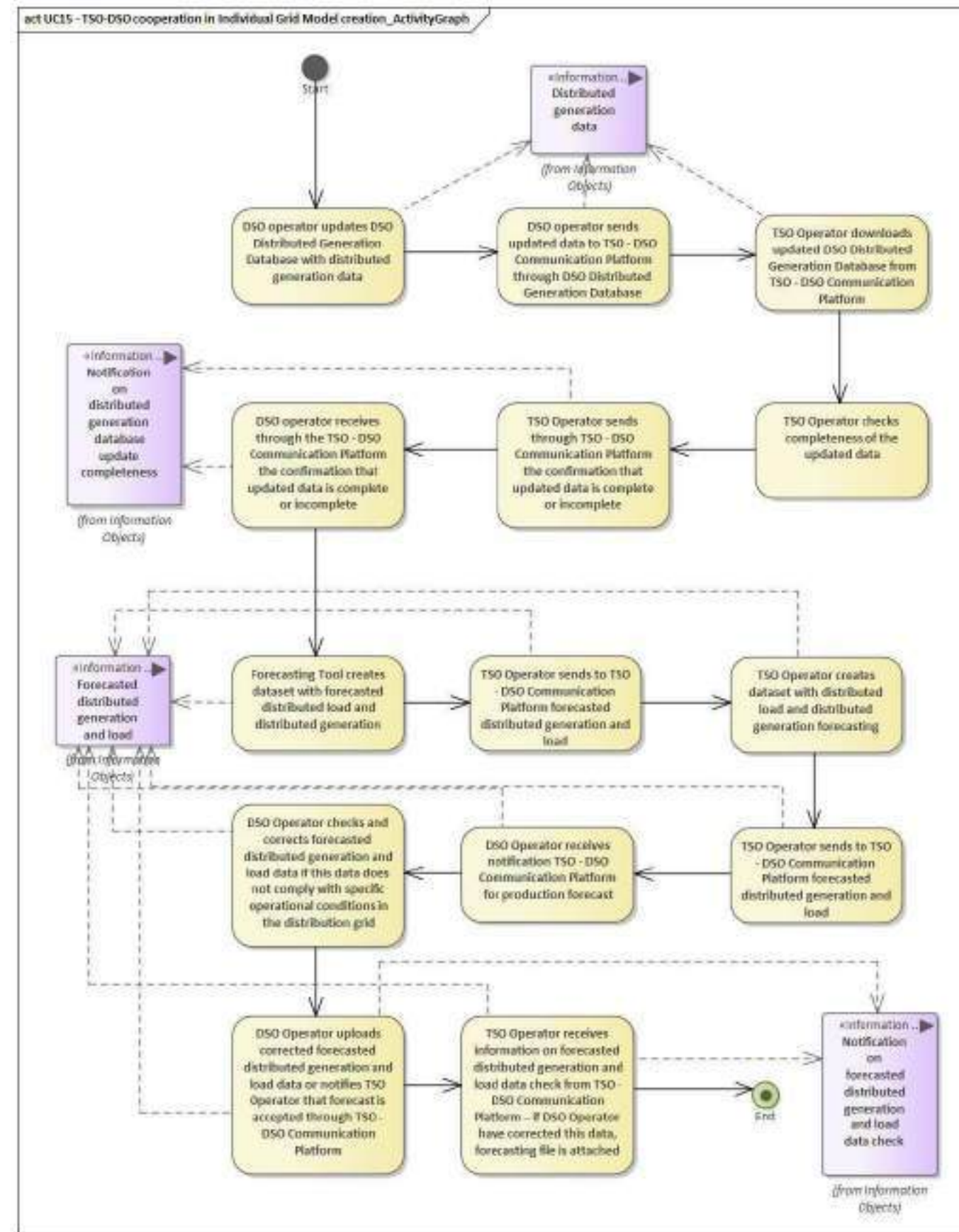


Figure 67 - UC15 Activity Graph

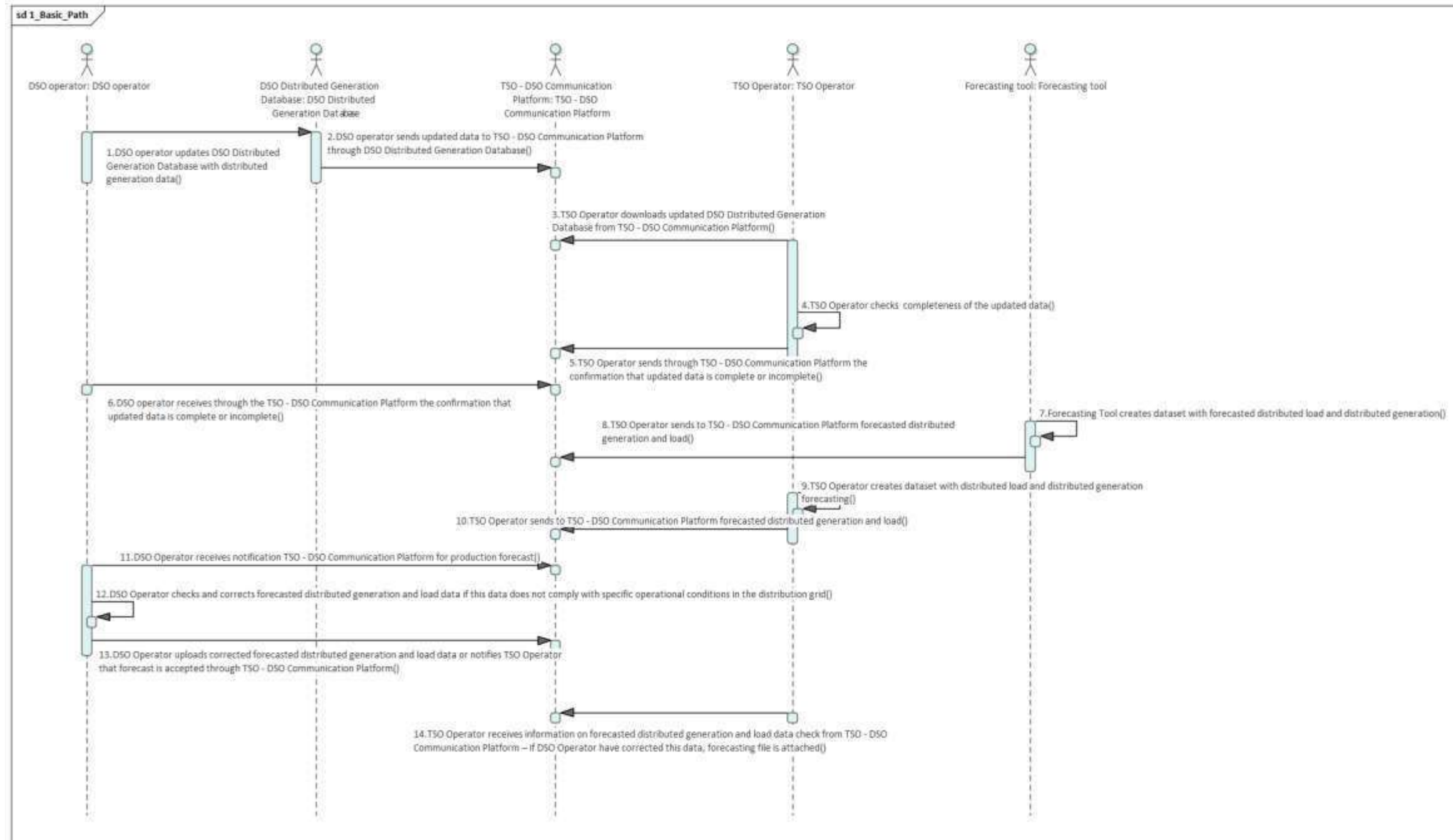


Figure 68 – UC15 Basic Path



UC16 – Phasor angles monitoring and prevention of instability

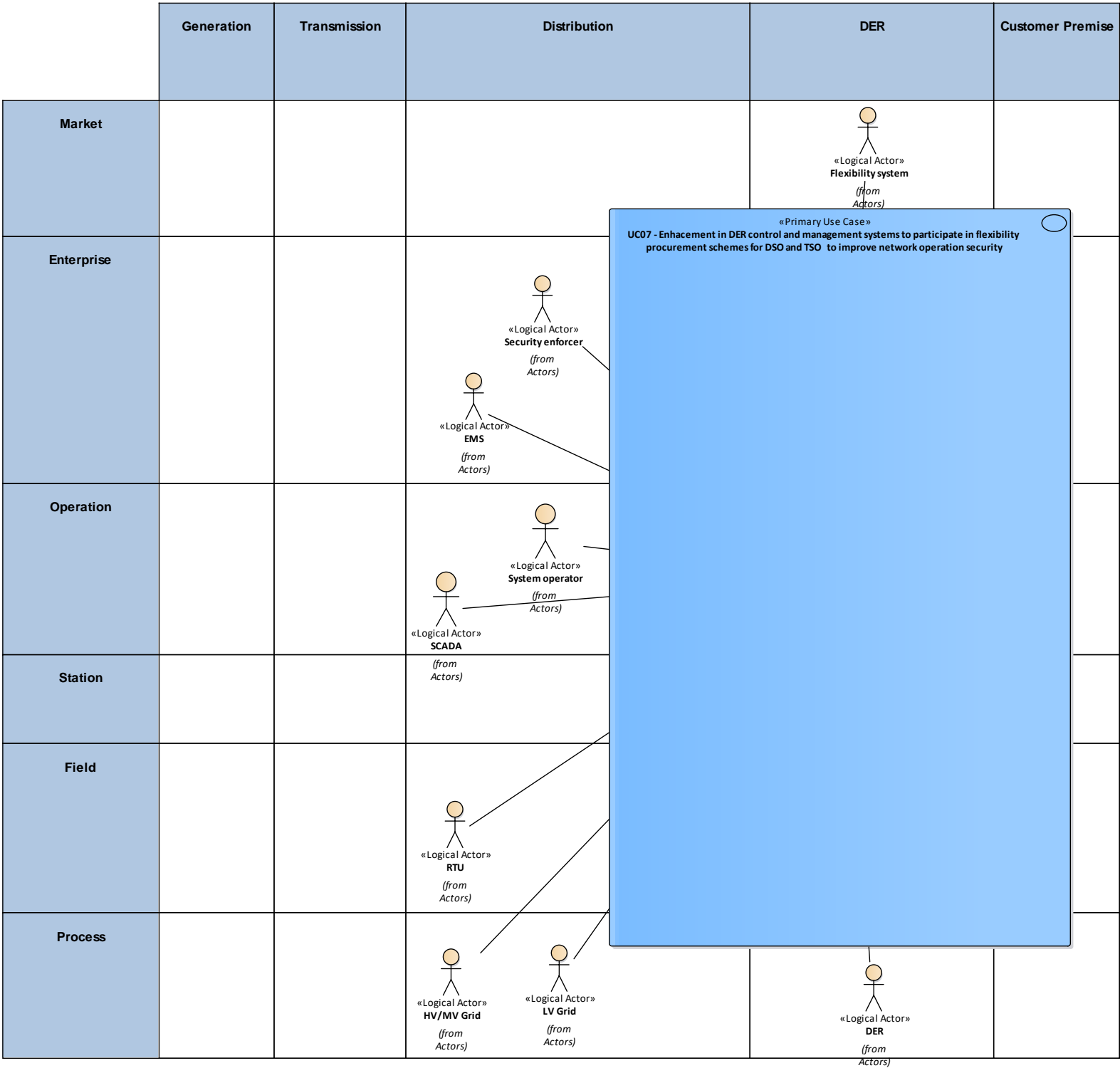


Figure 69 – UC16 Functional Layer

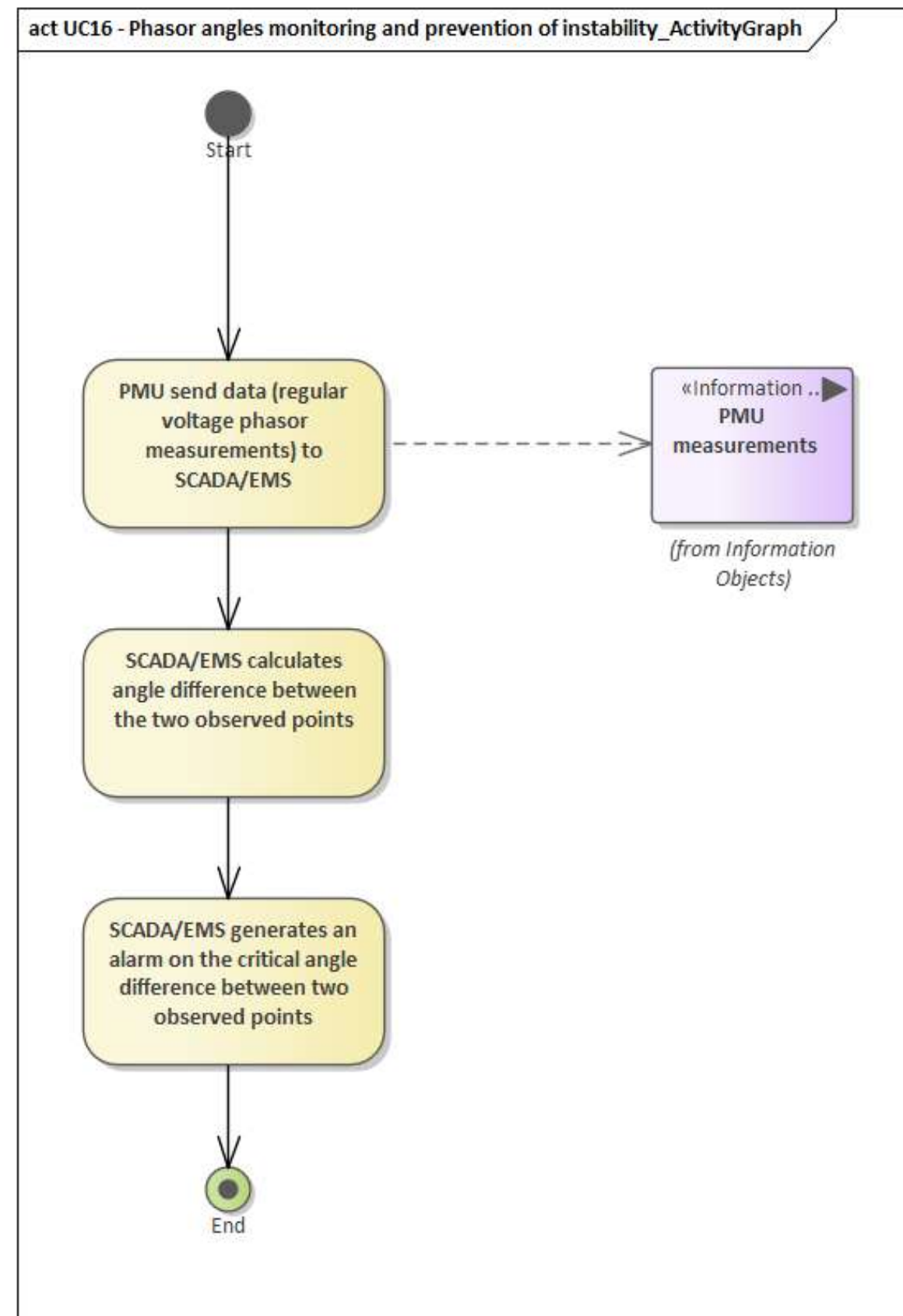


Figure 70 - UC16 Activity Graph

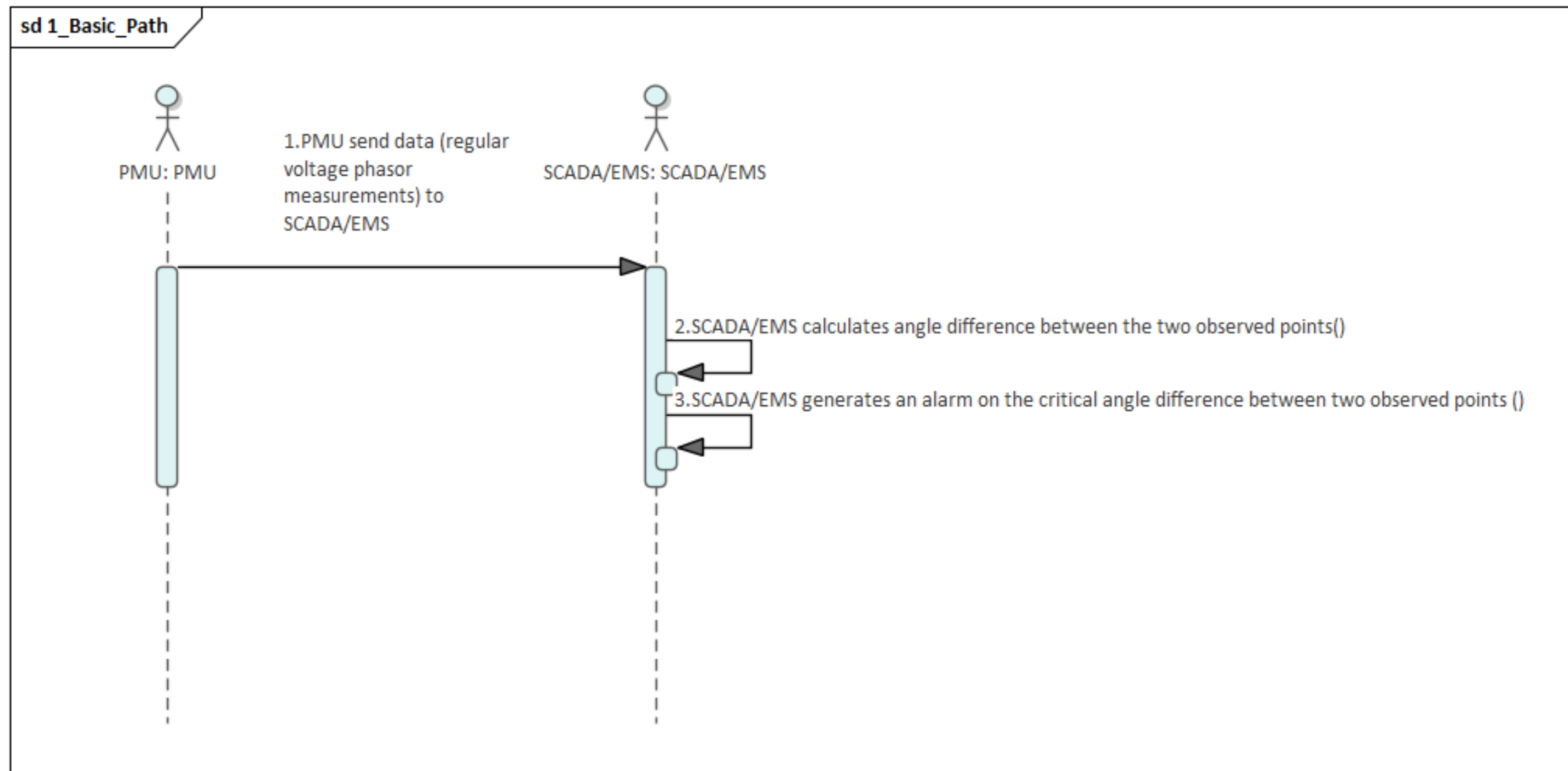


Figure 71 - UC16 Basic Path

UC18 – Optimization of PMU installation points

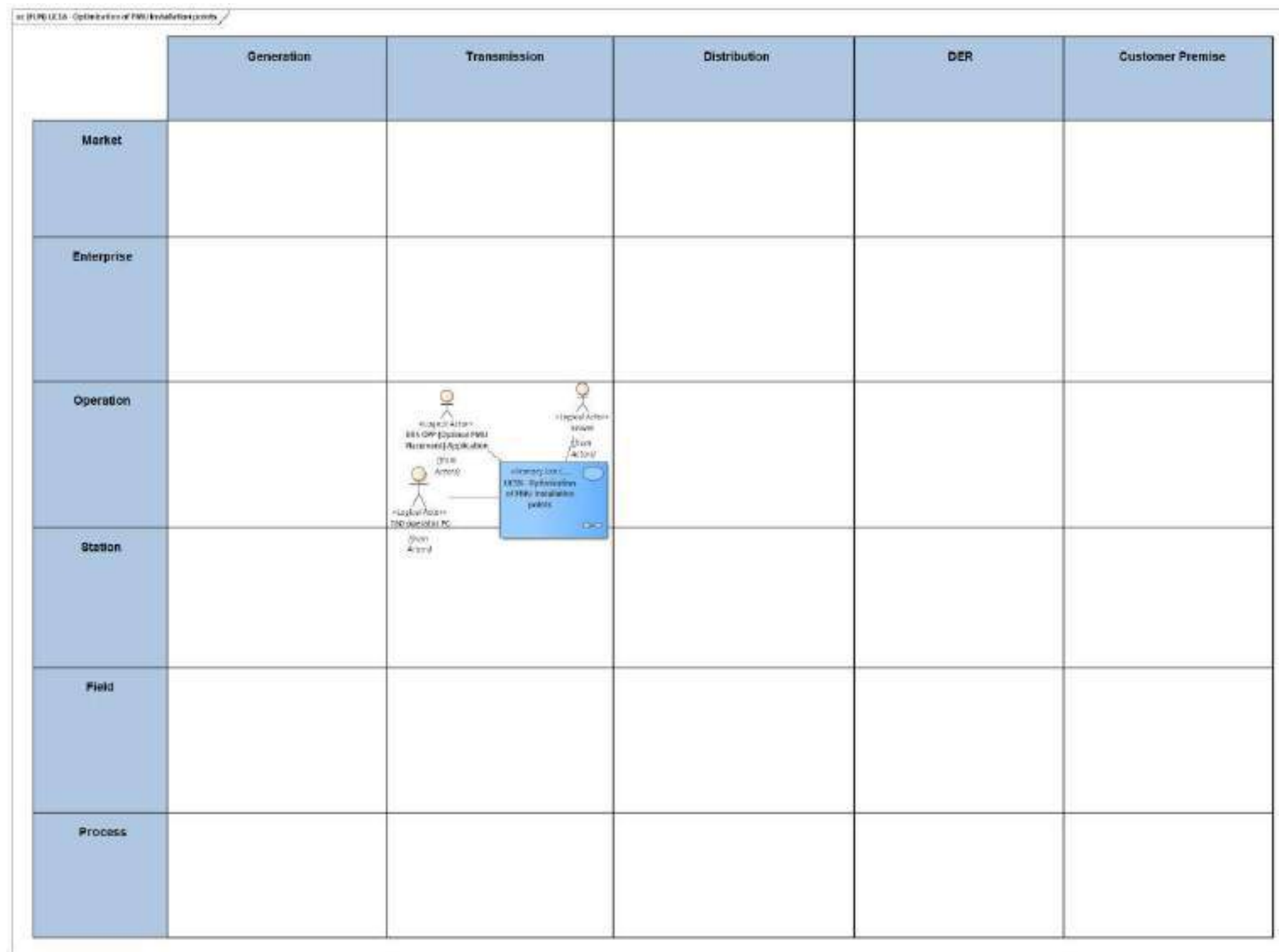


Figure 72 - UC18 Functional Layer

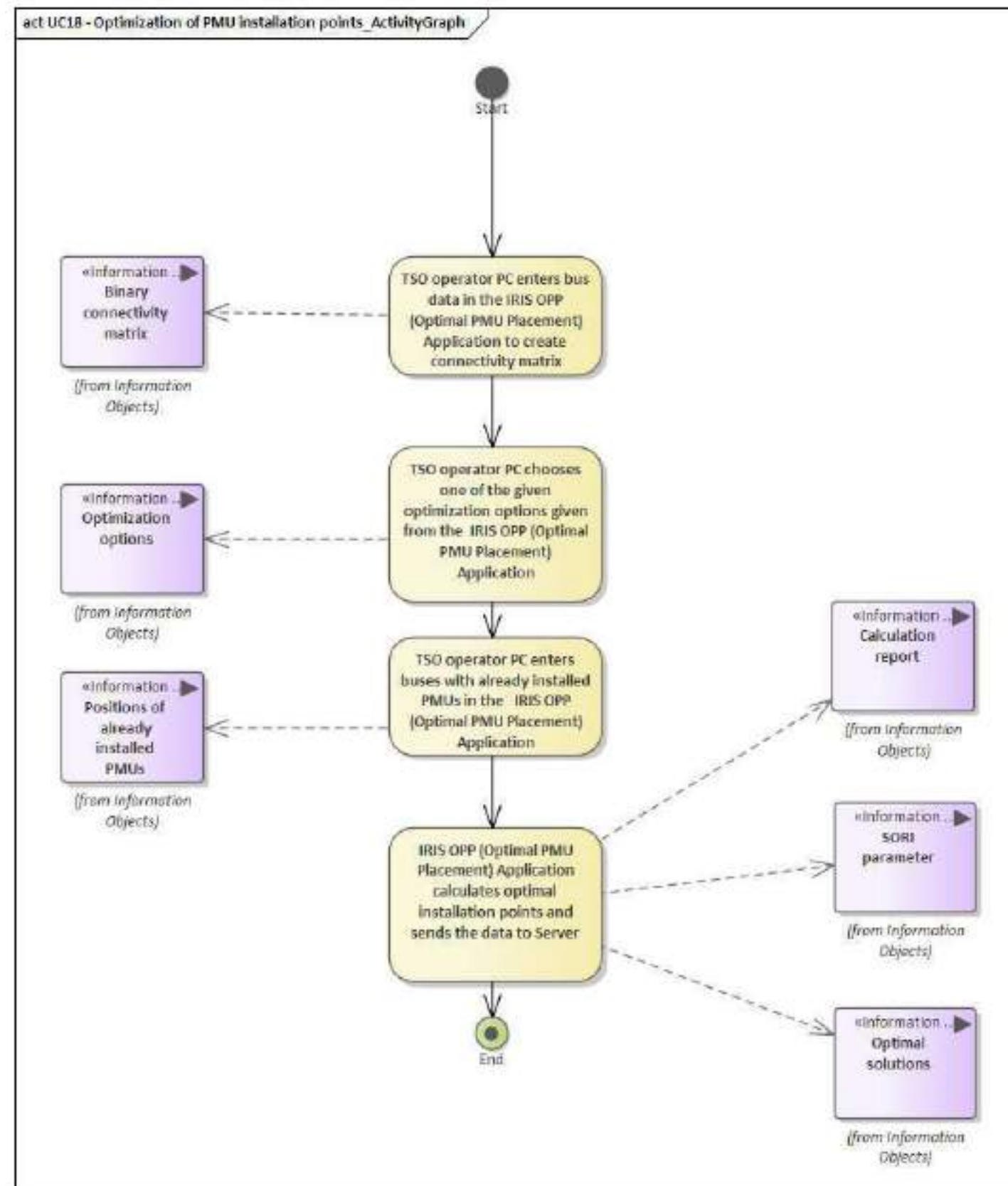


Figure 73 - UC18 Activity Graph

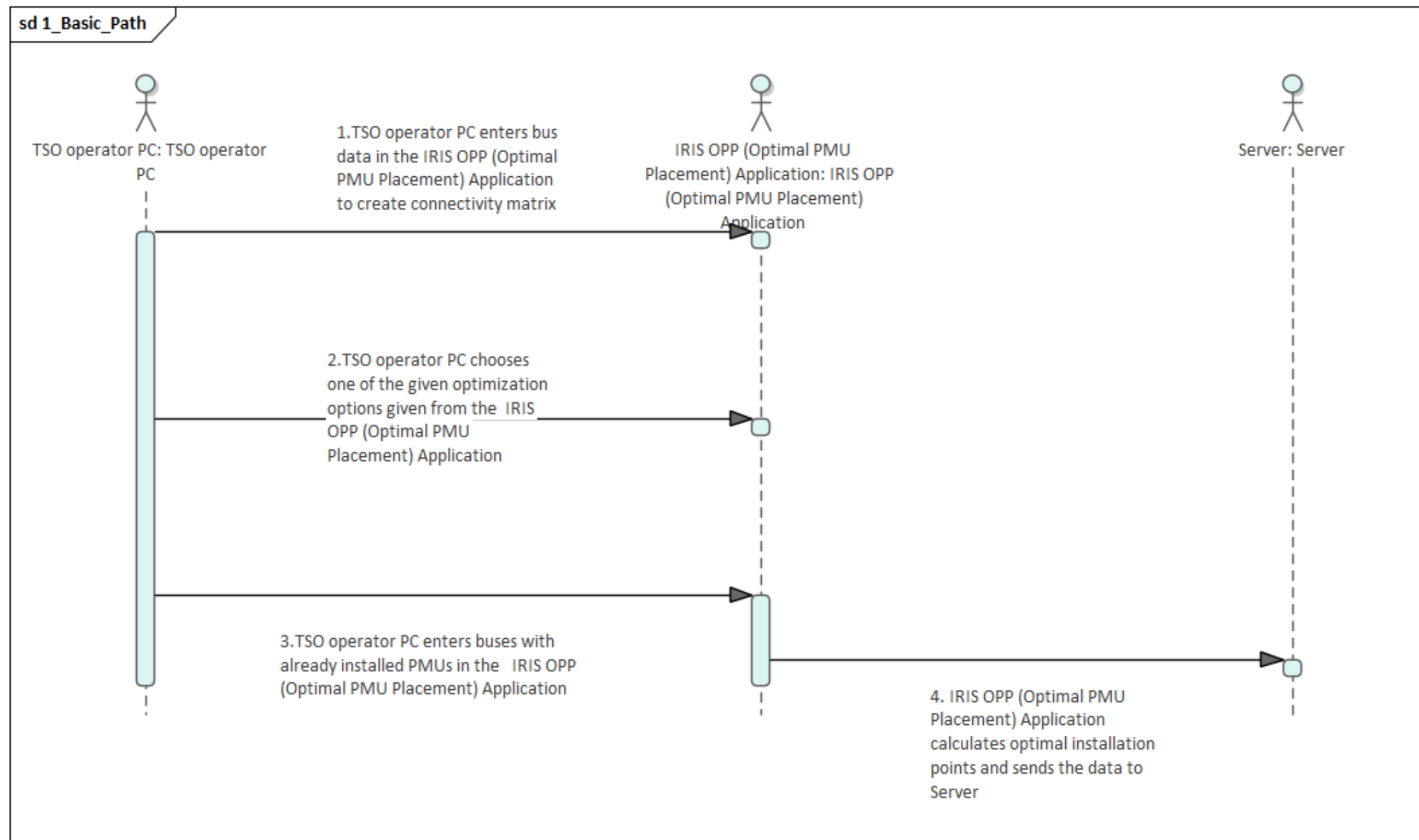


Figure 74 - UC18 Basic Path



UC19 – Emergency & Restoration – System Split module upgrade

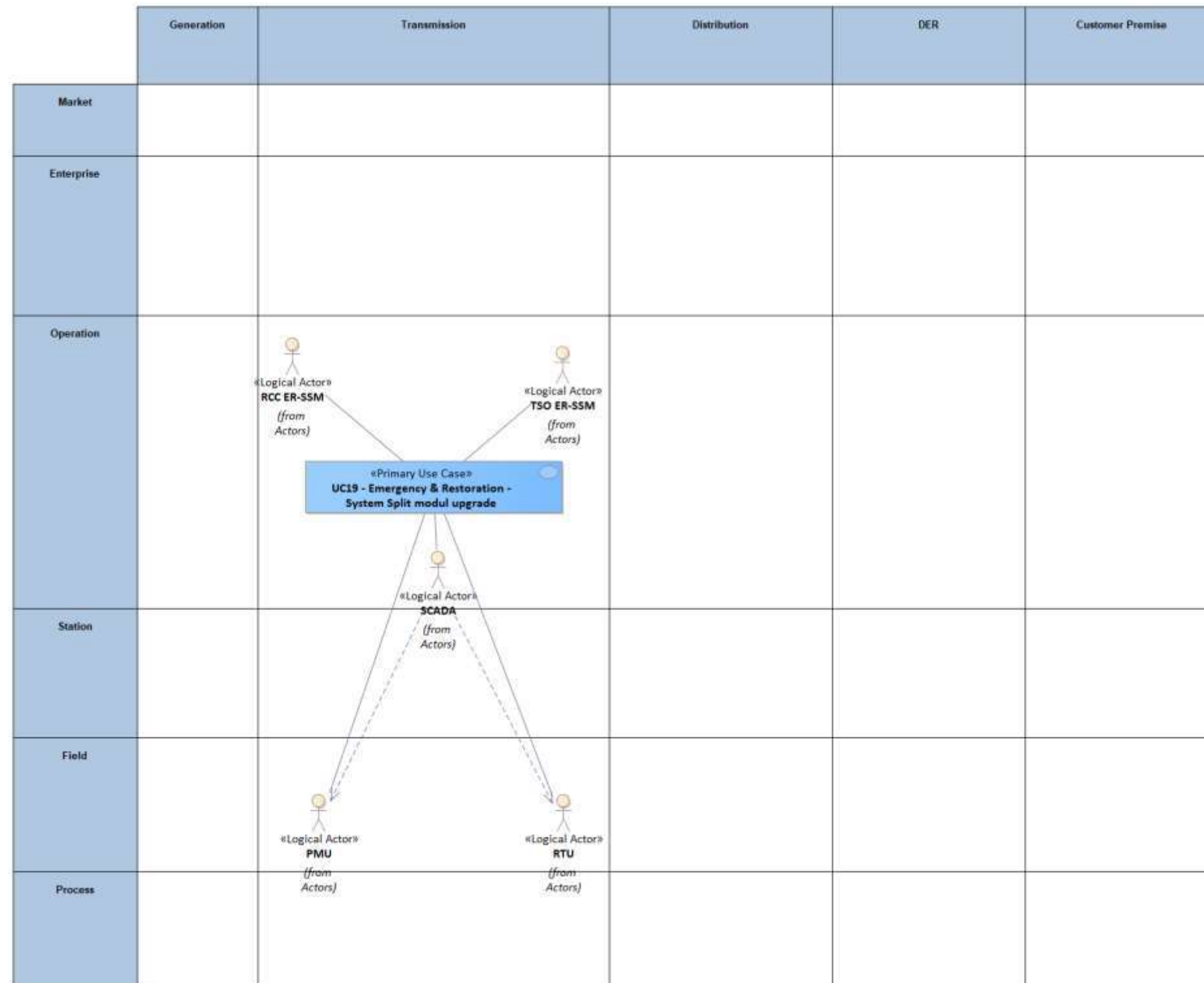


Figure 75 – UC19 Functional Layer

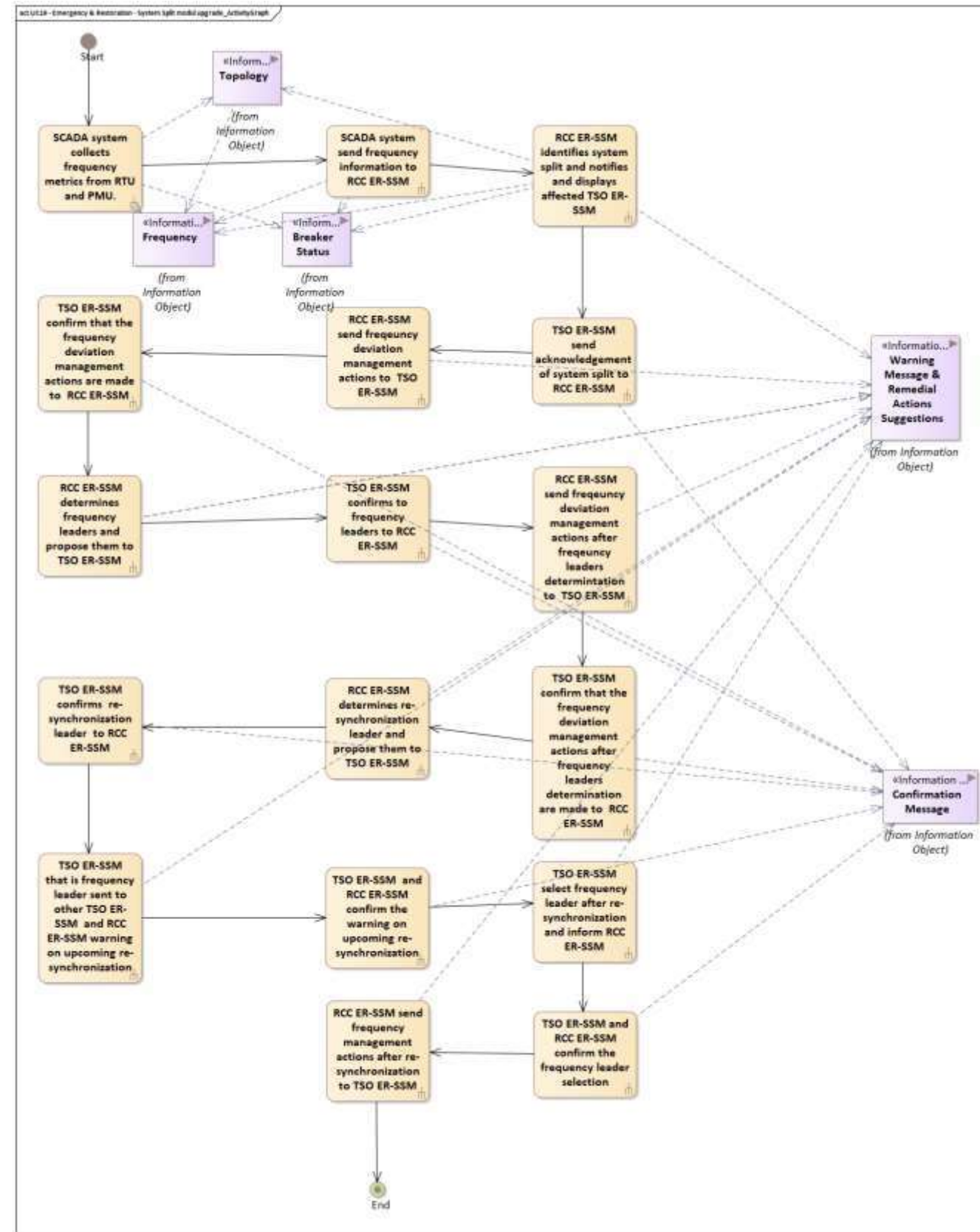


Figure 76 - UC19 Activity Graph

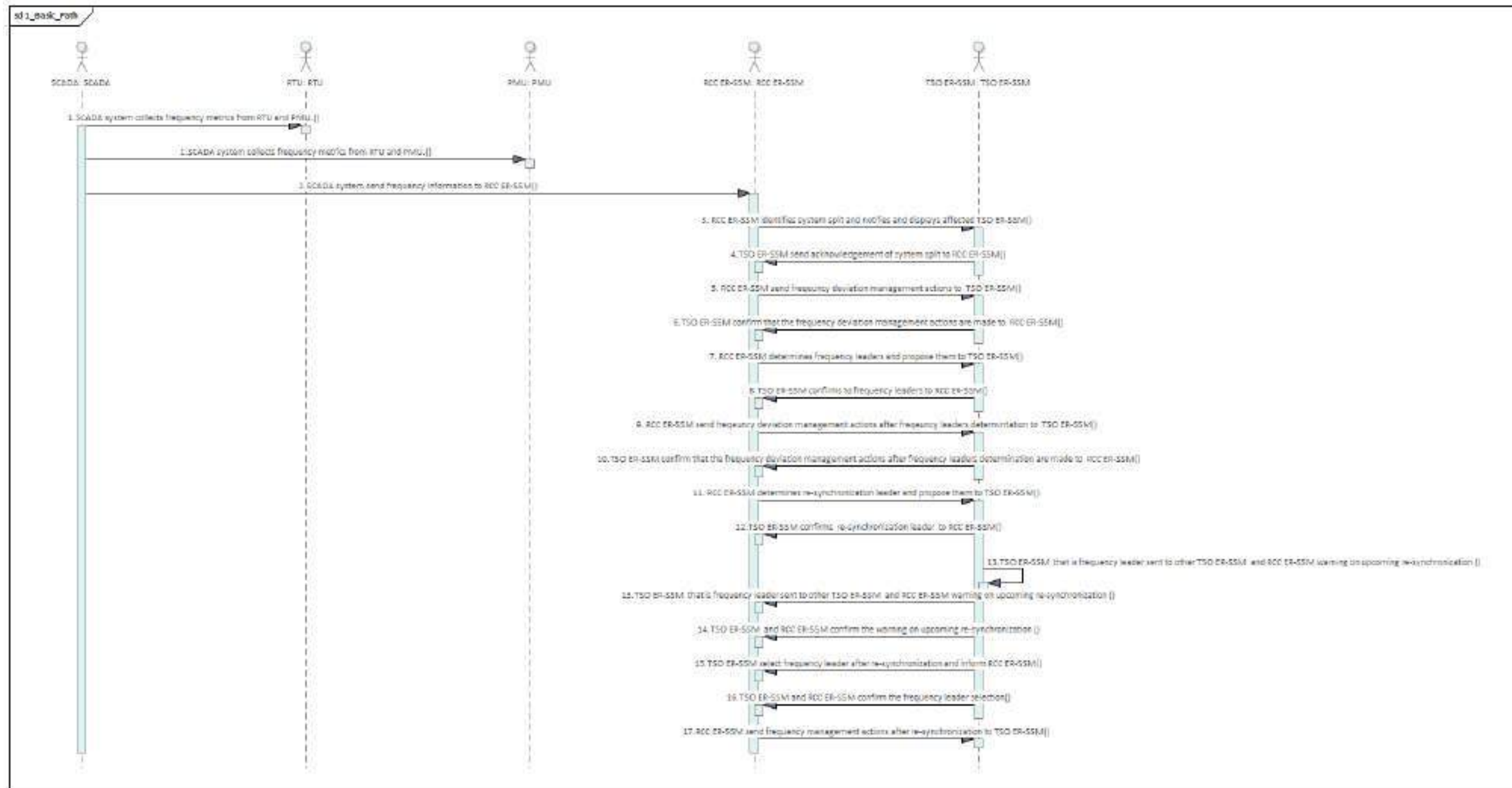


Figure 77 - UC19 Basic Path



UC21 - Remedial Actions Automation

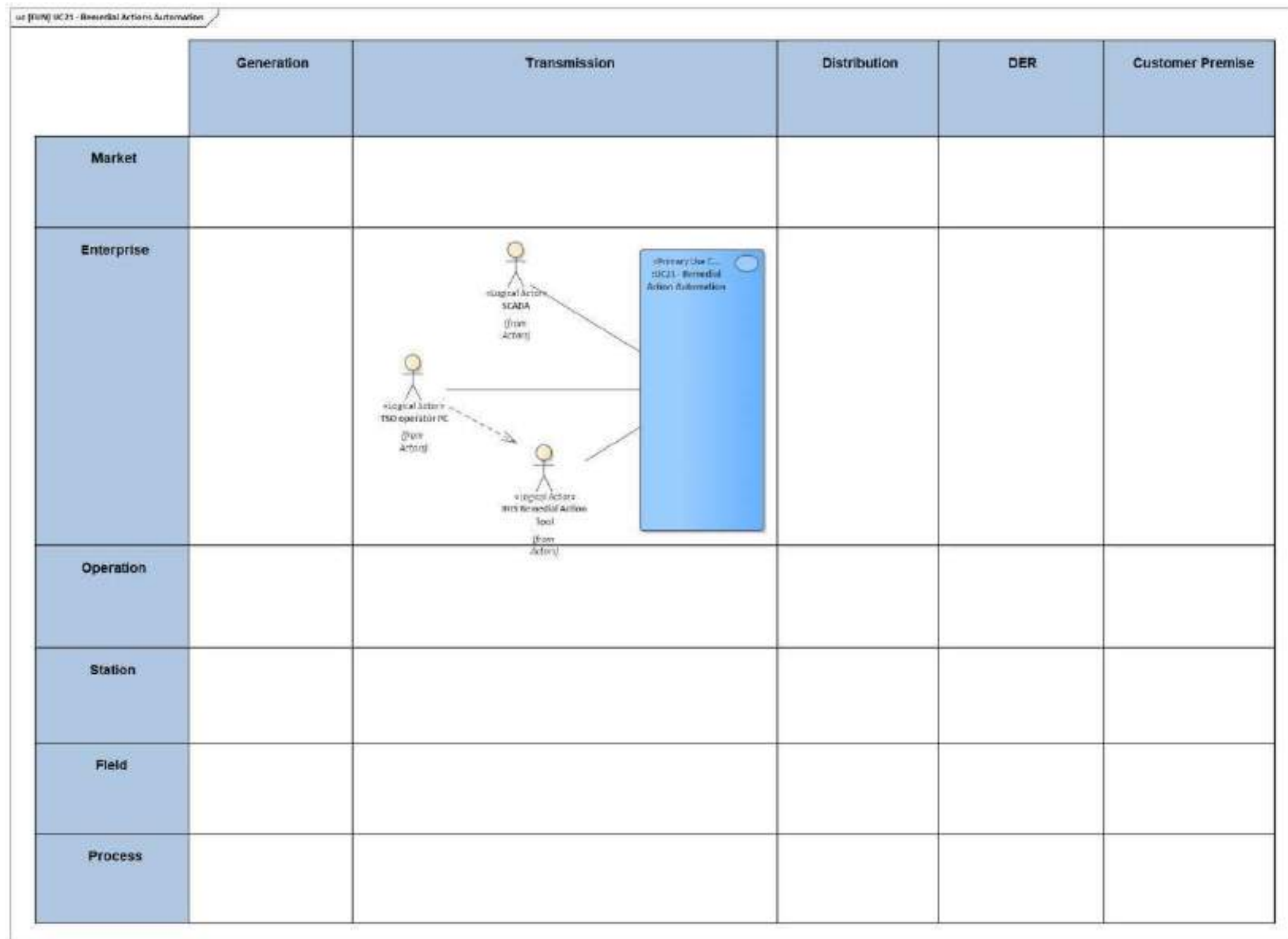


Figure 78 - UC21 Functional Layer

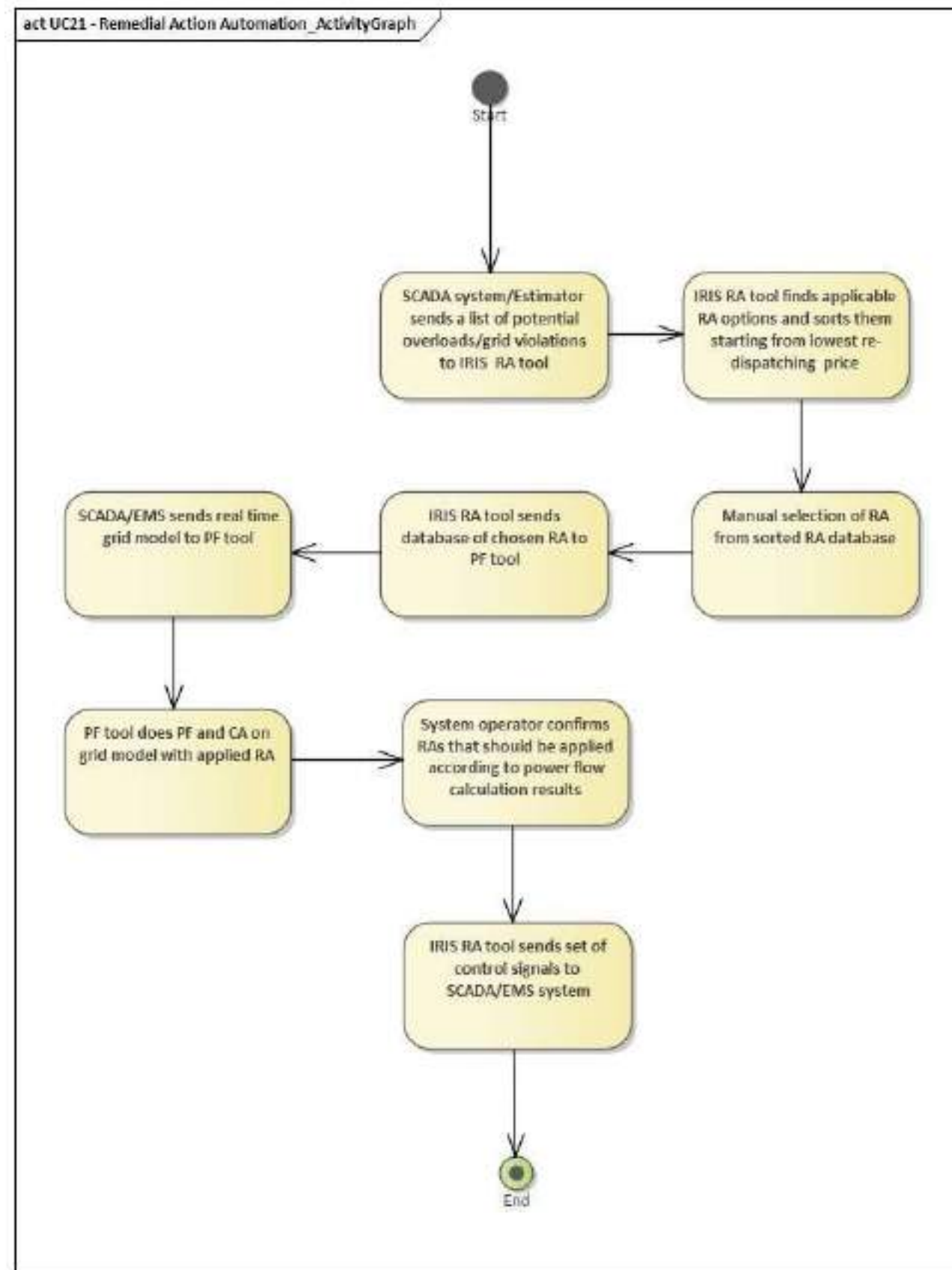


Figure 79 - Activity Graph

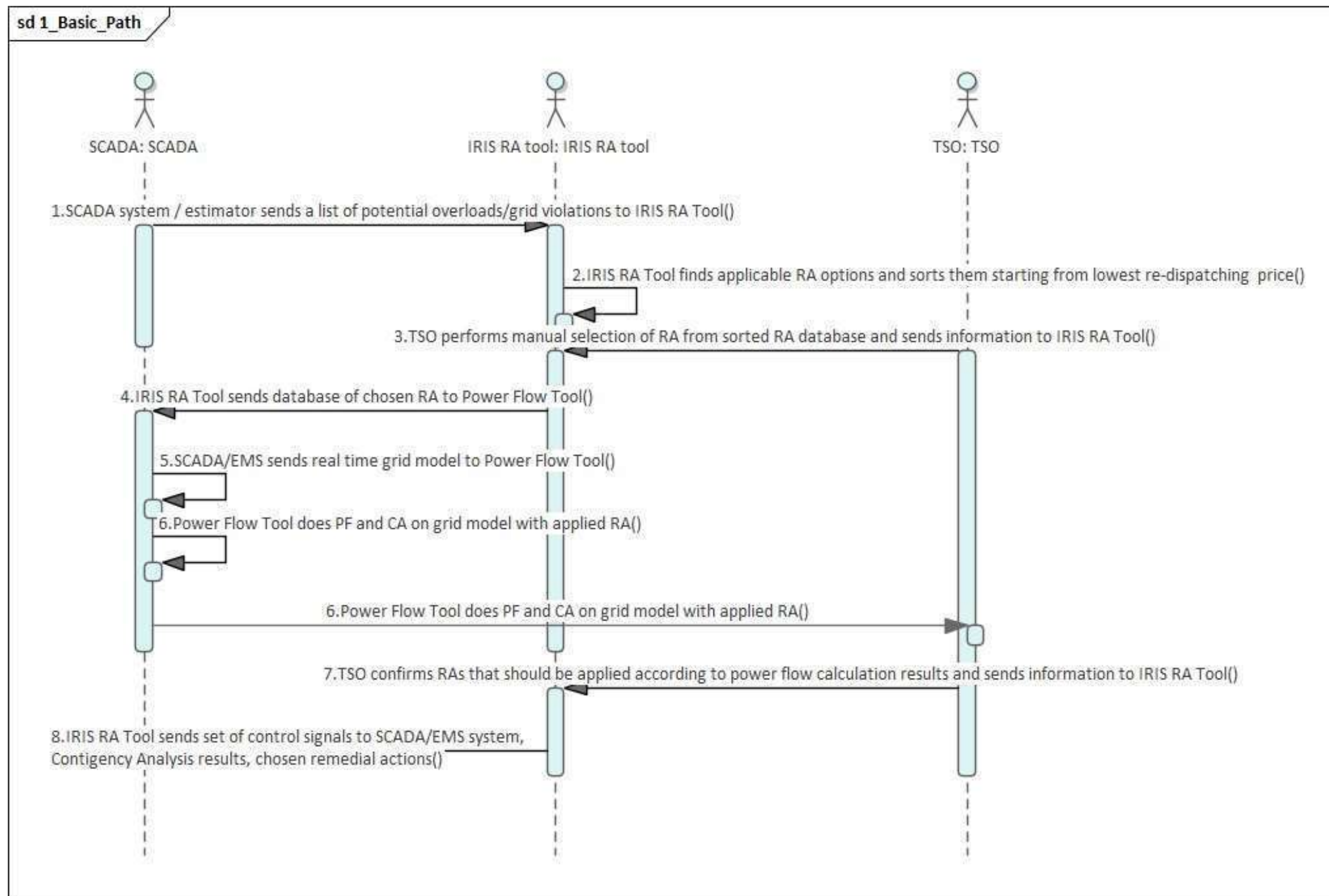


Figure 80 - UC21 Basic Path

UC35 - Upstream studies to validate the use of TS0/DS0 means during crisis situations

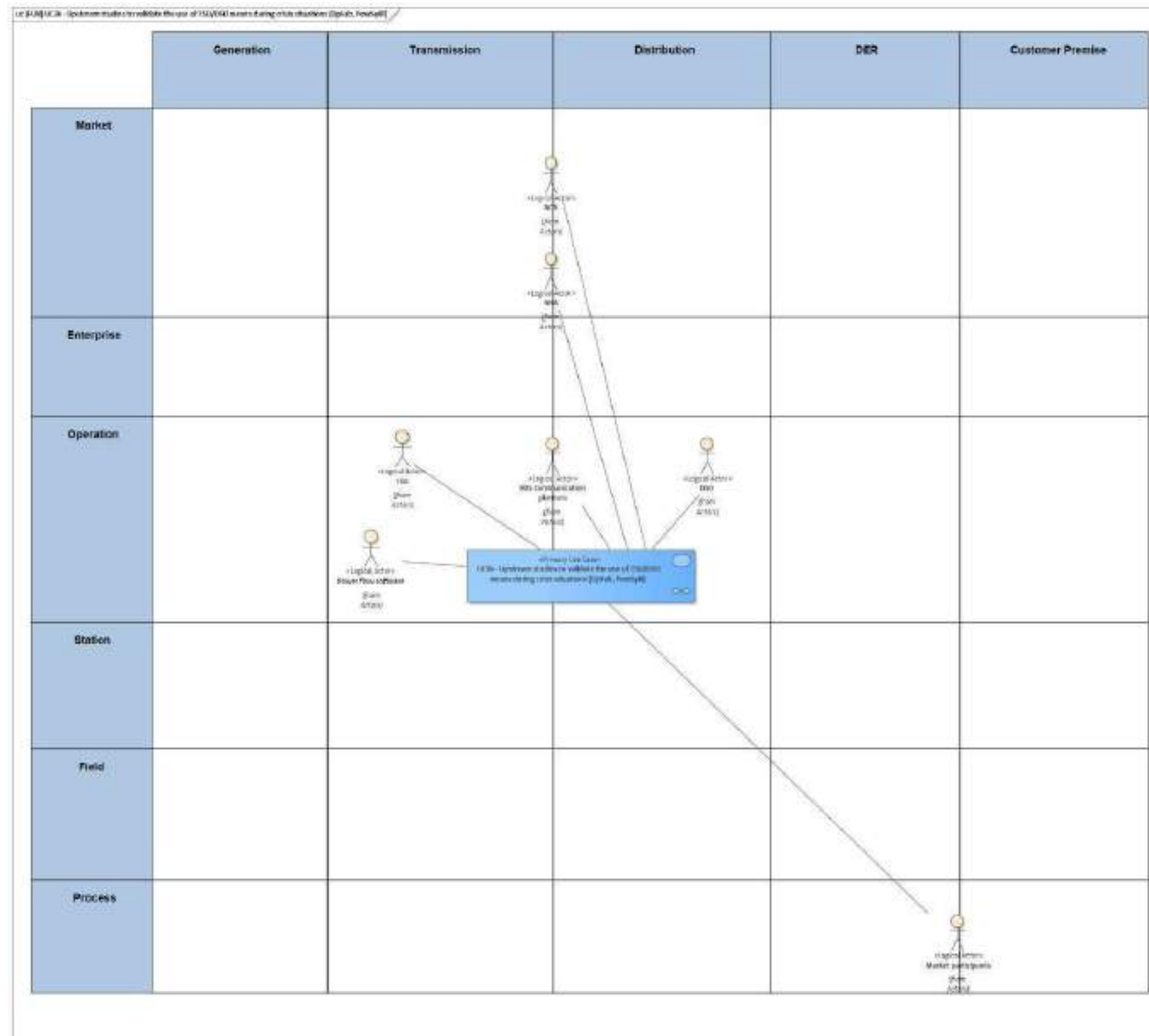


Figure 81 - UC35 Functional Layer

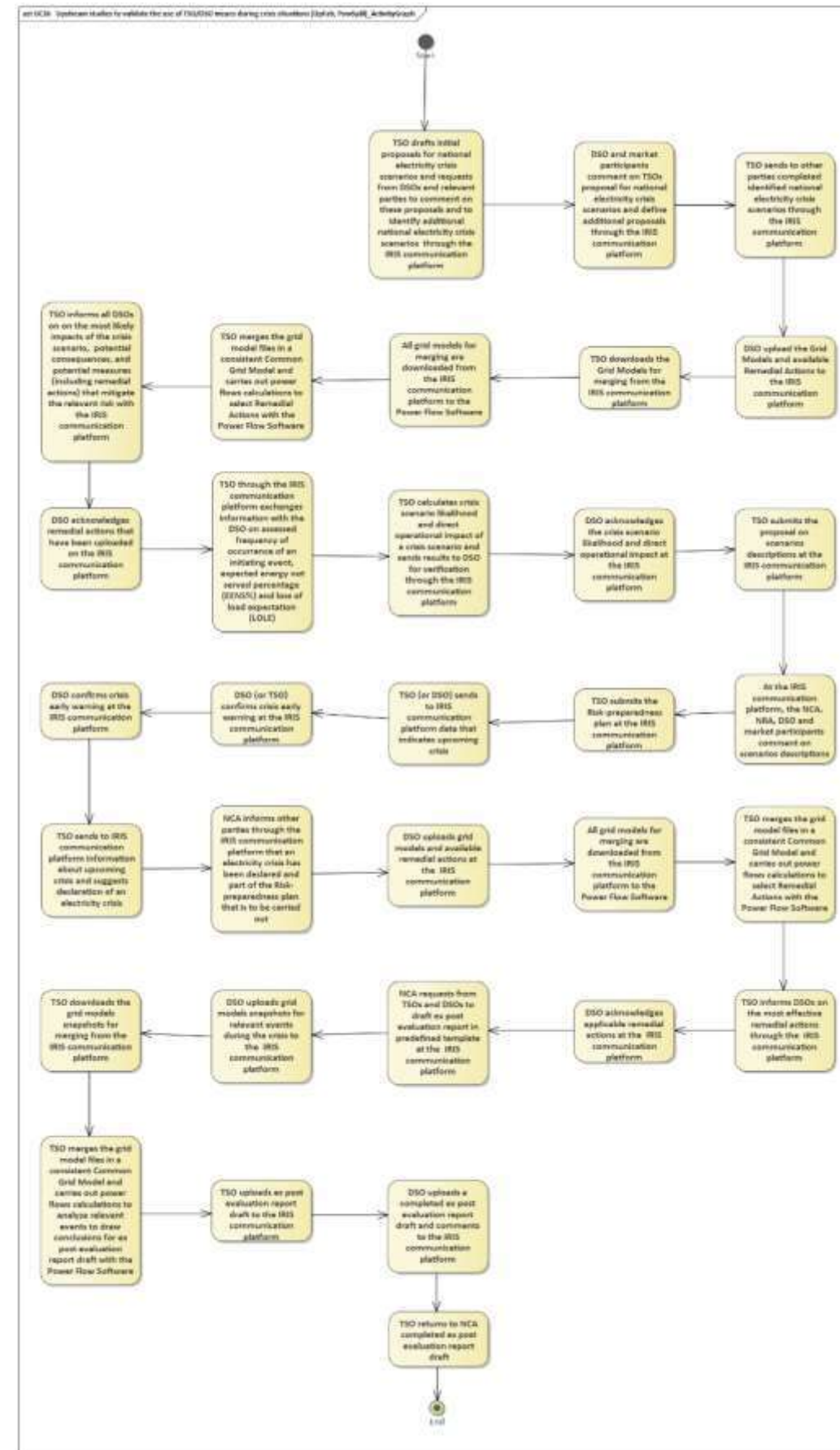


Figure 82- UC35 Activity Graph



Figure 83 - UC35 Basic Path



13.1.3 WP5-PRECOG

UC27 - Monitor communications behavior of newly deployed components in an EPES staging environment

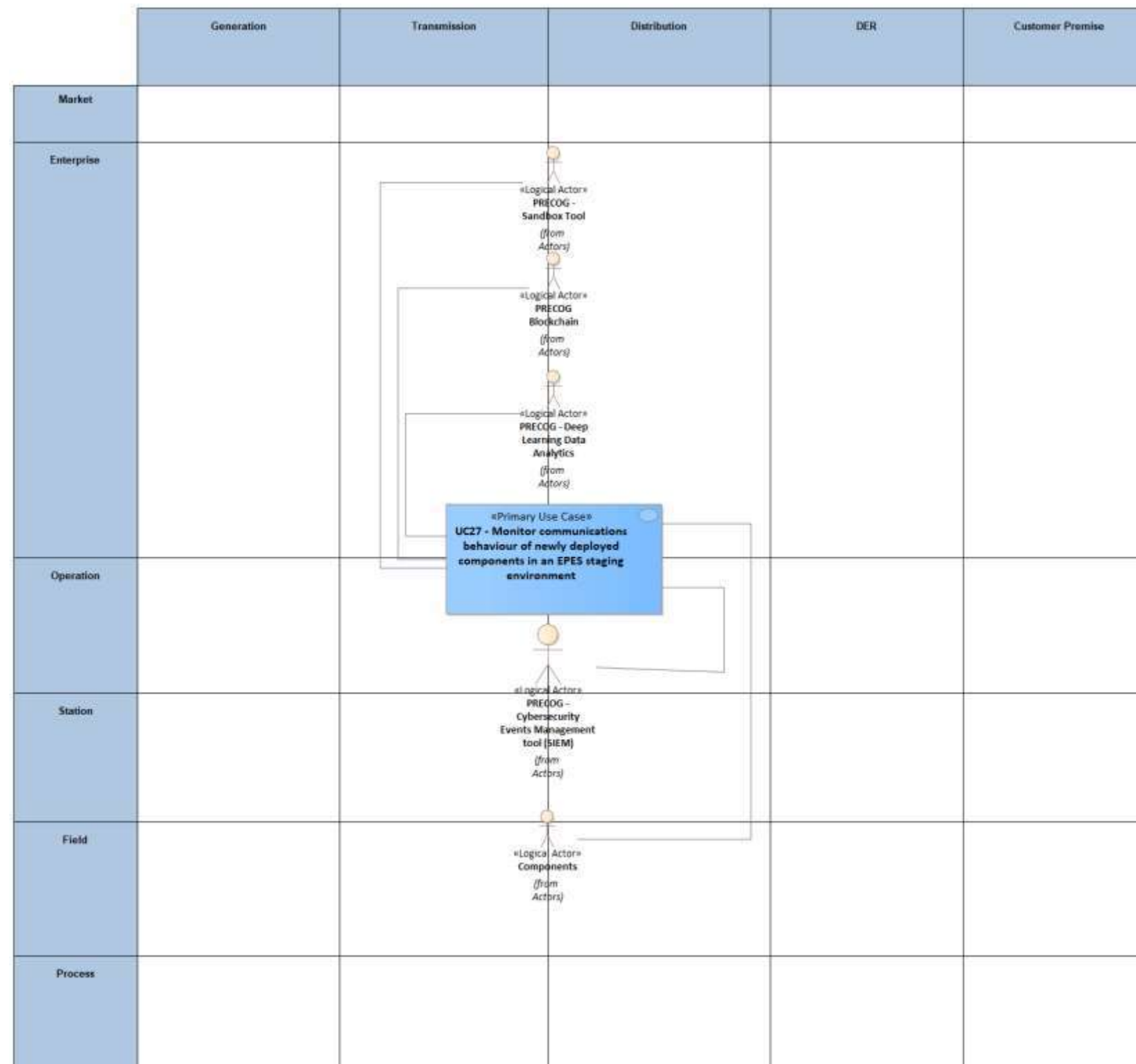


Figure 84 - UC27 Functional Layer

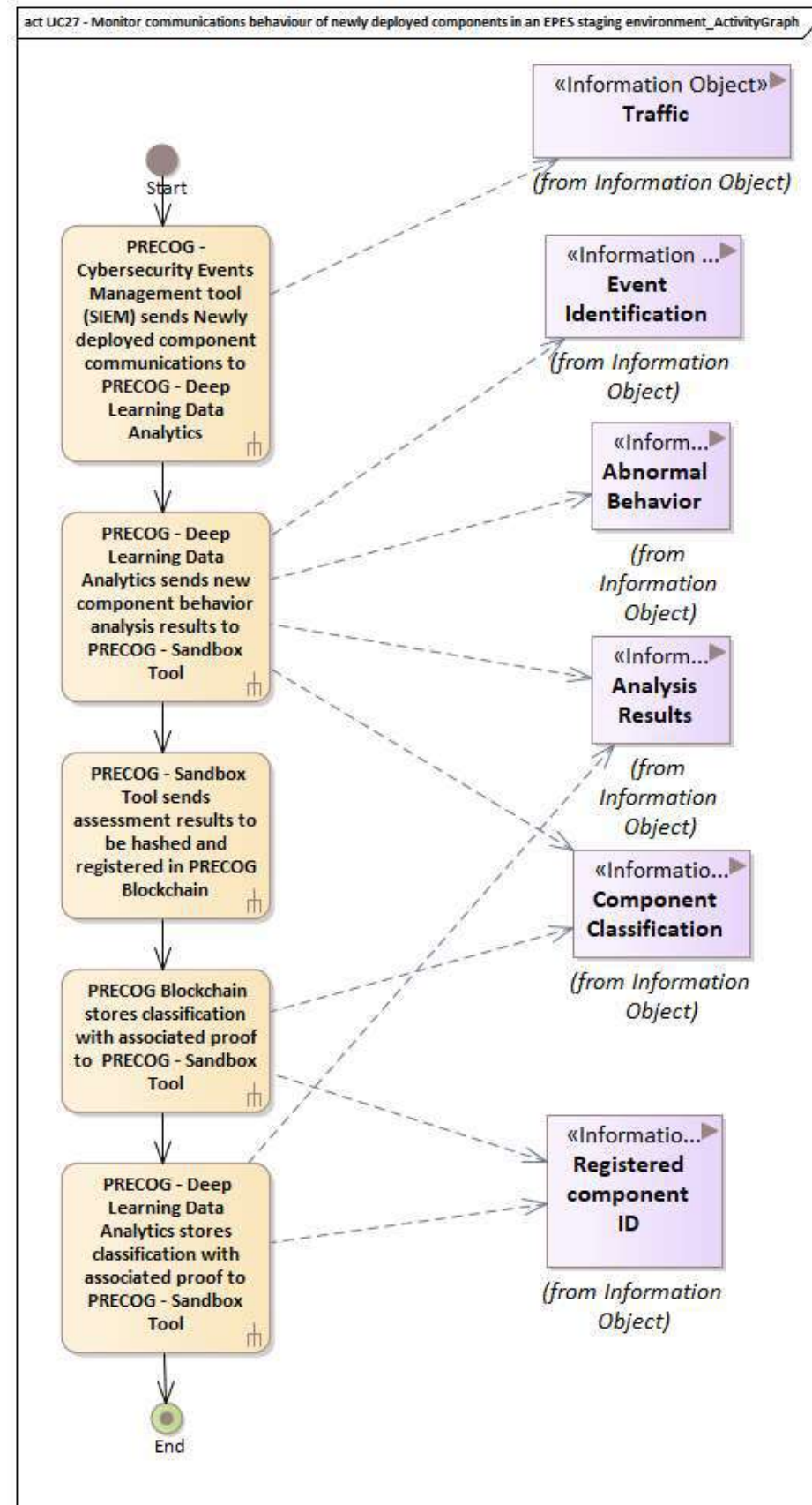


Figure 85 - UC27 Activity Graph

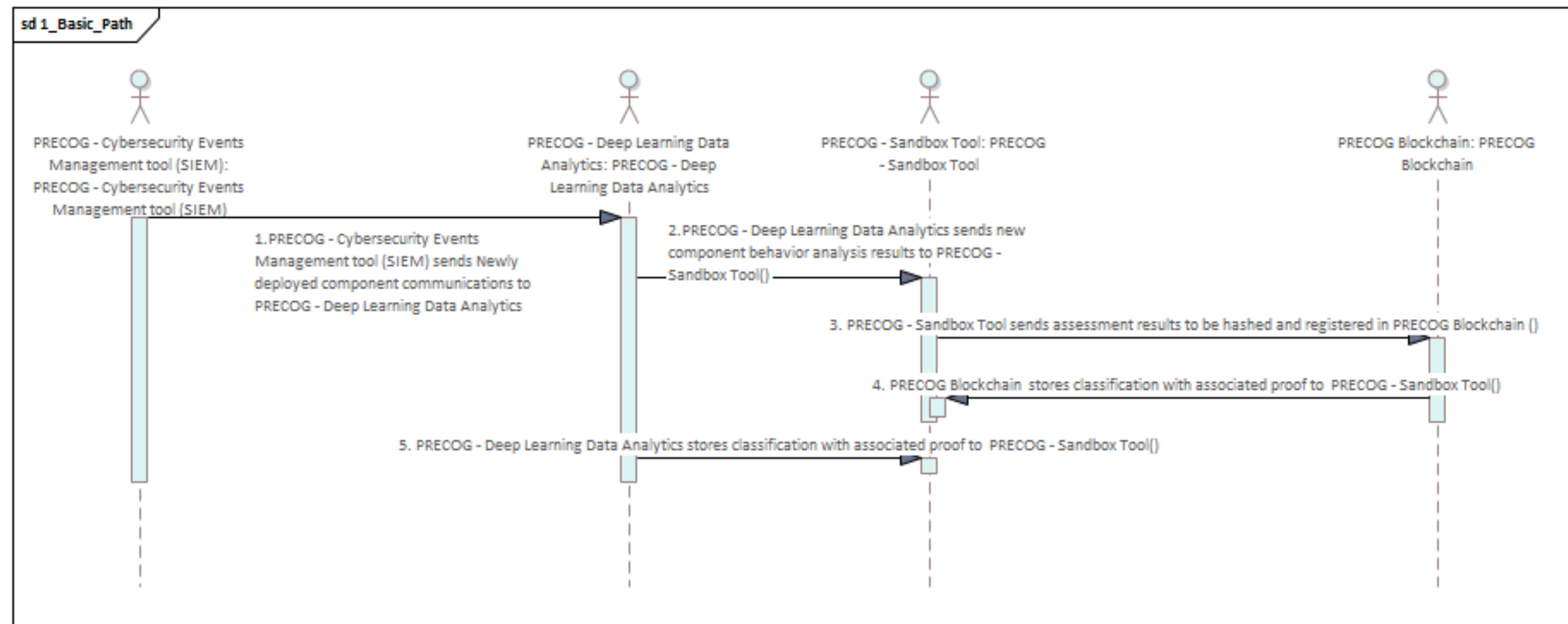


Figure 86 - UC27 Basic Path



UC28 - Adapt/Develop EPES specific vendor management & suppliers' audit practices

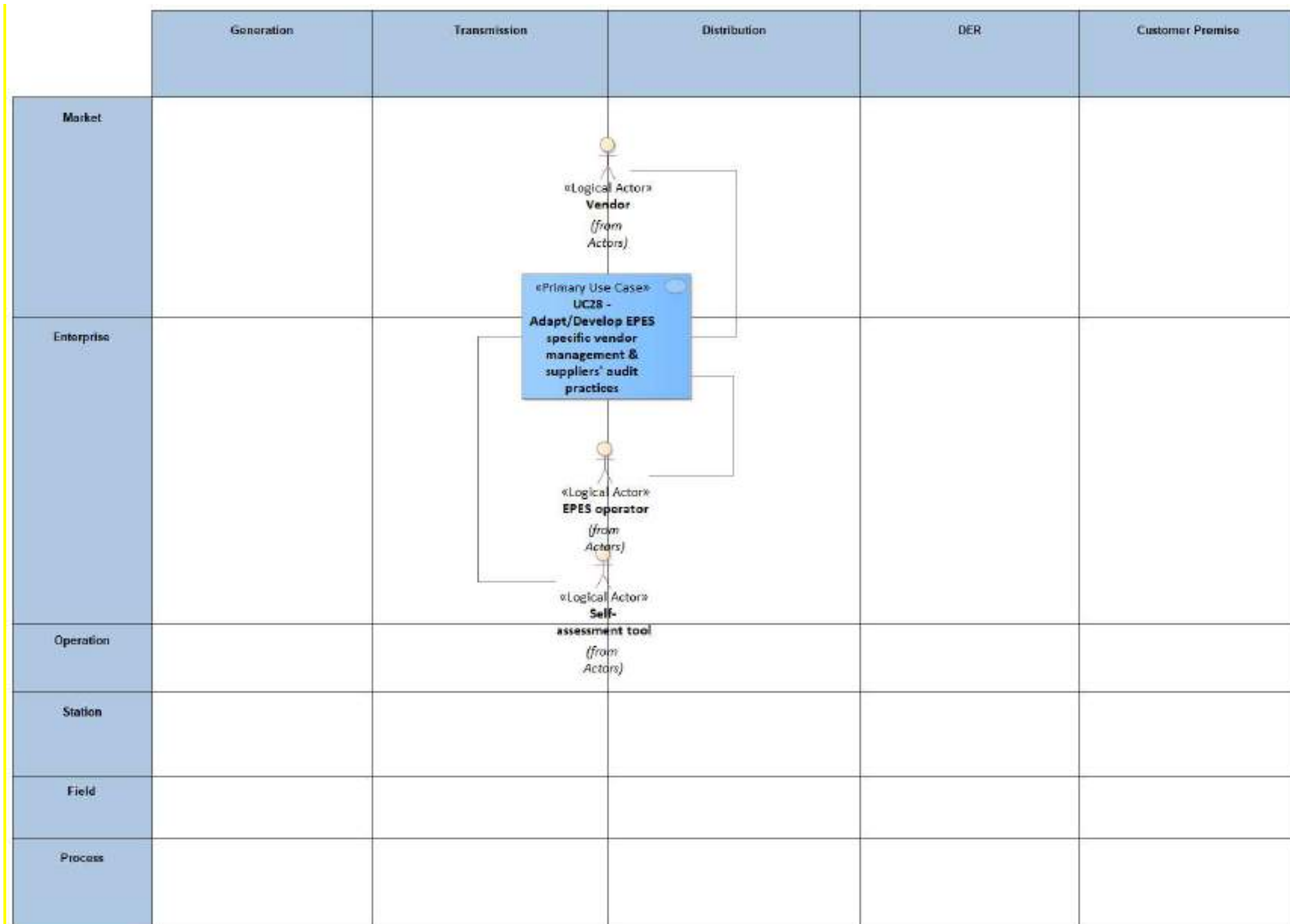


Figure 87 - UC28 Functional Layer

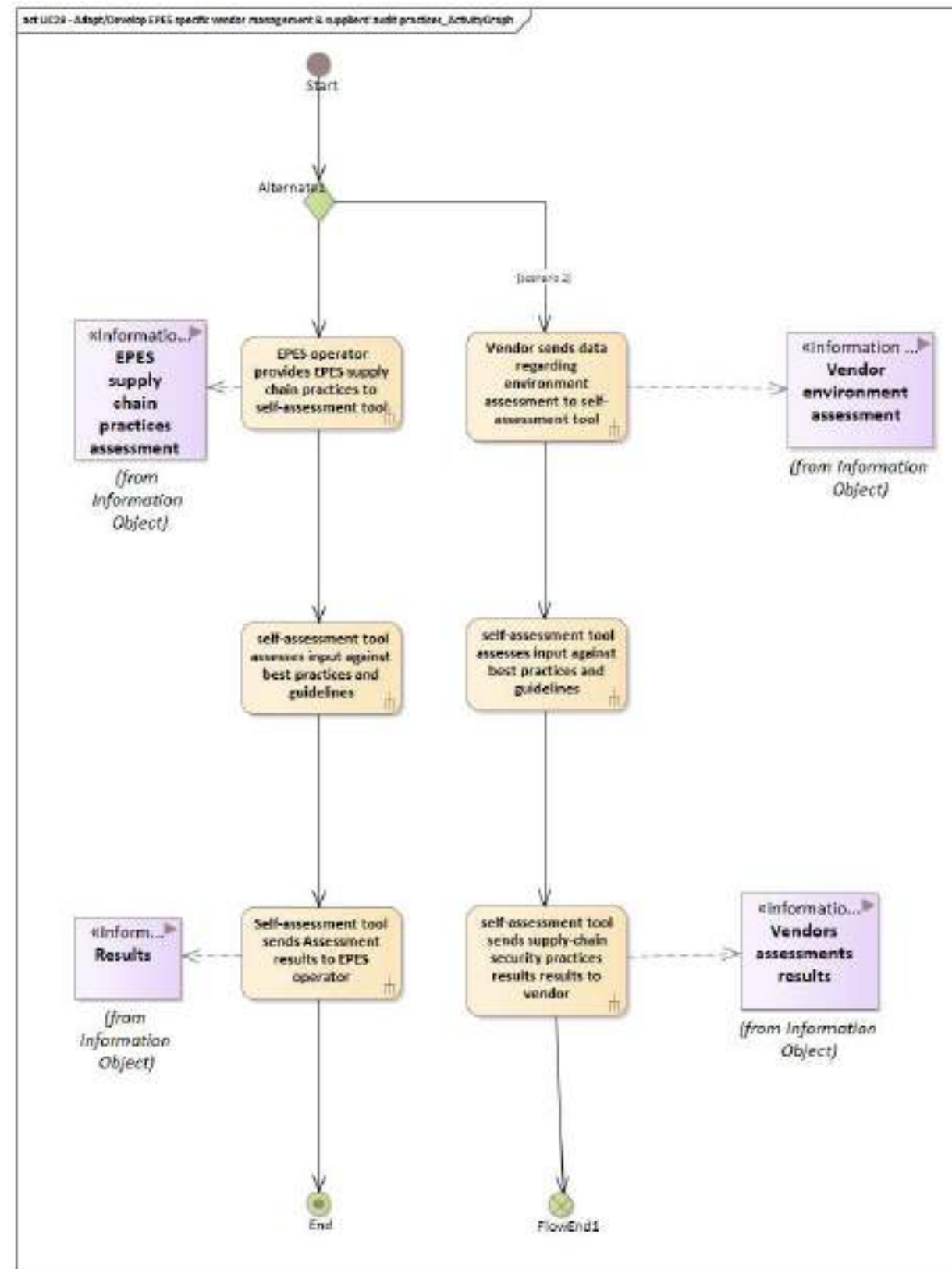


Figure 88 - UC28 Activity Graph

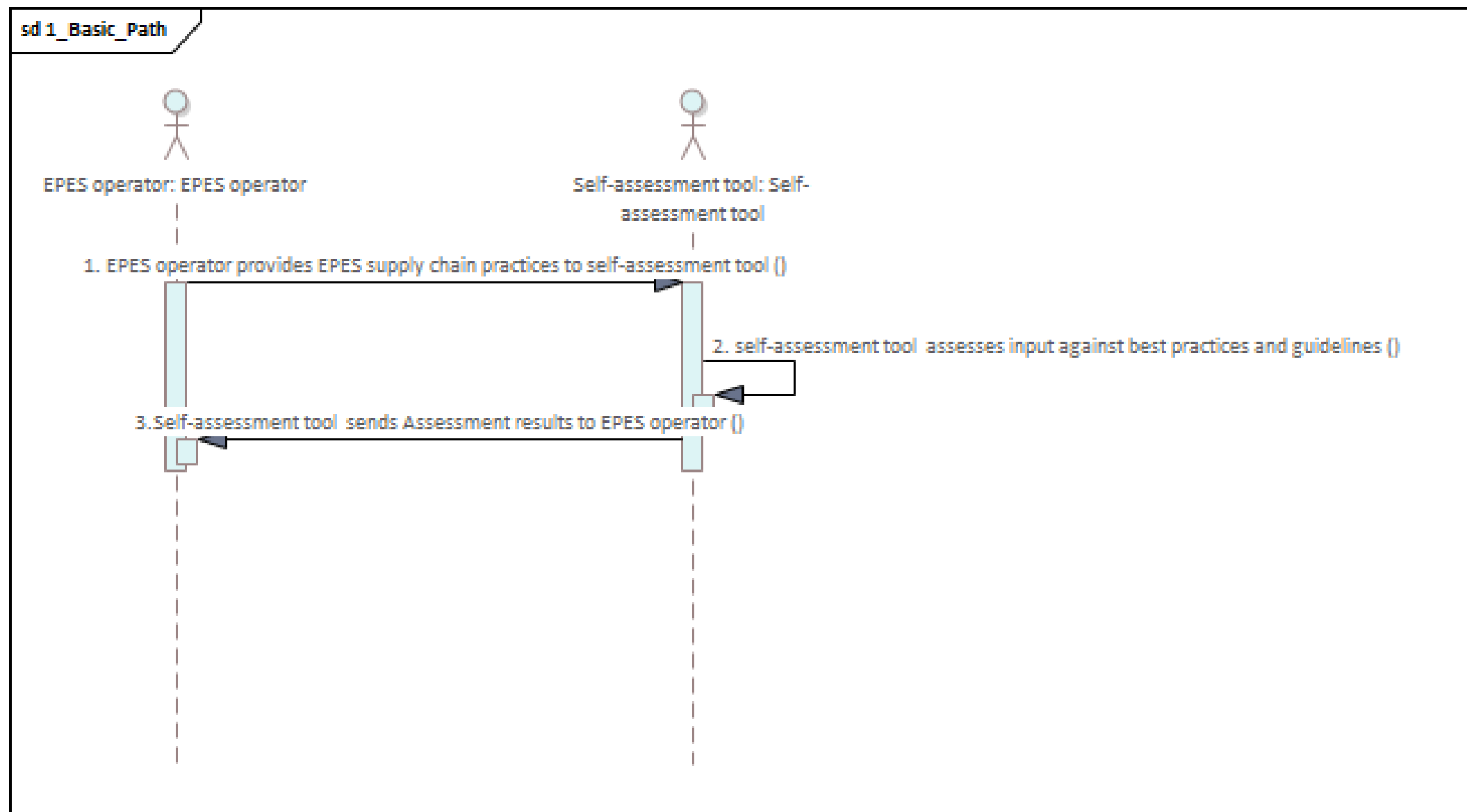


Figure 89 - UC28 Basic Path

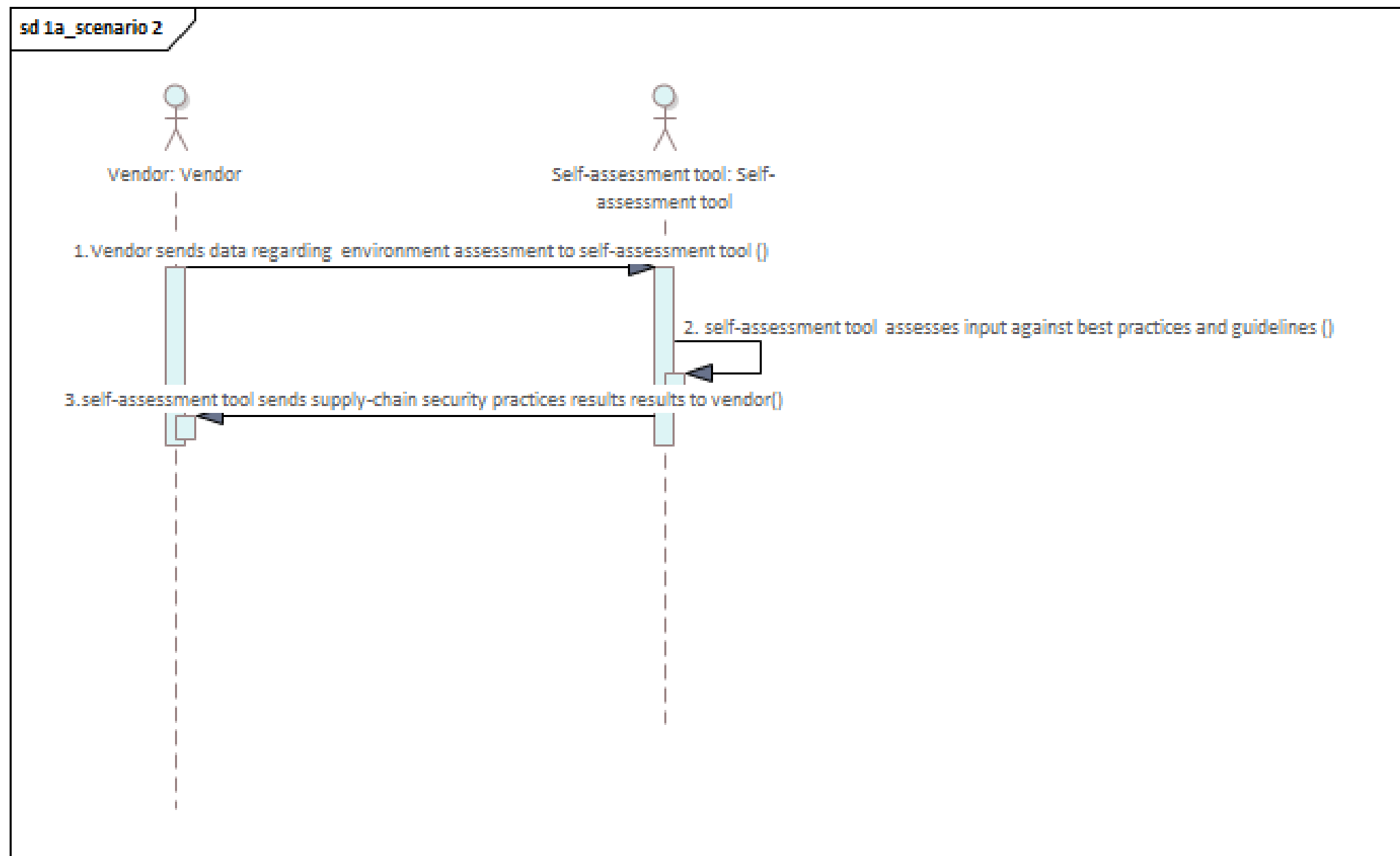


Figure 90 - UC28 Alternative Scenario Basic Path

UC33 - Detection of anomalies associated with cybersecurity through the characterization of traffic in the perimeter, levels of control and supervision, operation and in physical environments

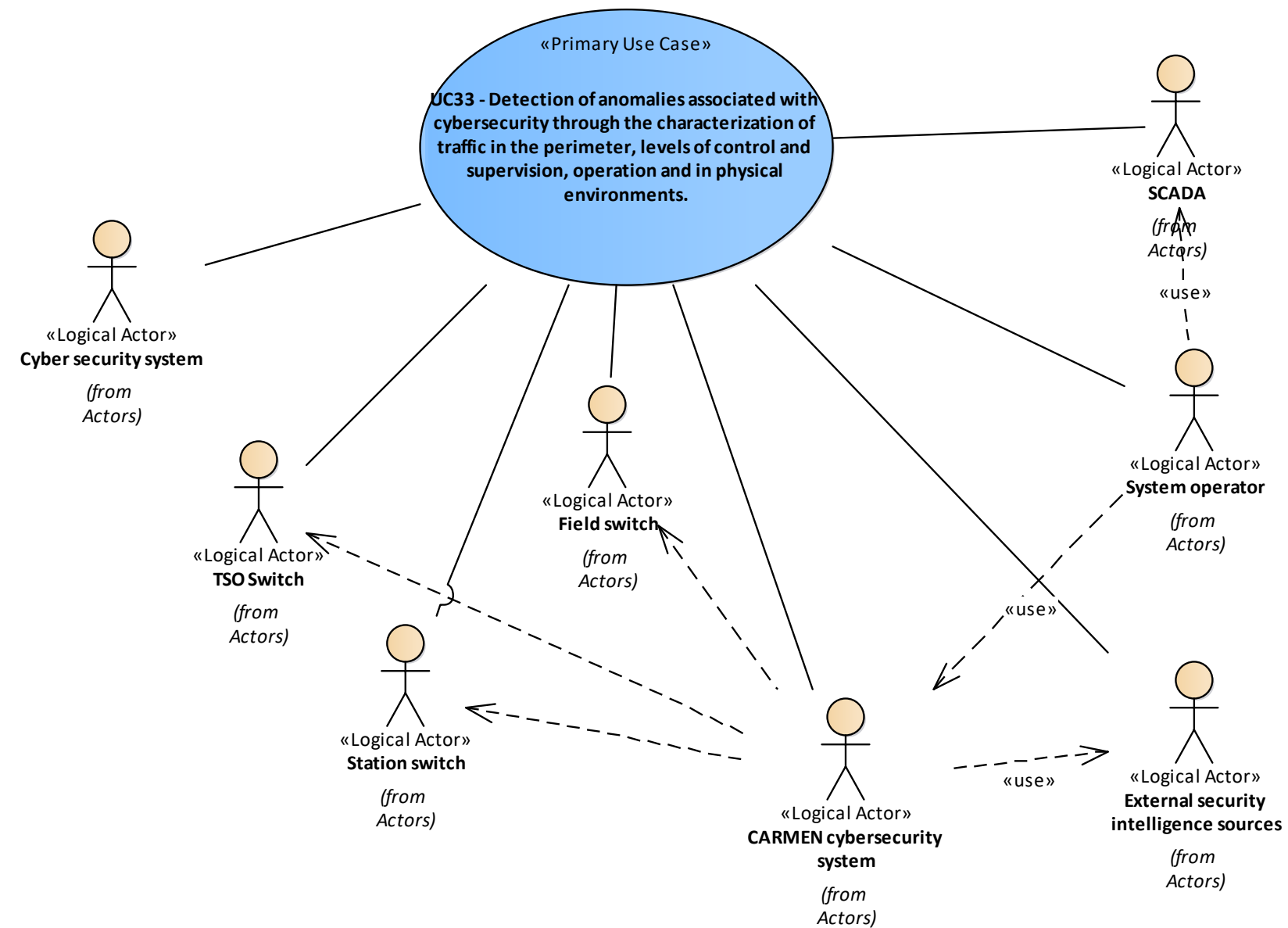


Figure 91 - UC33 Actors involved

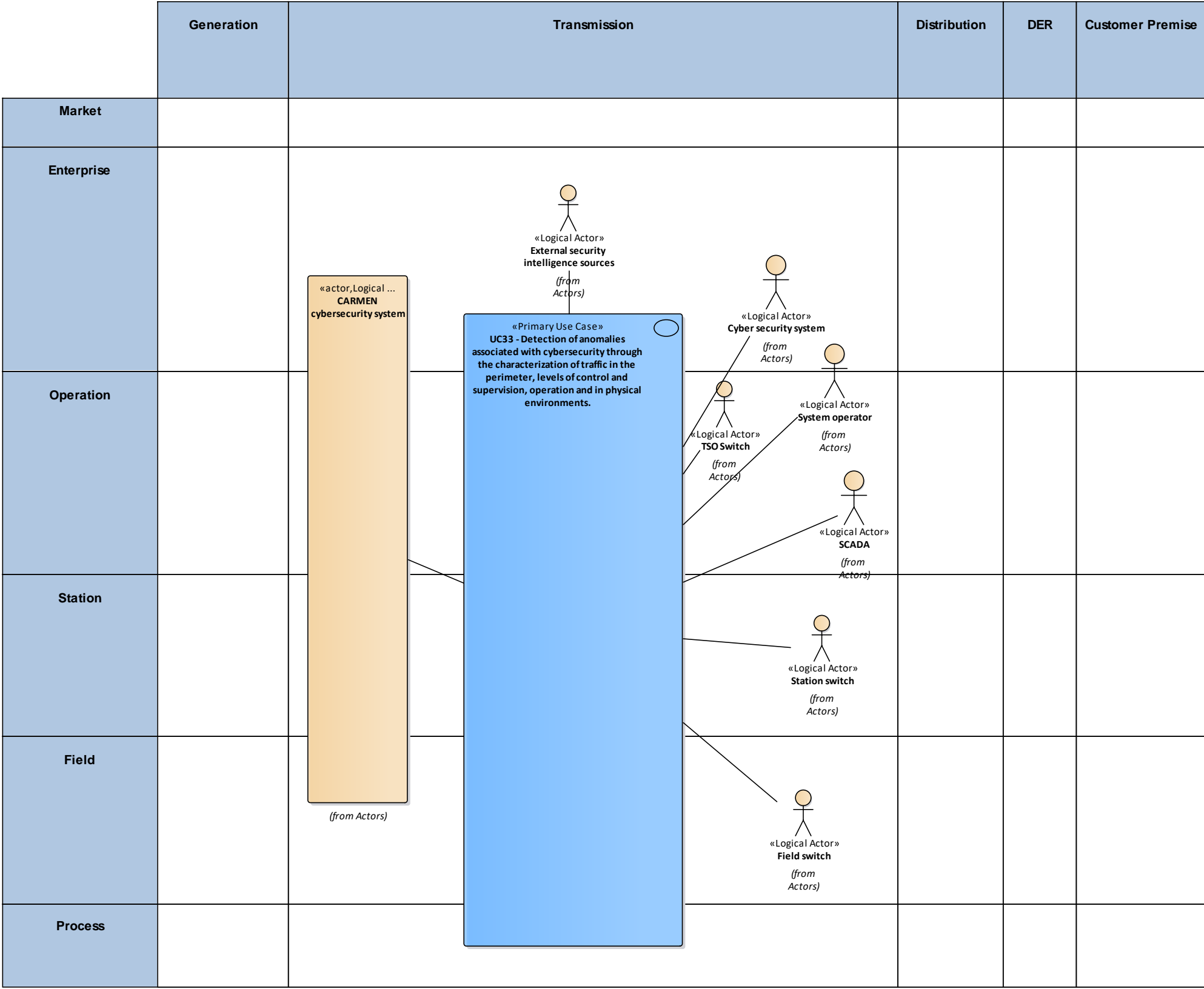


Figure 92 - UC33 Functional Layer

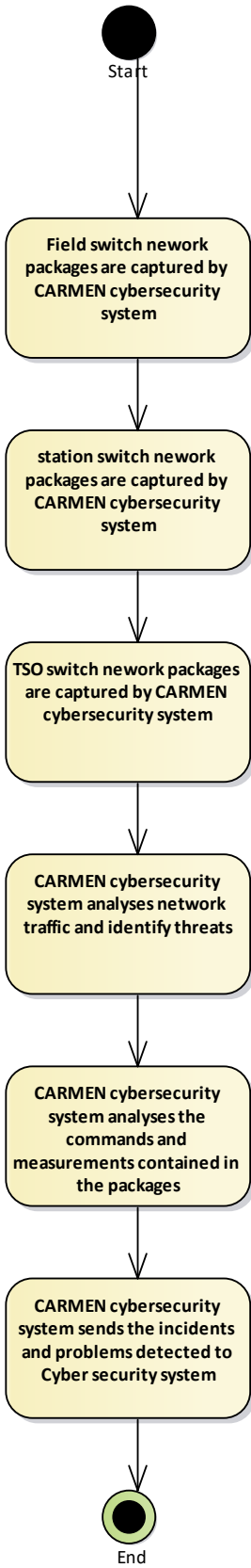


Figure 93 – UC33 Activity Graph

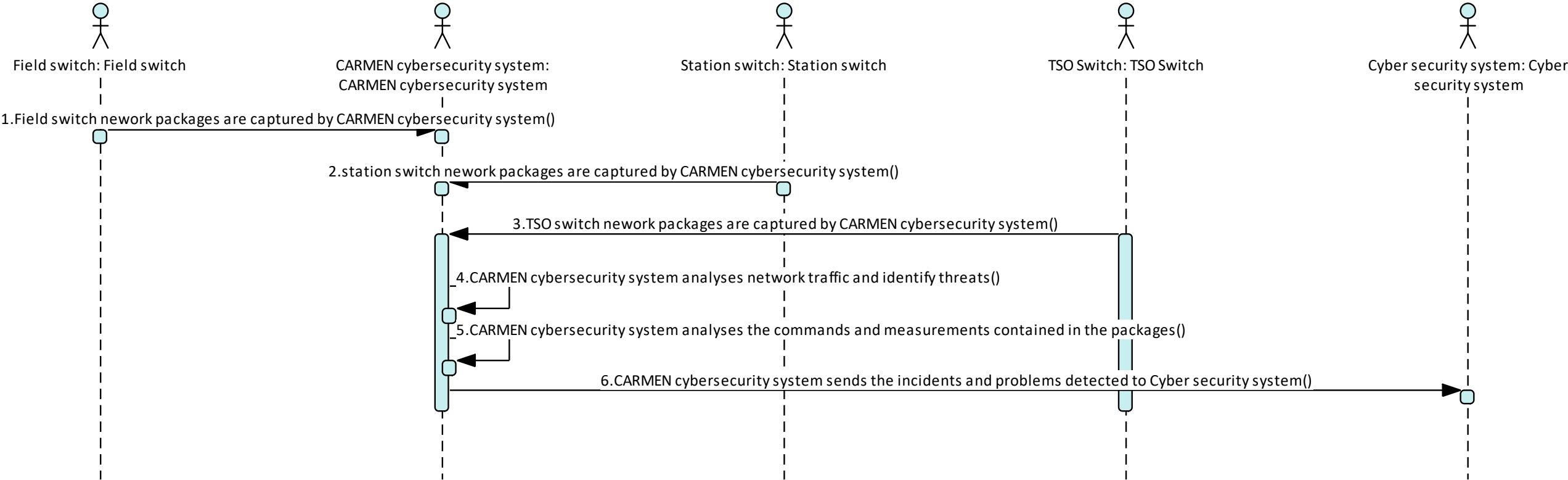


Figure 94 - UC33 Basic Path

UC34 - Pattern detection and correlation with information from other cyberattacks in order to detect potential threats

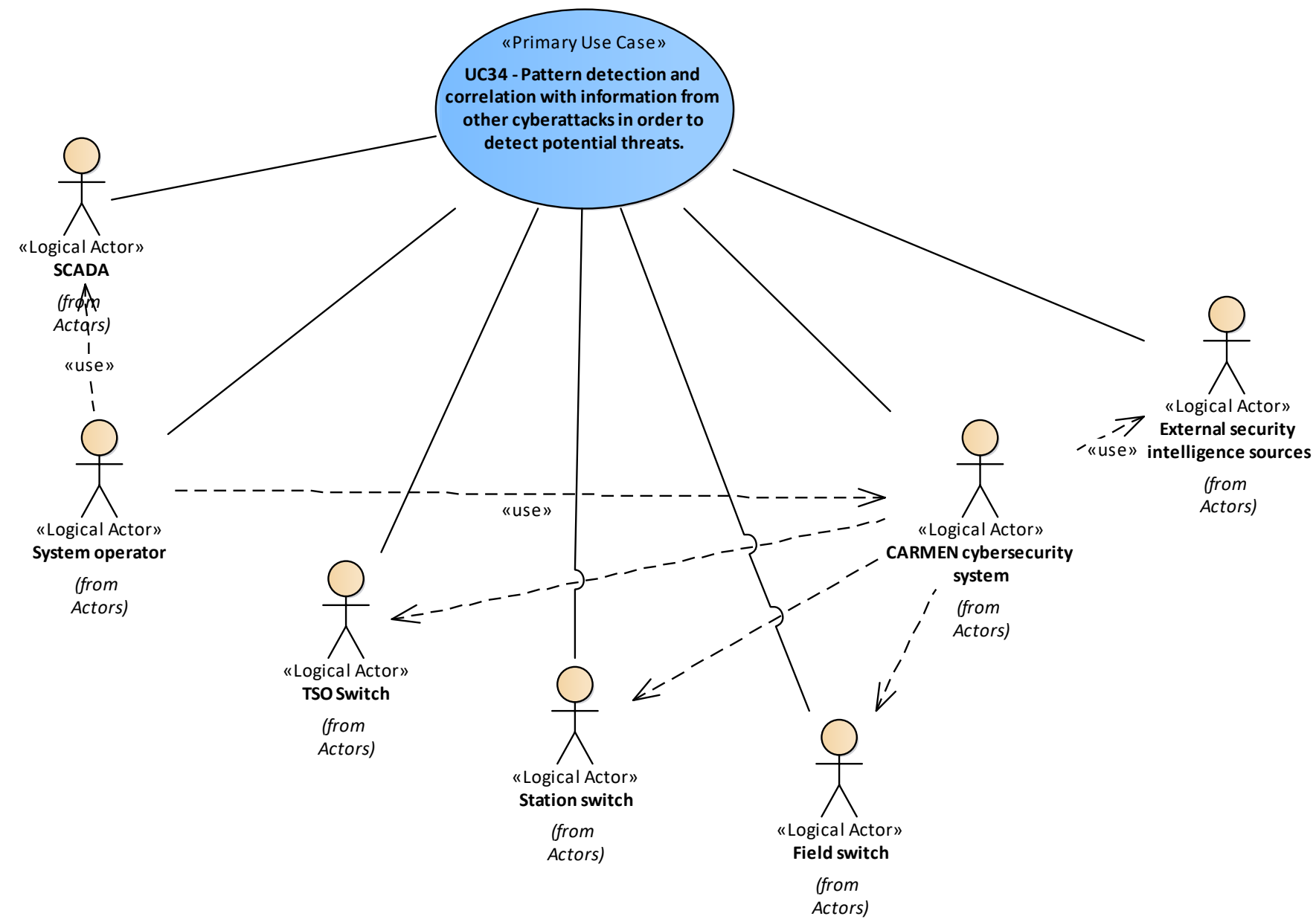


Figure 95 - UC34 Actors Involved

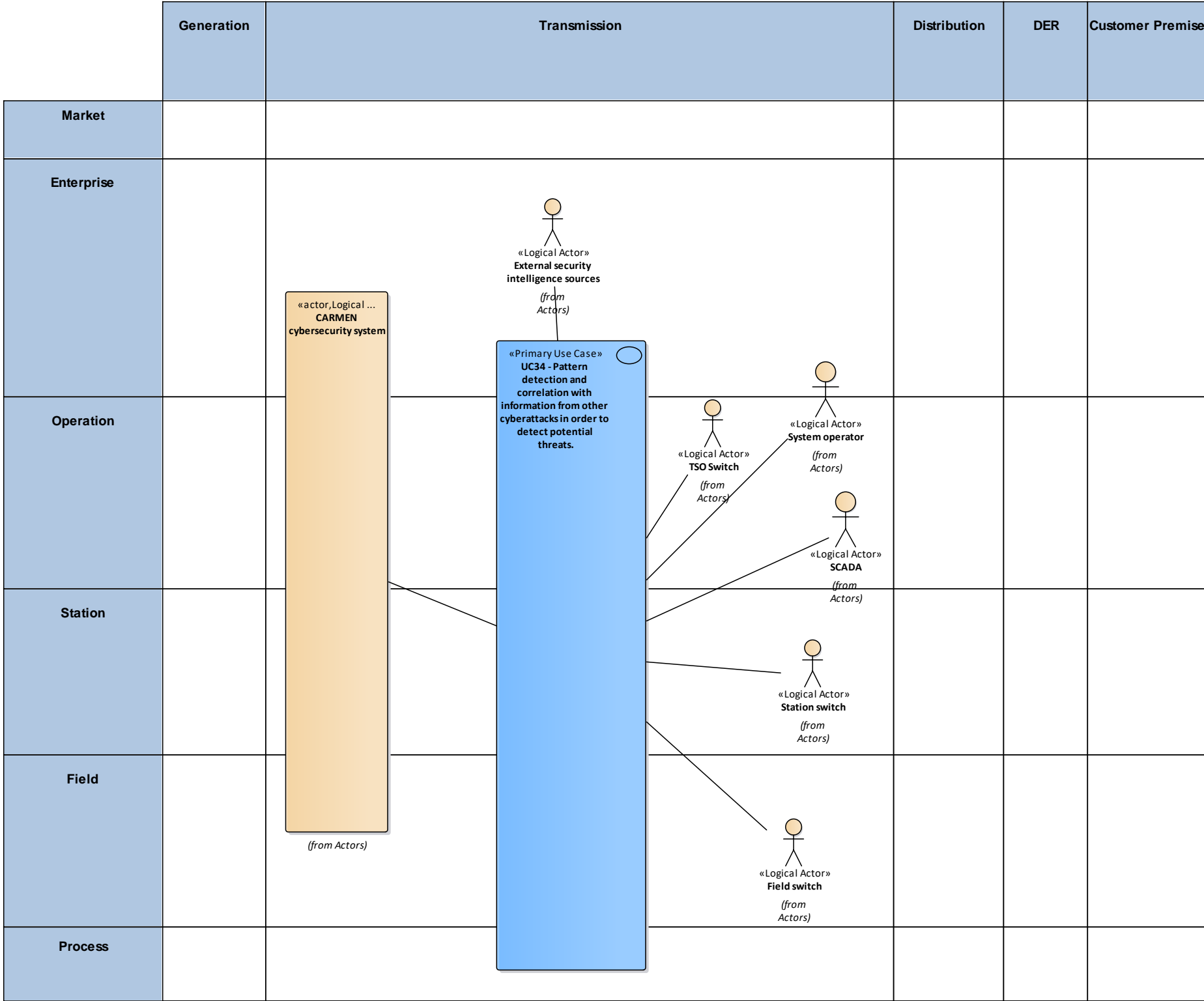


Figure 96 - UC34 Functional Layer

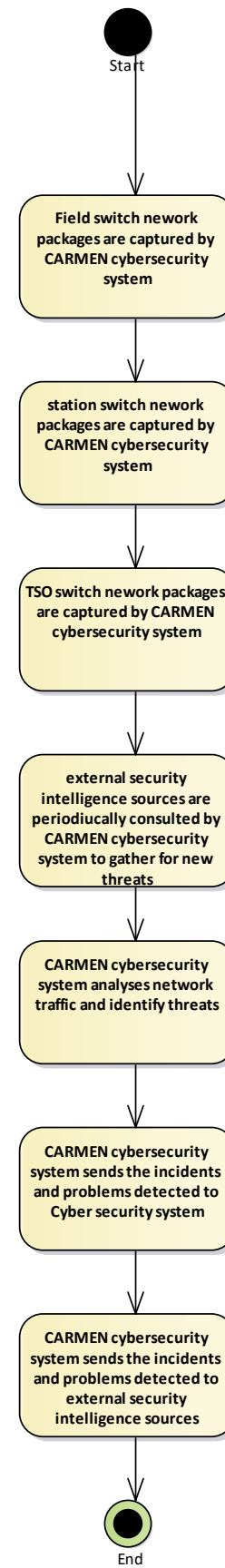


Figure 97 – UC34 Activity Graph

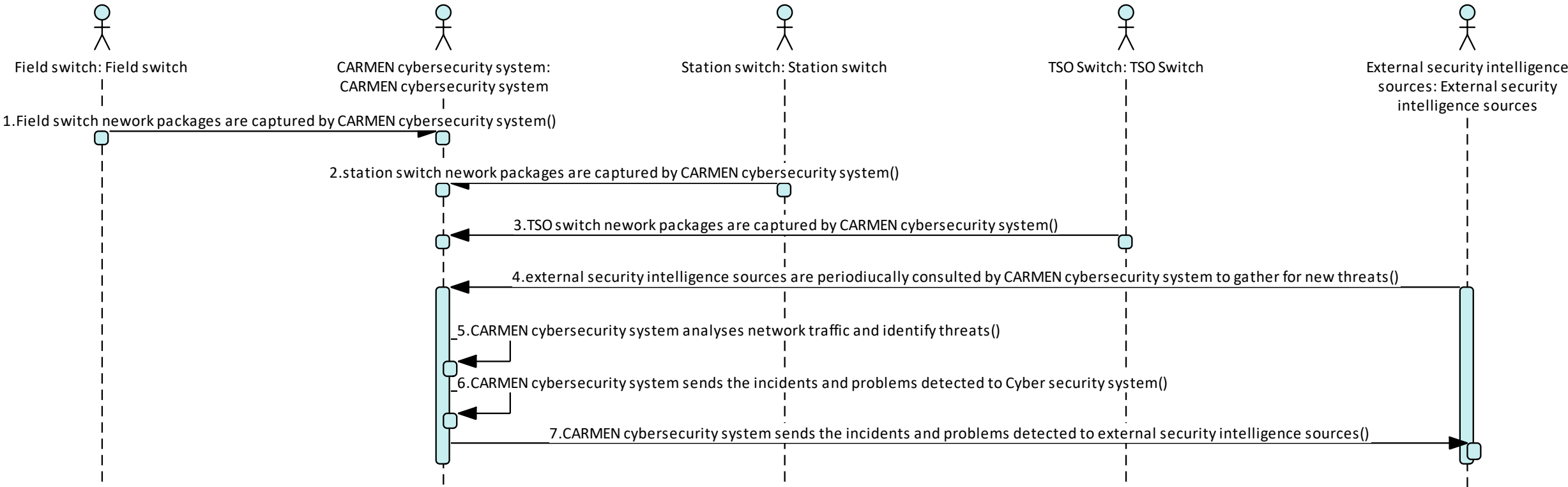


Figure 98 - UC34 Basic Path

UC36 - Validation of network model integrity

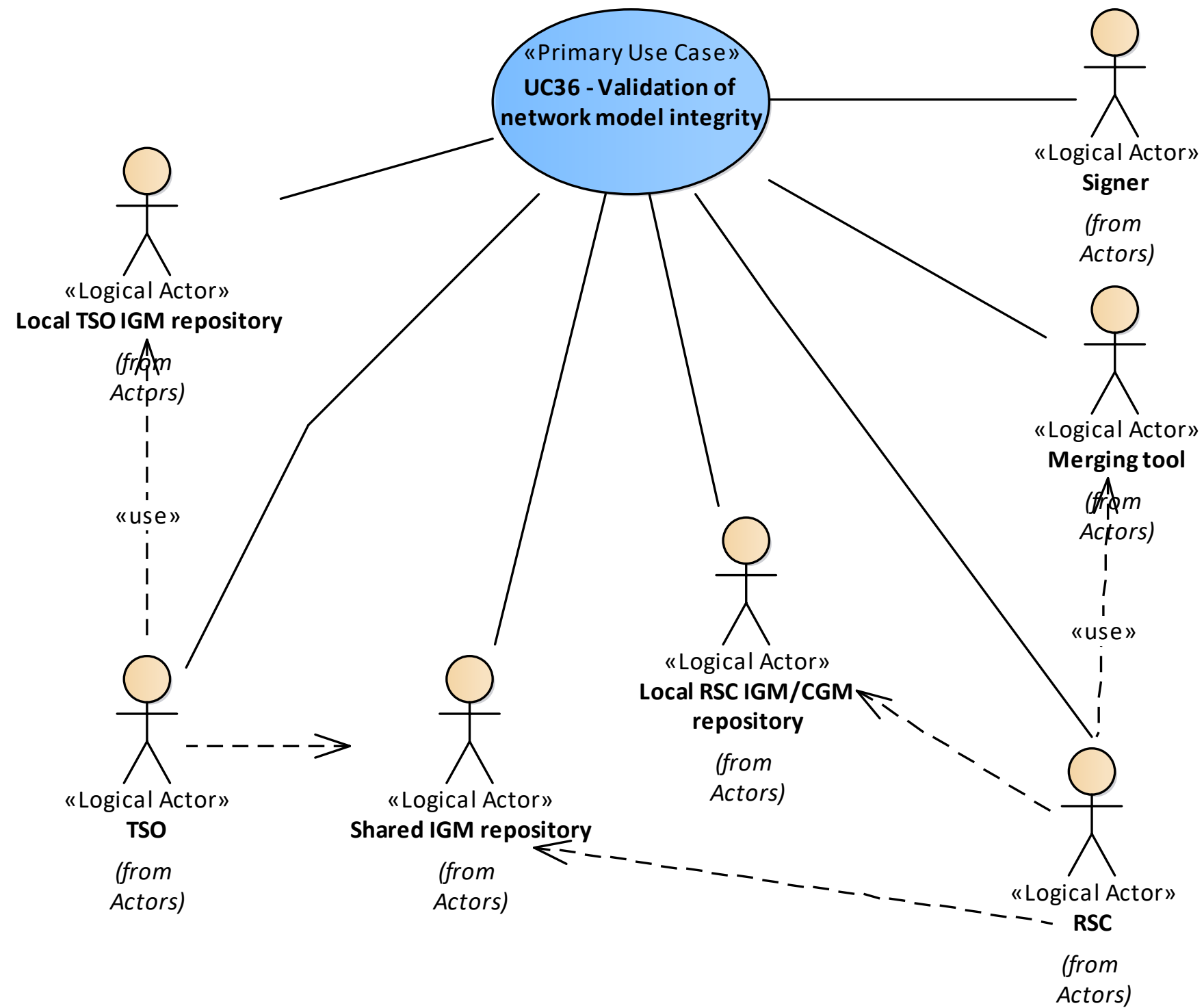


Figure 99 - UC36 Actors Involved

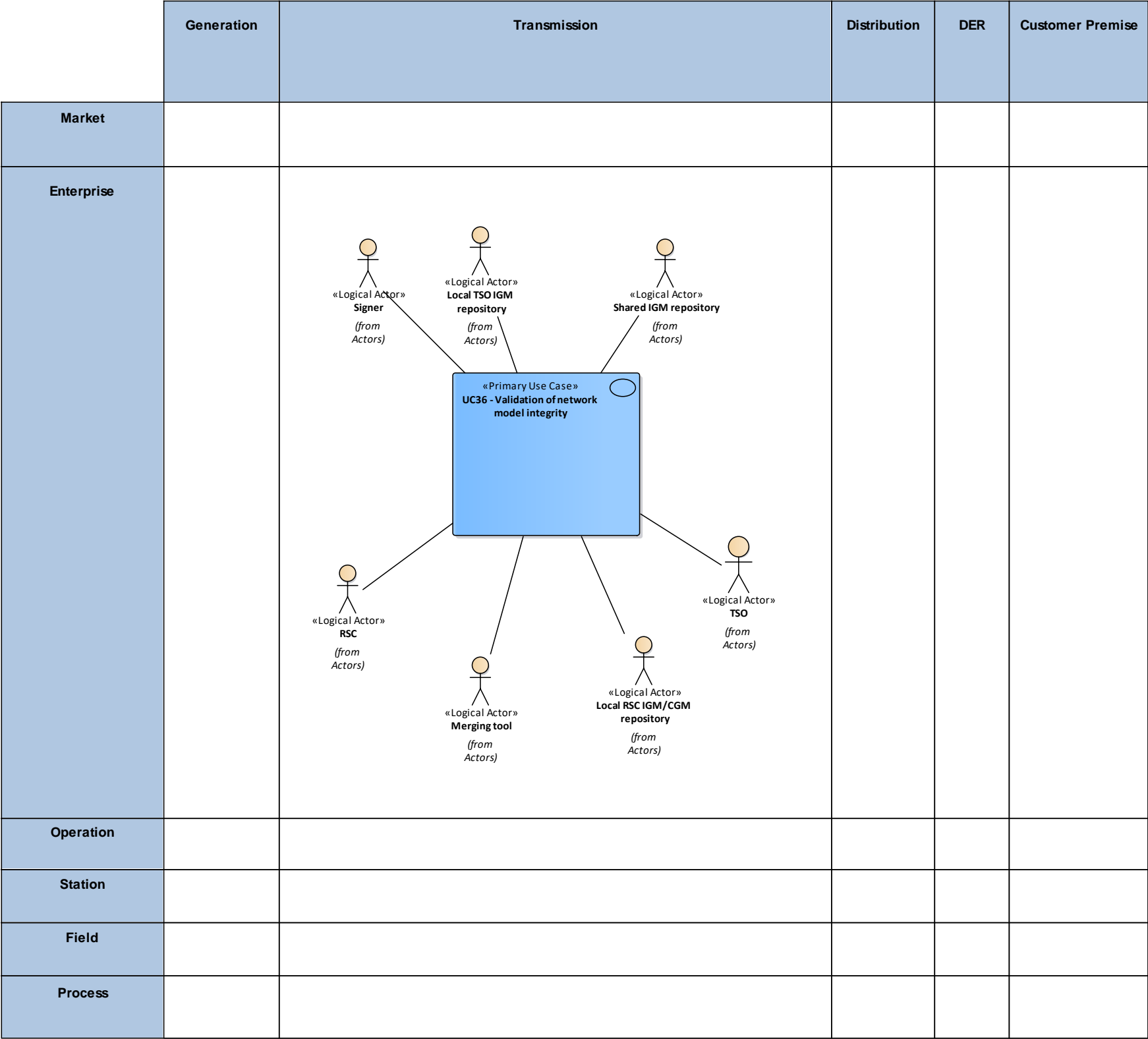


Figure 100 - UC36 Functional Layer

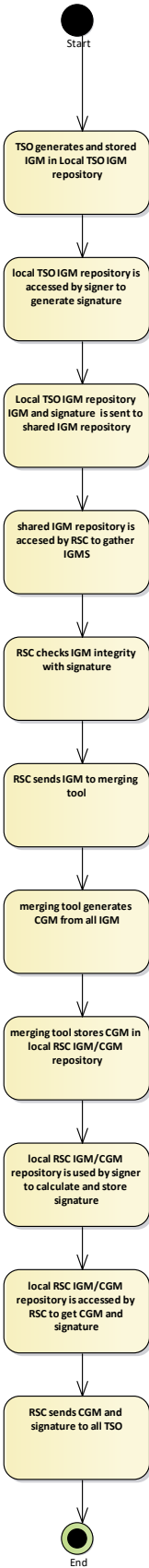


Figure 101 - UC36 Activity Graph

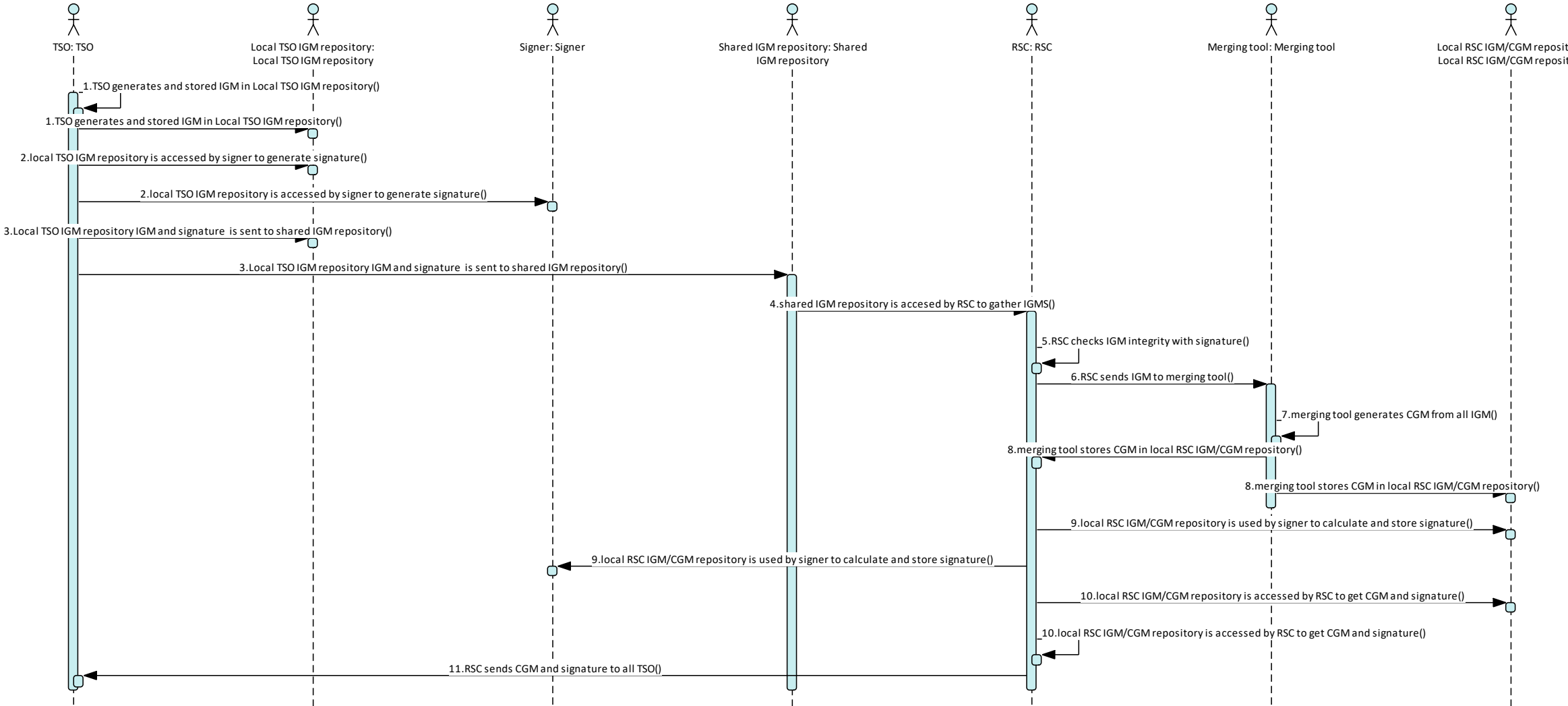


Figure 102 - UC36 Basic Path

UC37 - Energy data tokenization

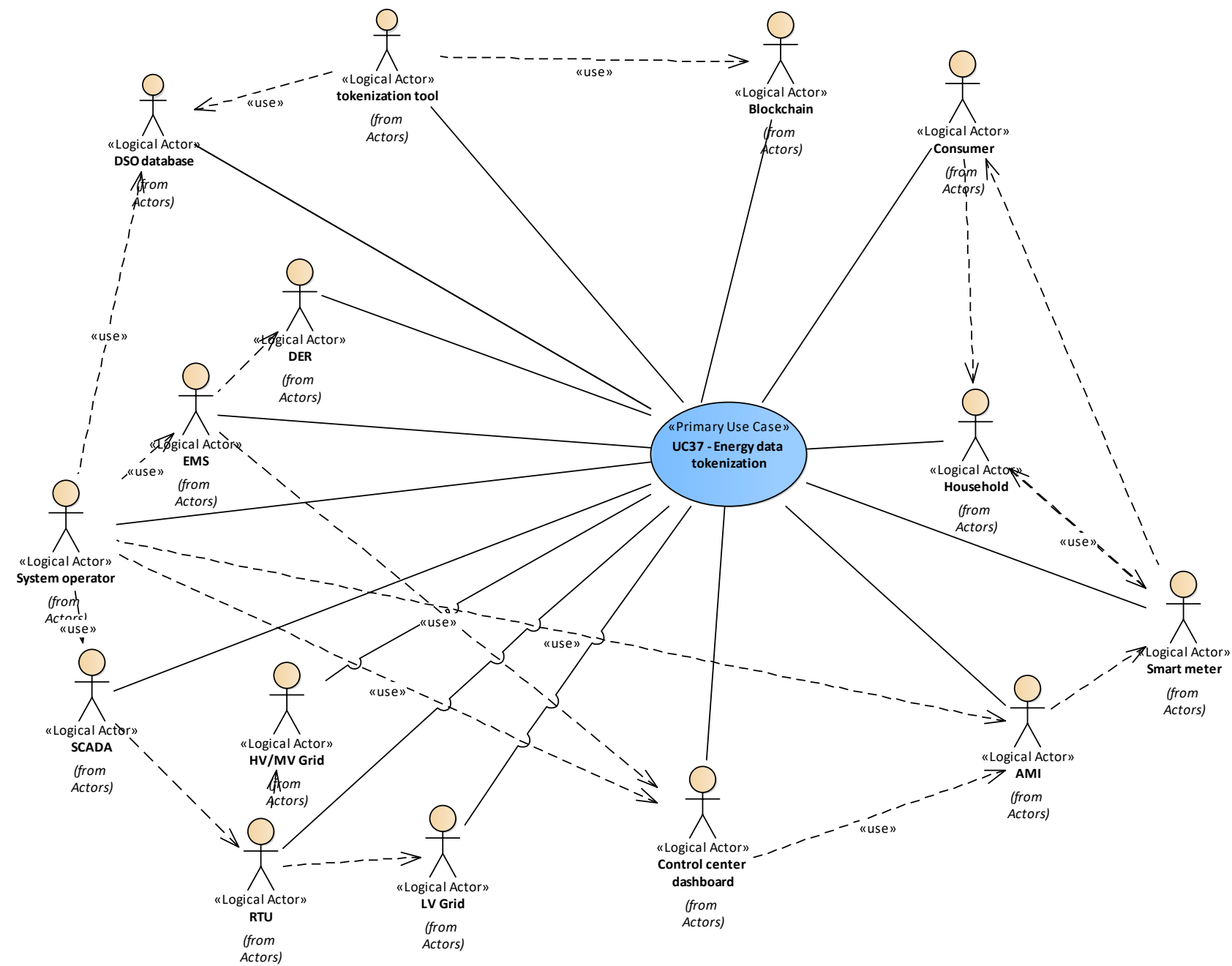


Figure 103 - UC37 Actors Involved

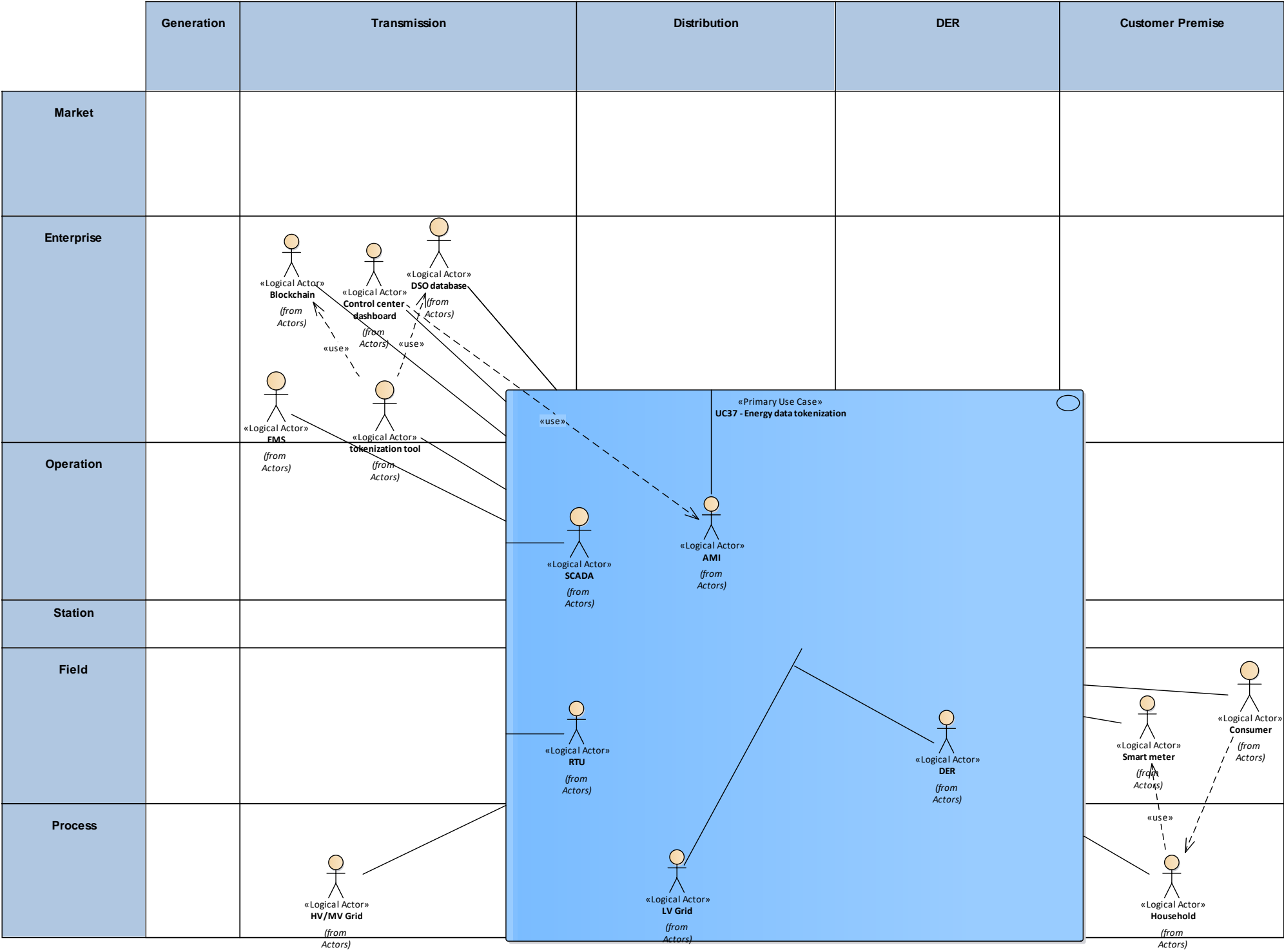


Figure 104 - UC37 Functional Layer

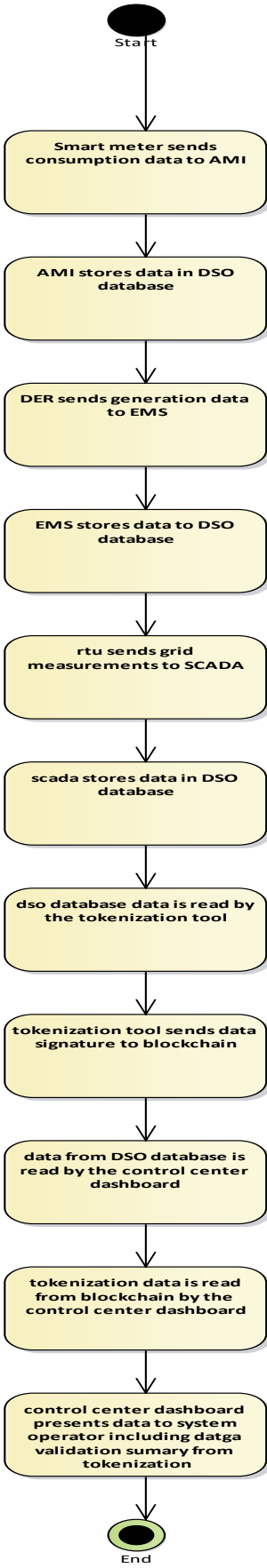


Figure 105 - UC37 Activity Graph

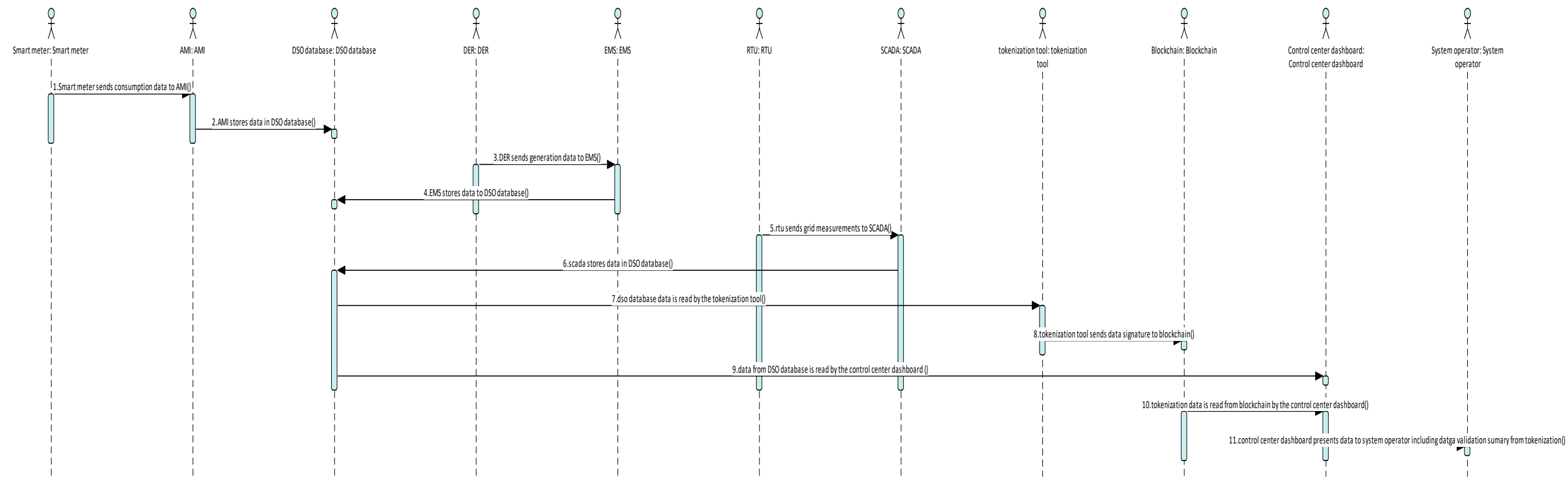


Figure 106 – UC37 Basic Path



UC38 - DSO grid balancing data tokenization

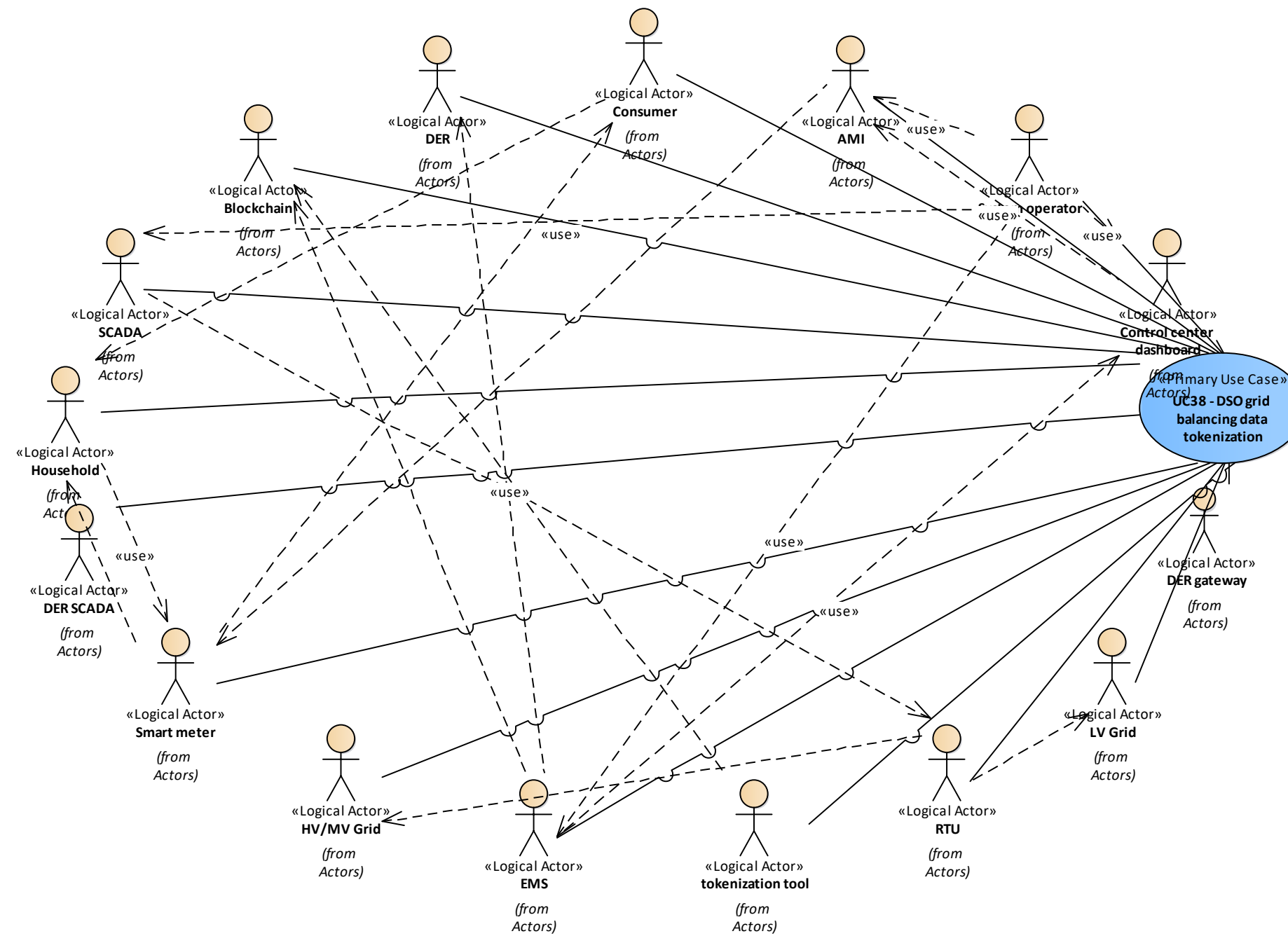


Figure 107 - UC38 Actors Involved

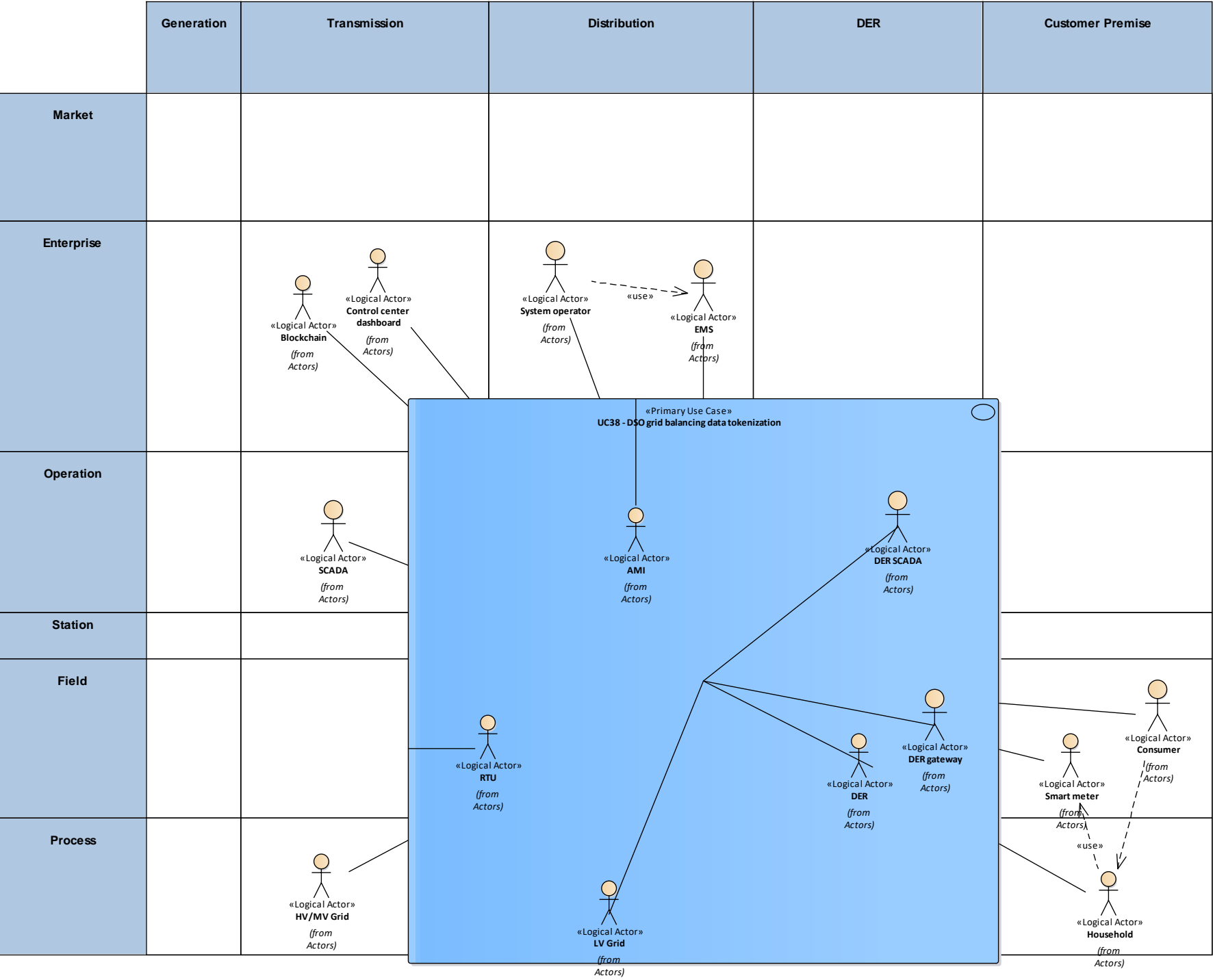


Figure 108 - UC38 Functional Layer

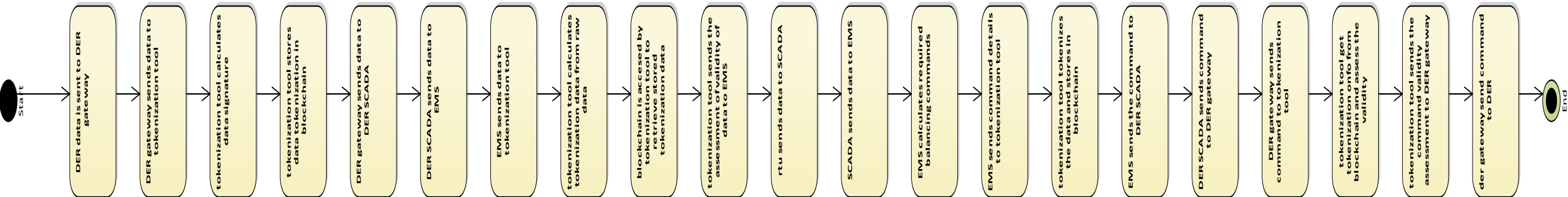


Figure 109 - UC38 Activity Graph

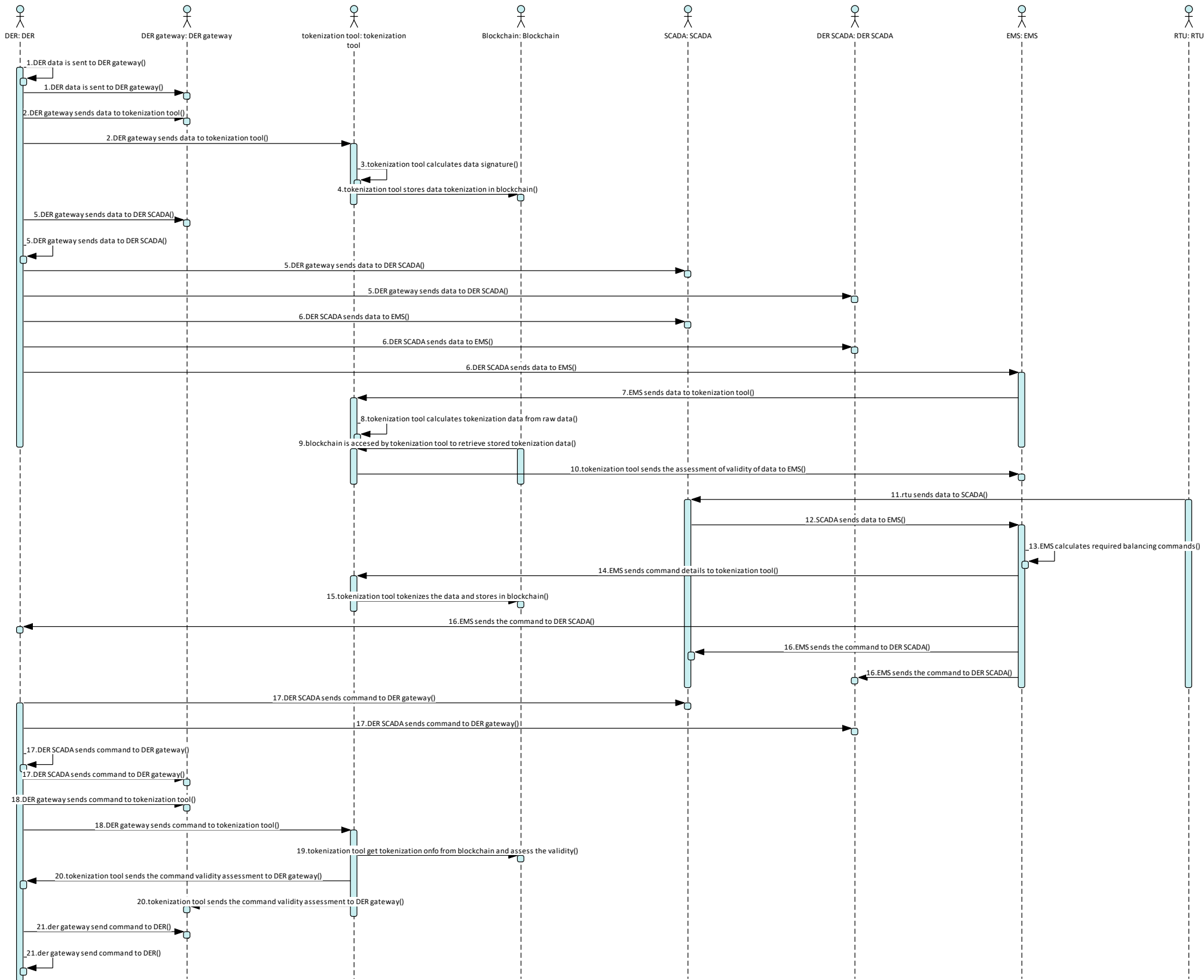


Figure 110 - UC38 Basic Path

UC40 - IoT data security enforcement

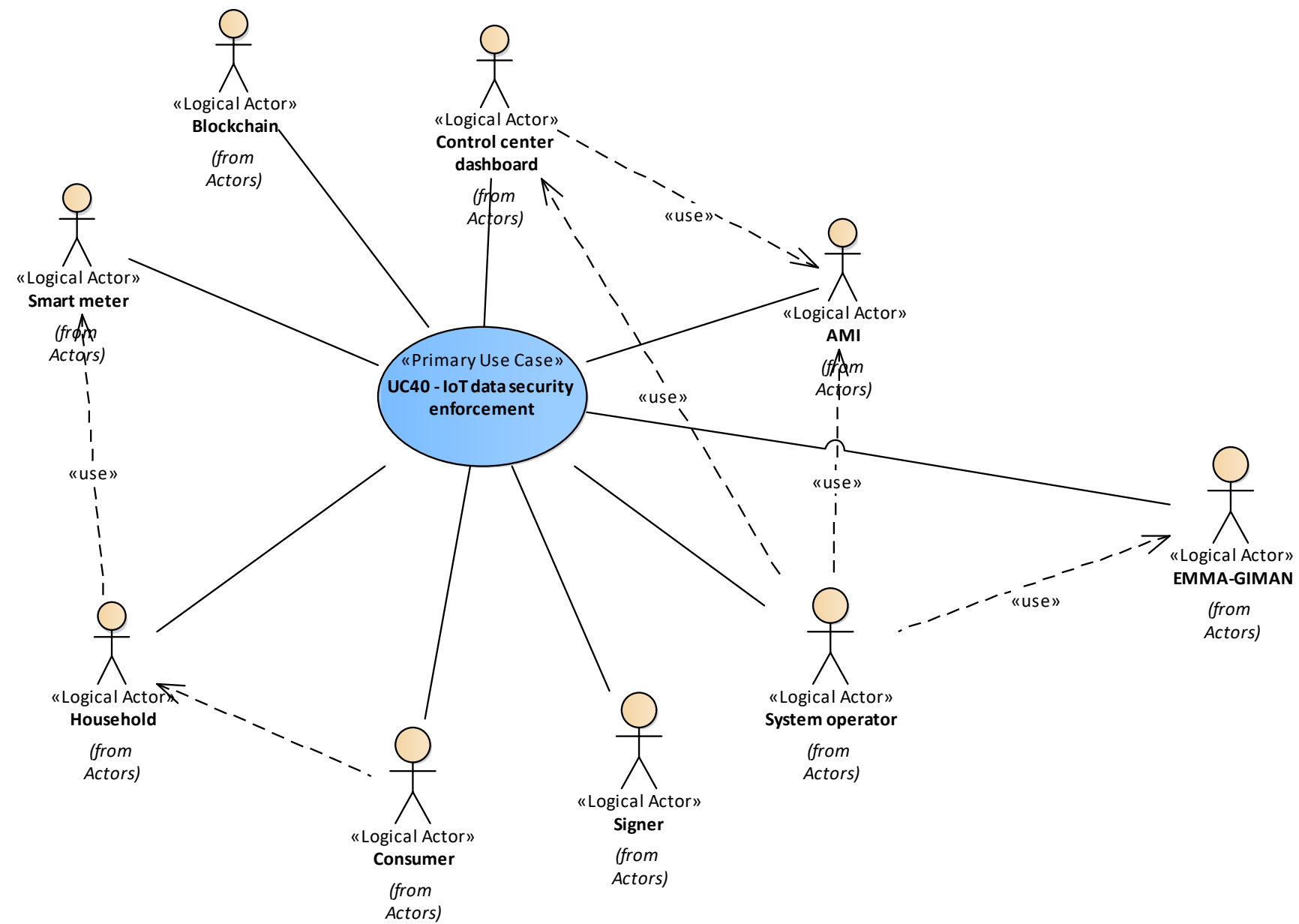


Figure 111 - UC40 Actors Involved

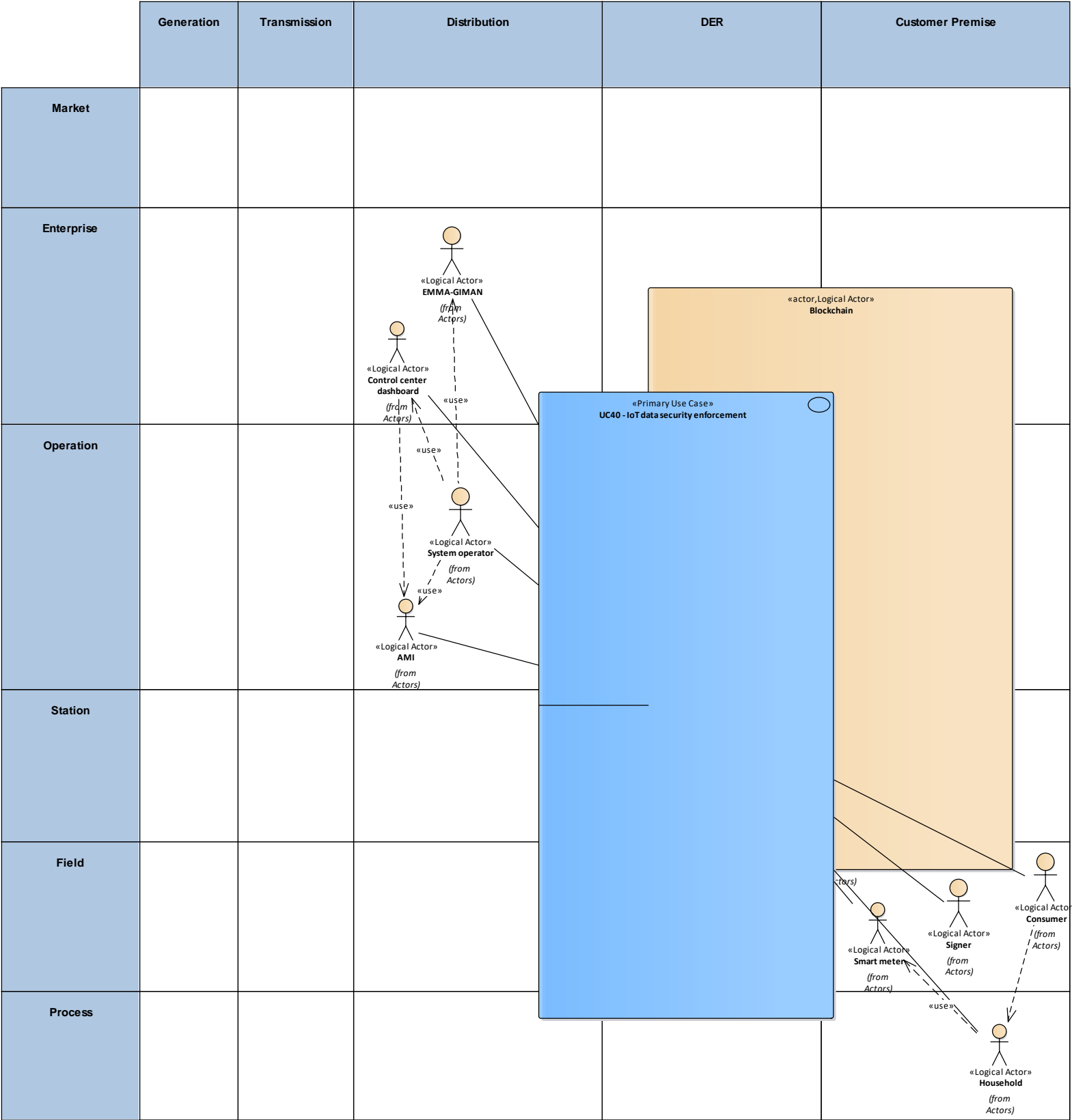


Figure 112 - UC40 Functional Layer

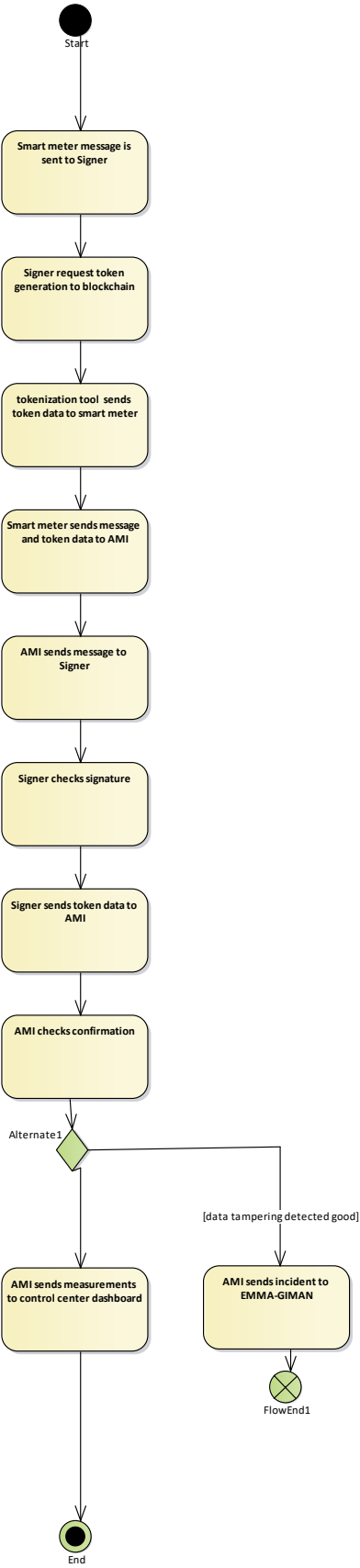


Figure 113 – UC40 Activity Graph

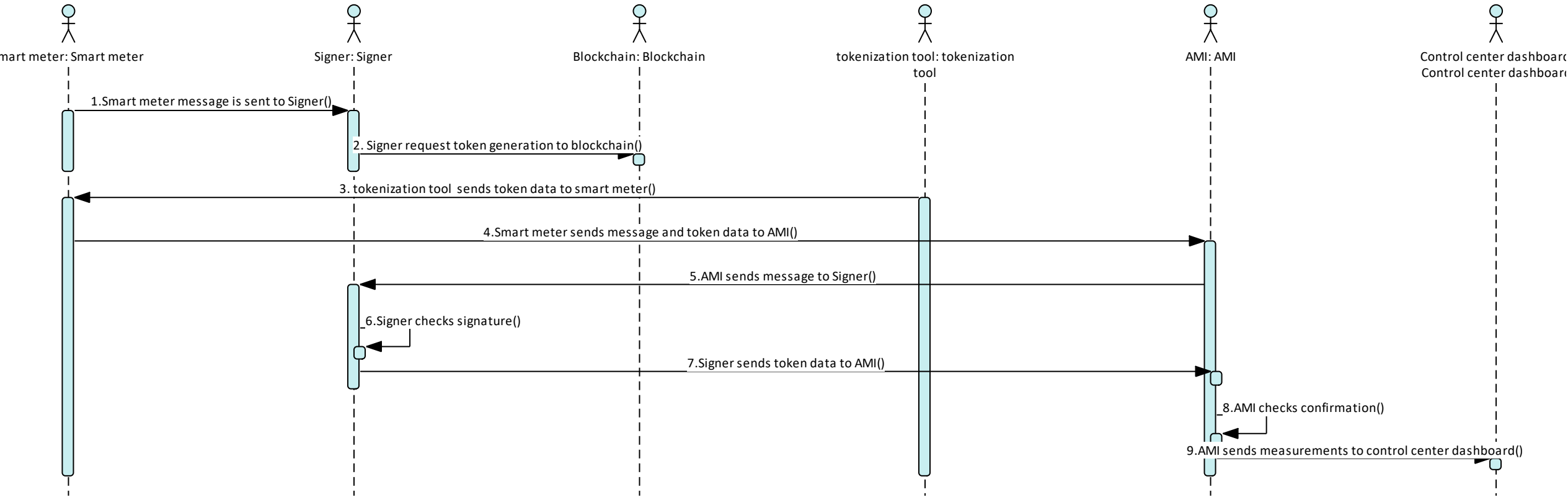


Figure 114 - UC40 Basic Path

13.1.4 WP6-EMMA

UC01 - Improvement in overhead power lines inspection and maintenance using IA applied to UAV-captured images and data

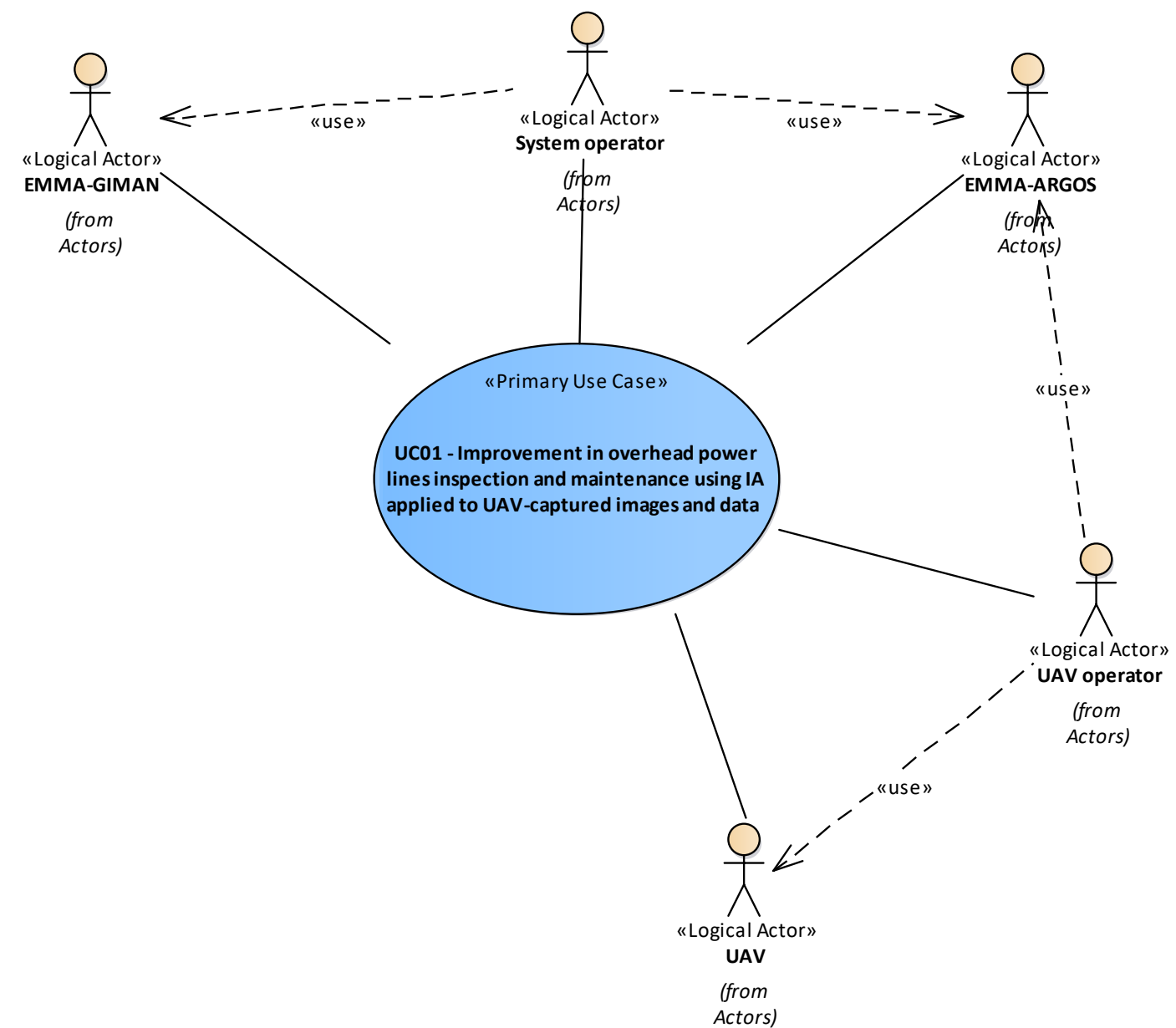


Figure 115 - UC01 Actors Involved

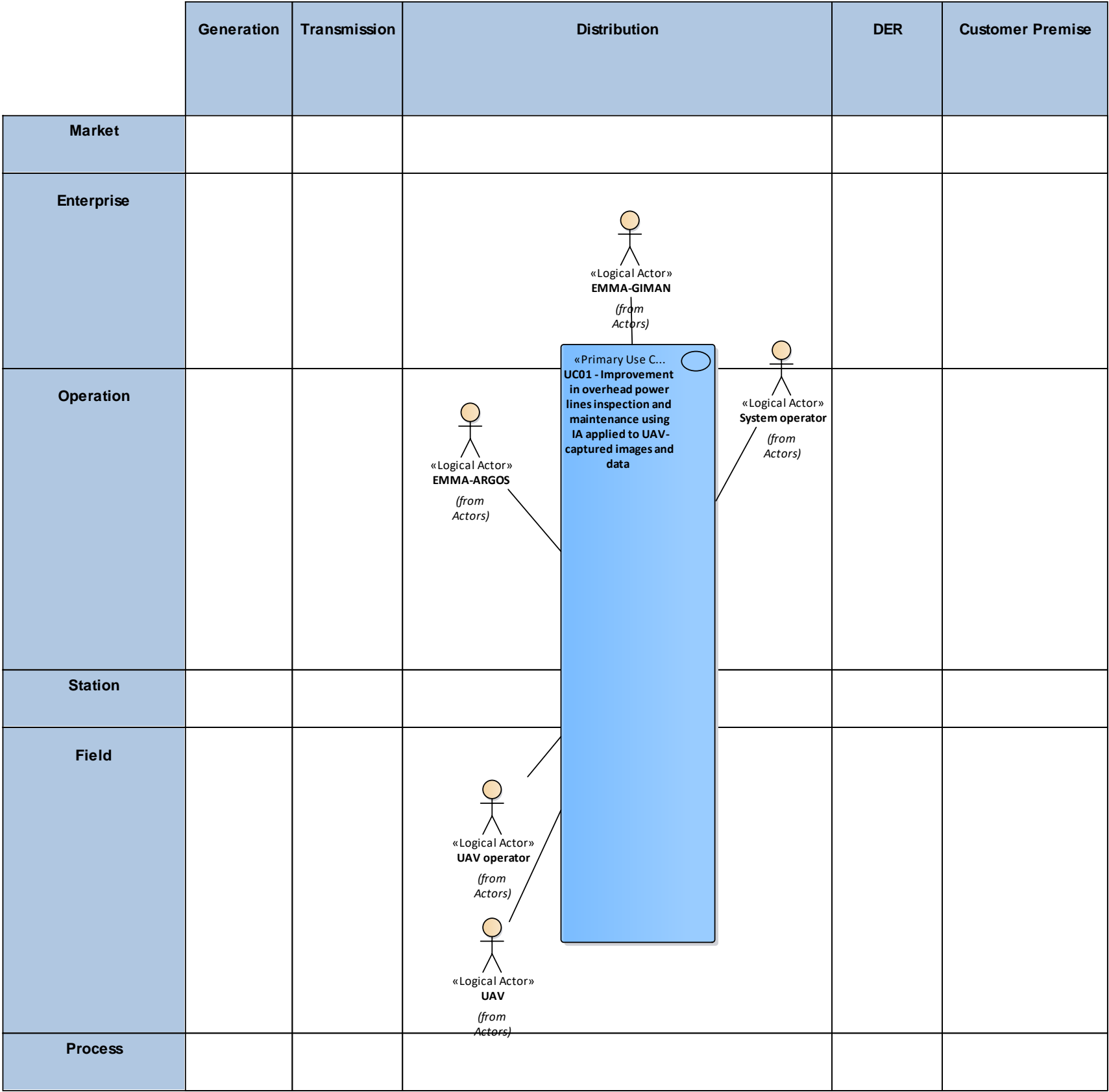


Figure 116 - UC01 Functional Layer

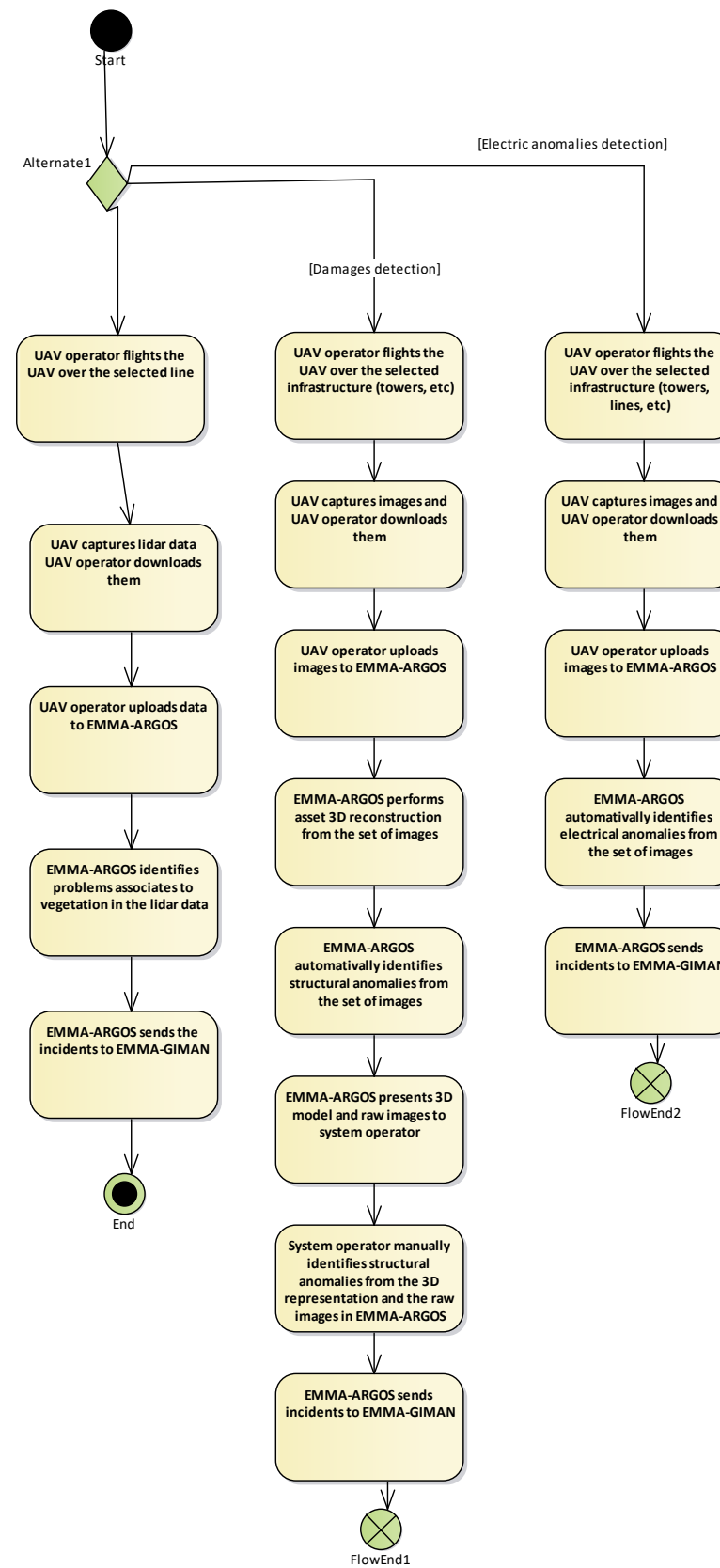


Figure 117 – UC01 Activity Graph

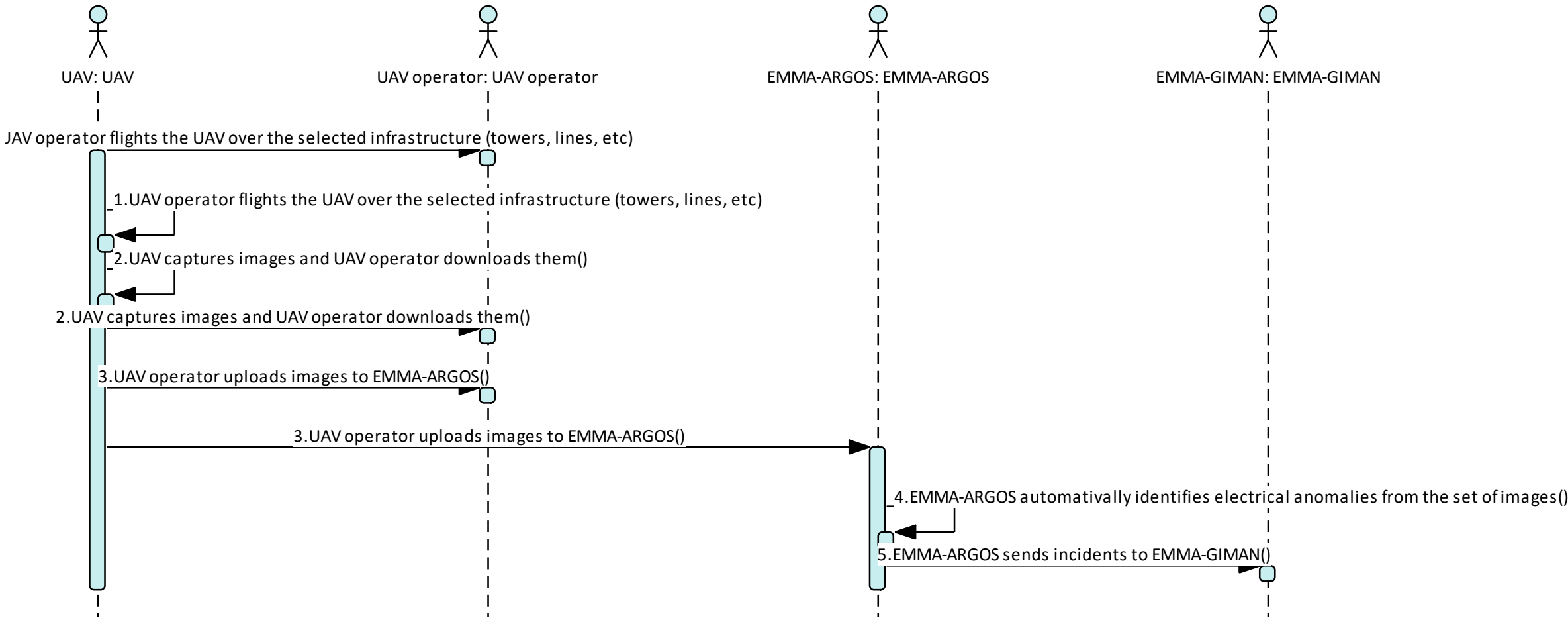


Figure 118 - UC01 Basic Path (1)



D2.3 - Requirements and Detailed Architecture Design

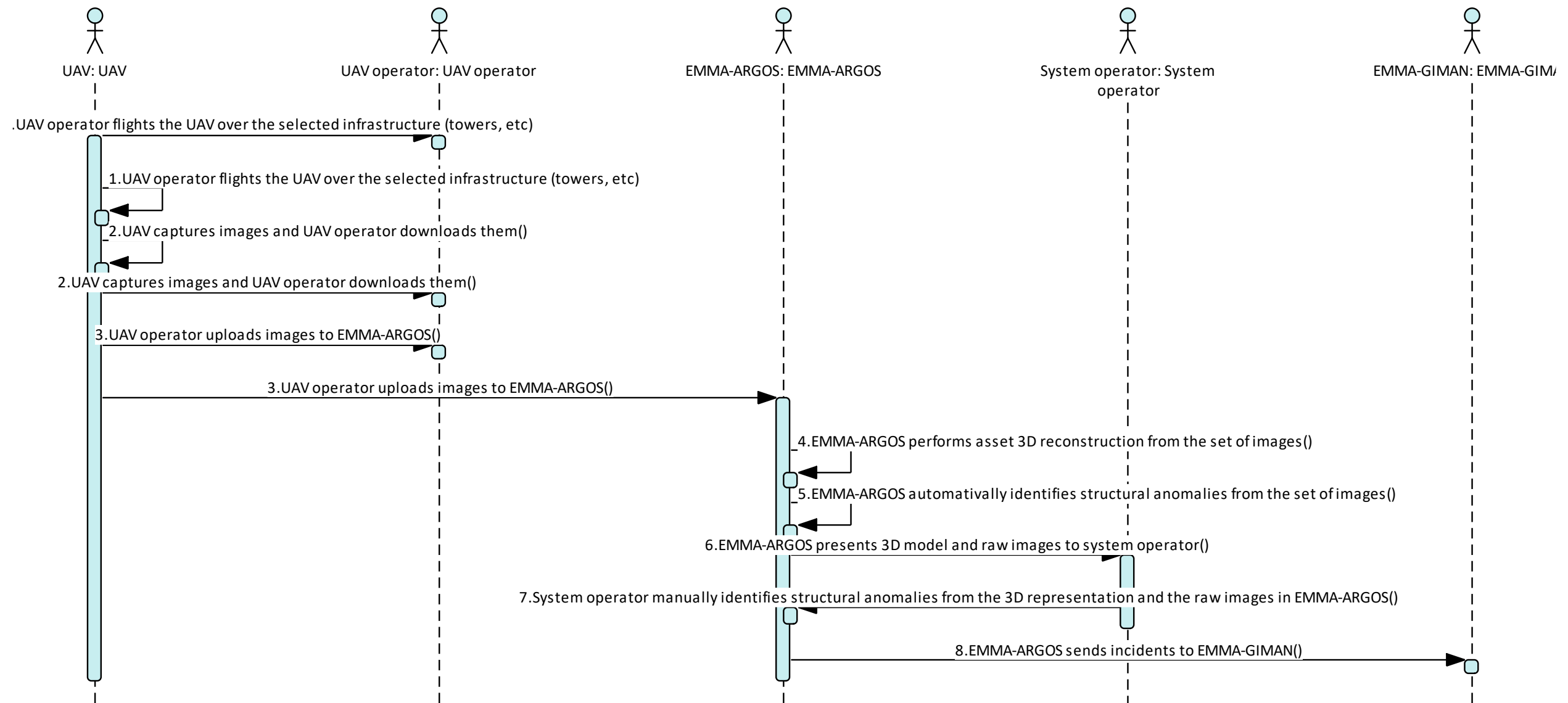


Figure 119 - UC01 Basic Path (2)

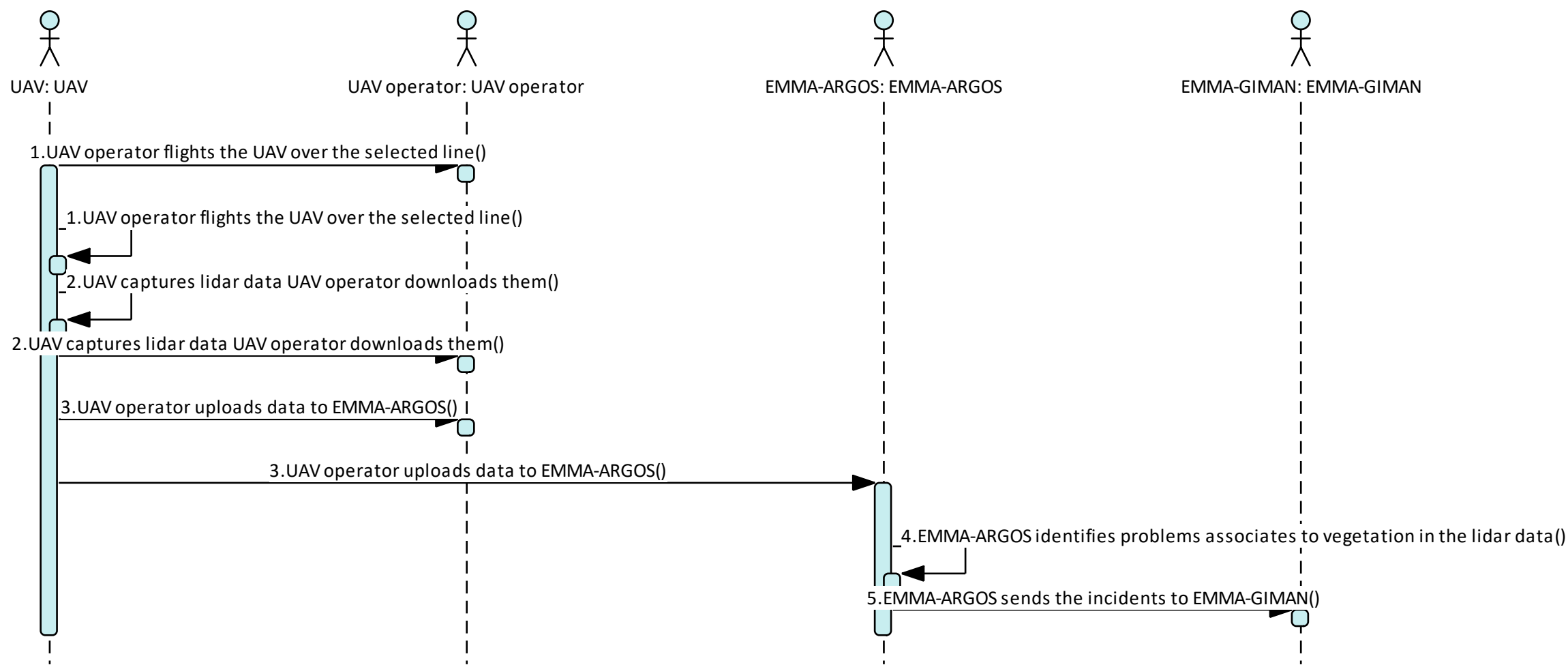


Figure 120 - UC01 Basic Path (3)

UC02 - Substation component status of health calculation based on SCADA measurements and DGA data

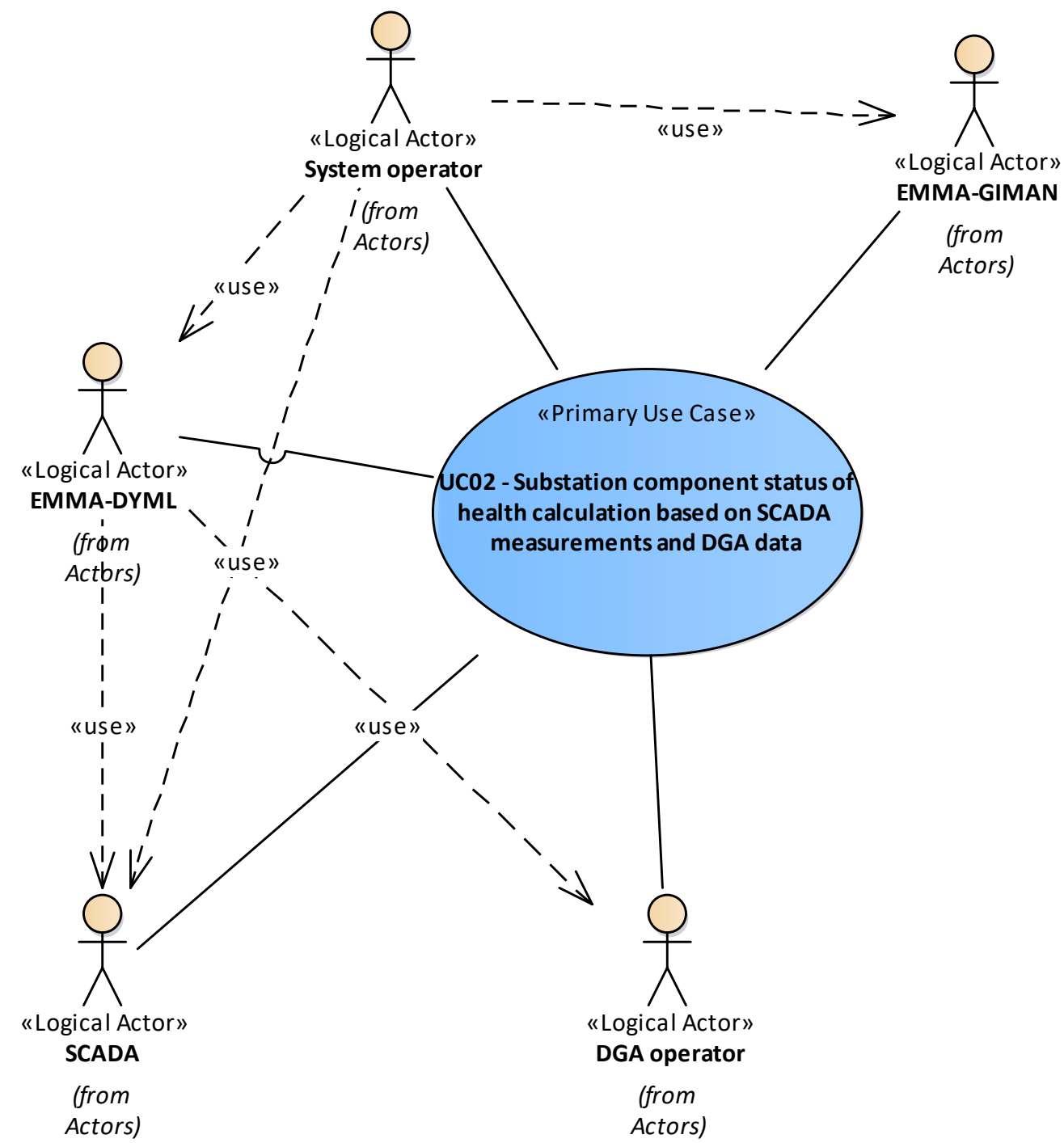


Figure 121 - UC02 Actor Involved

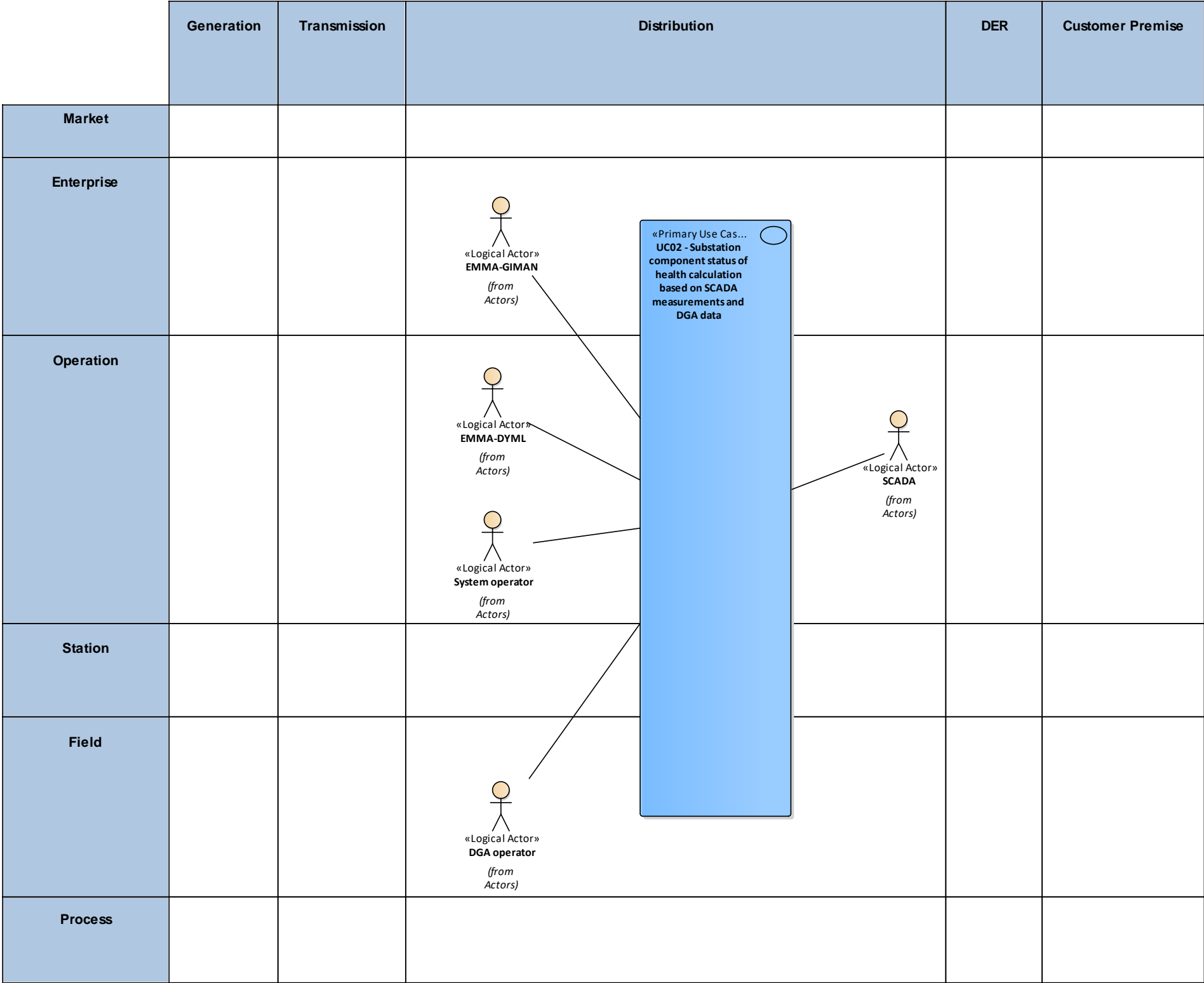


Figure 122 - UC02 Functional Layer

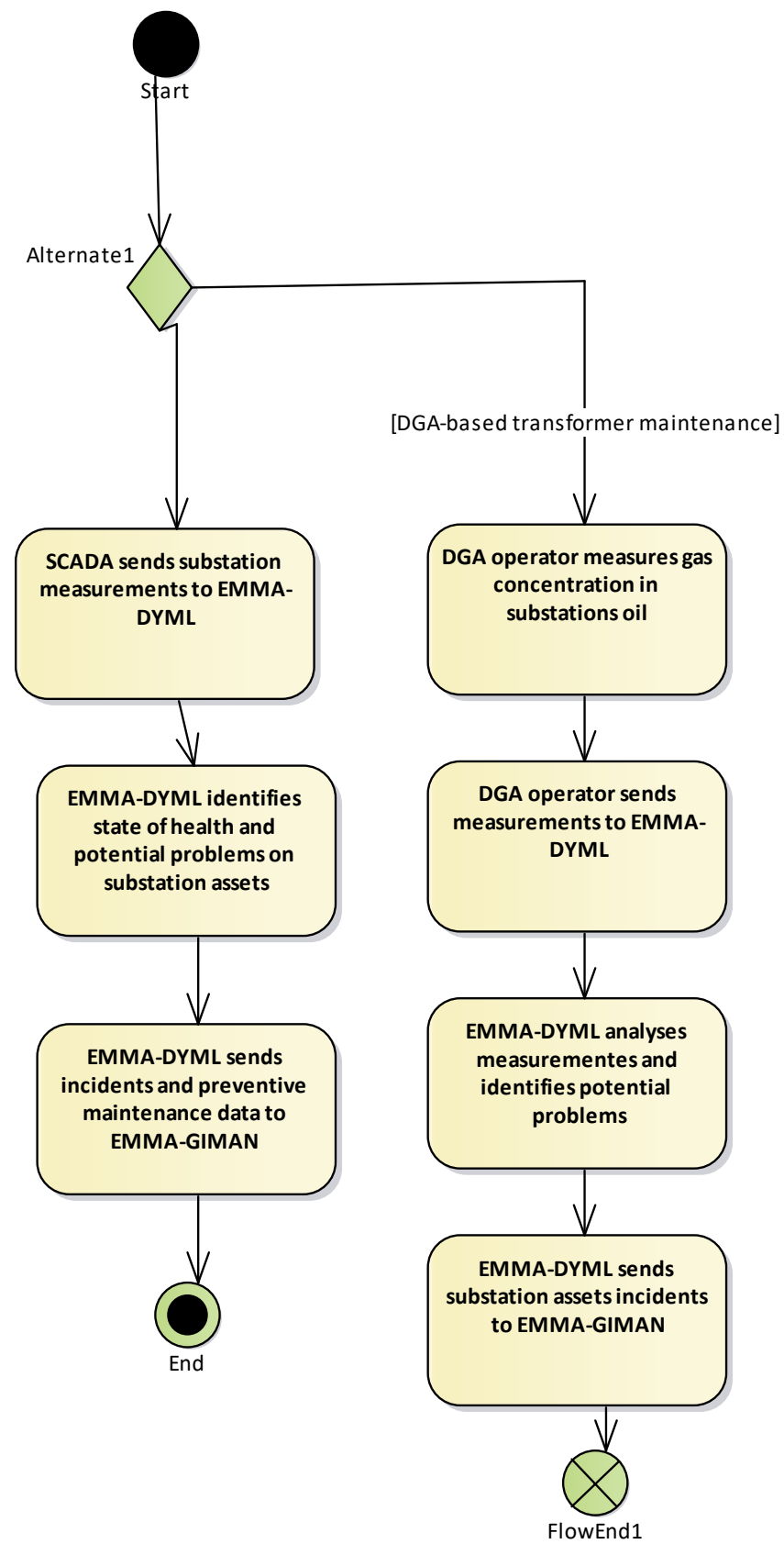


Figure 123 - UC02 Activity Graph

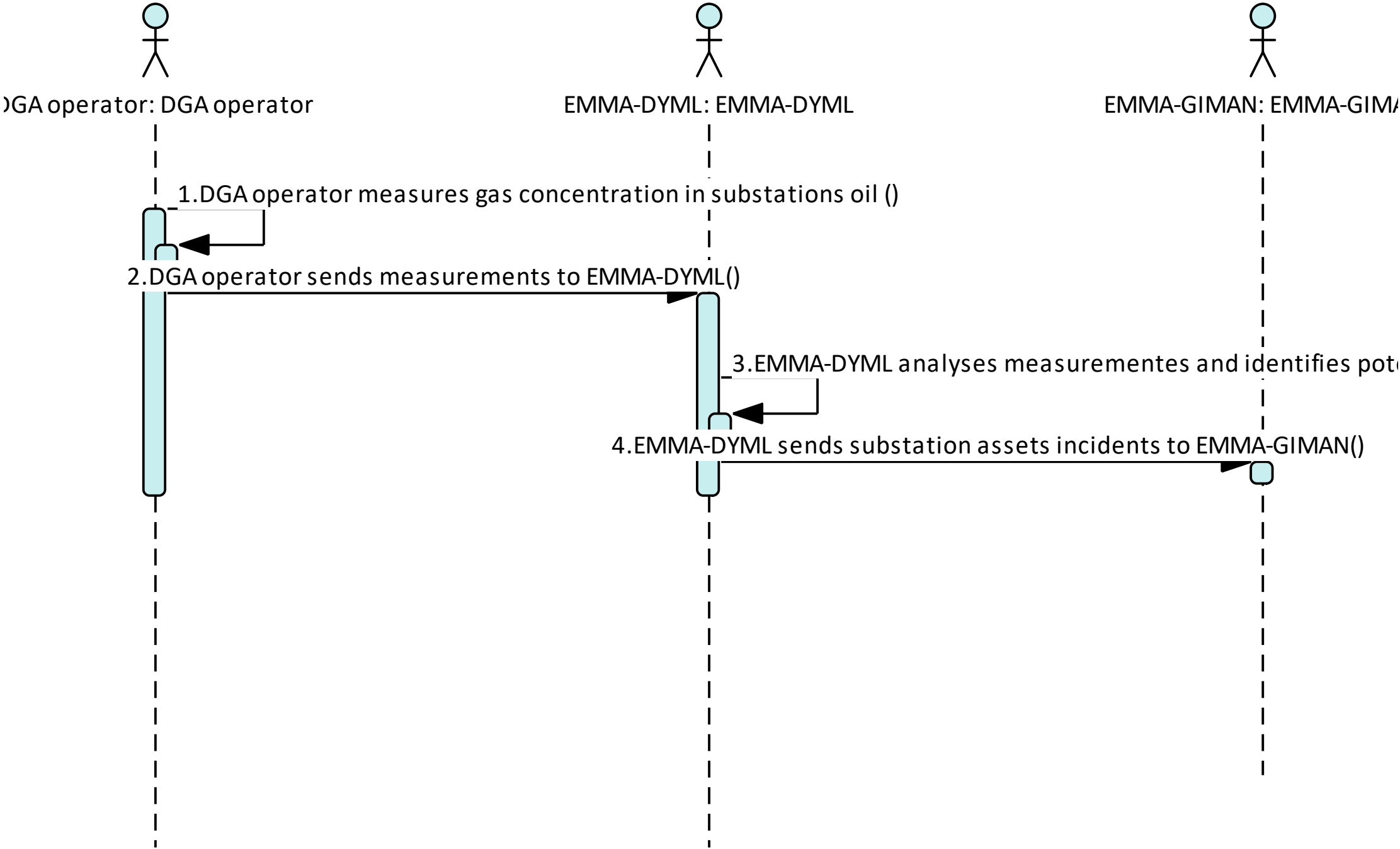


Figure 124 - UC02 Basic Path (1)

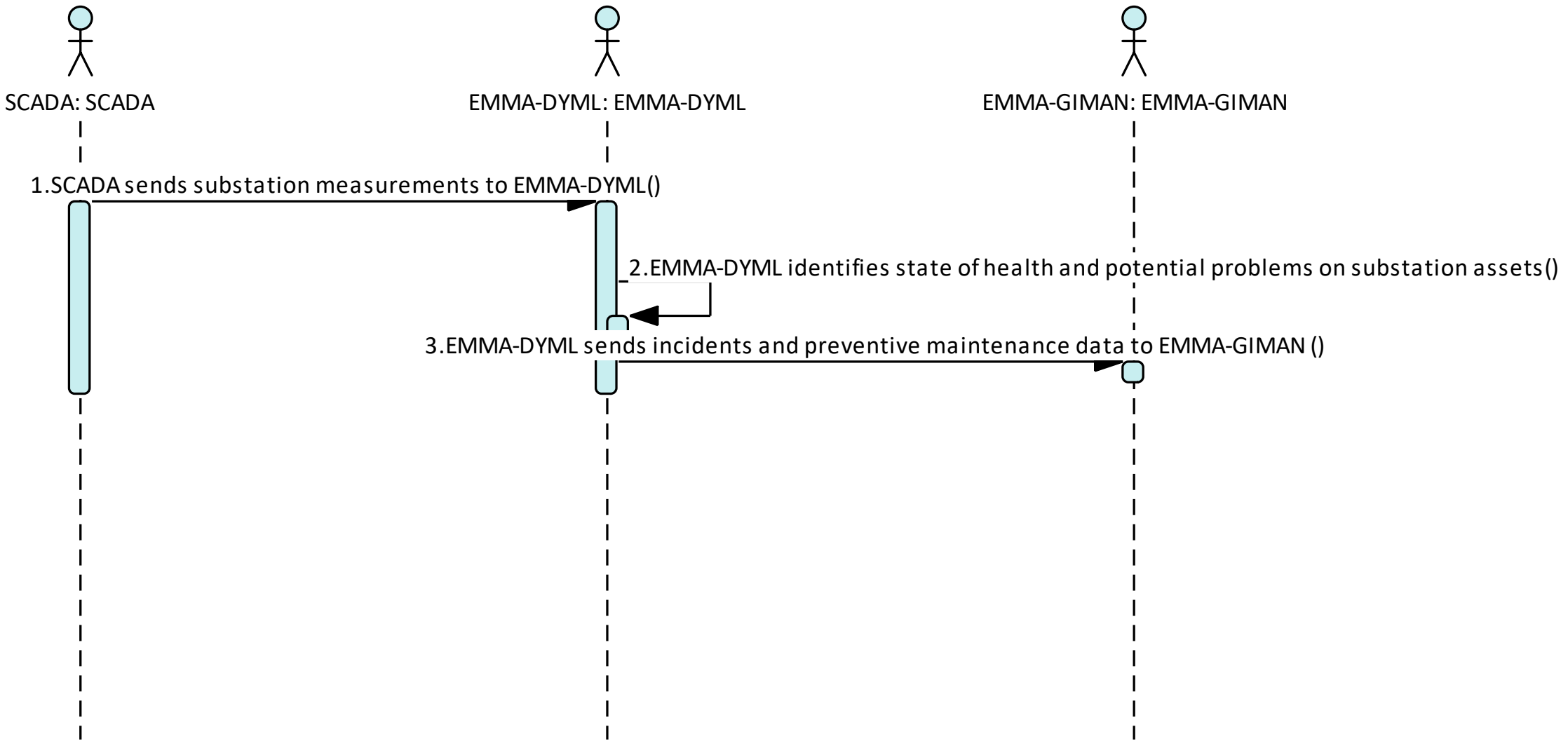


Figure 125 - UC02 Basic Path (2)



UC03 - Malfunctioning detection of PV panels through autonomous UAV image acquisition

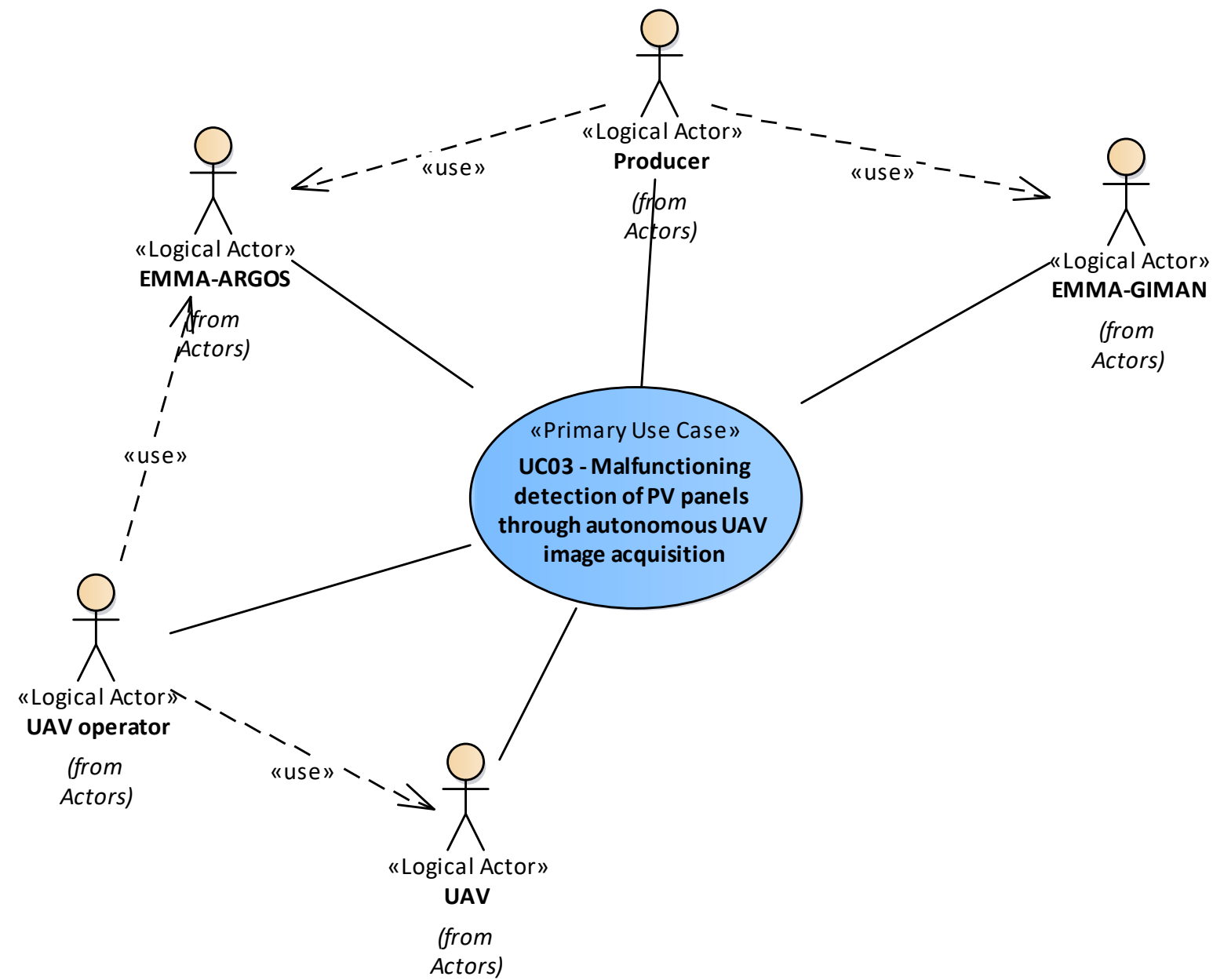


Figure 126- UC03 Actors Involved

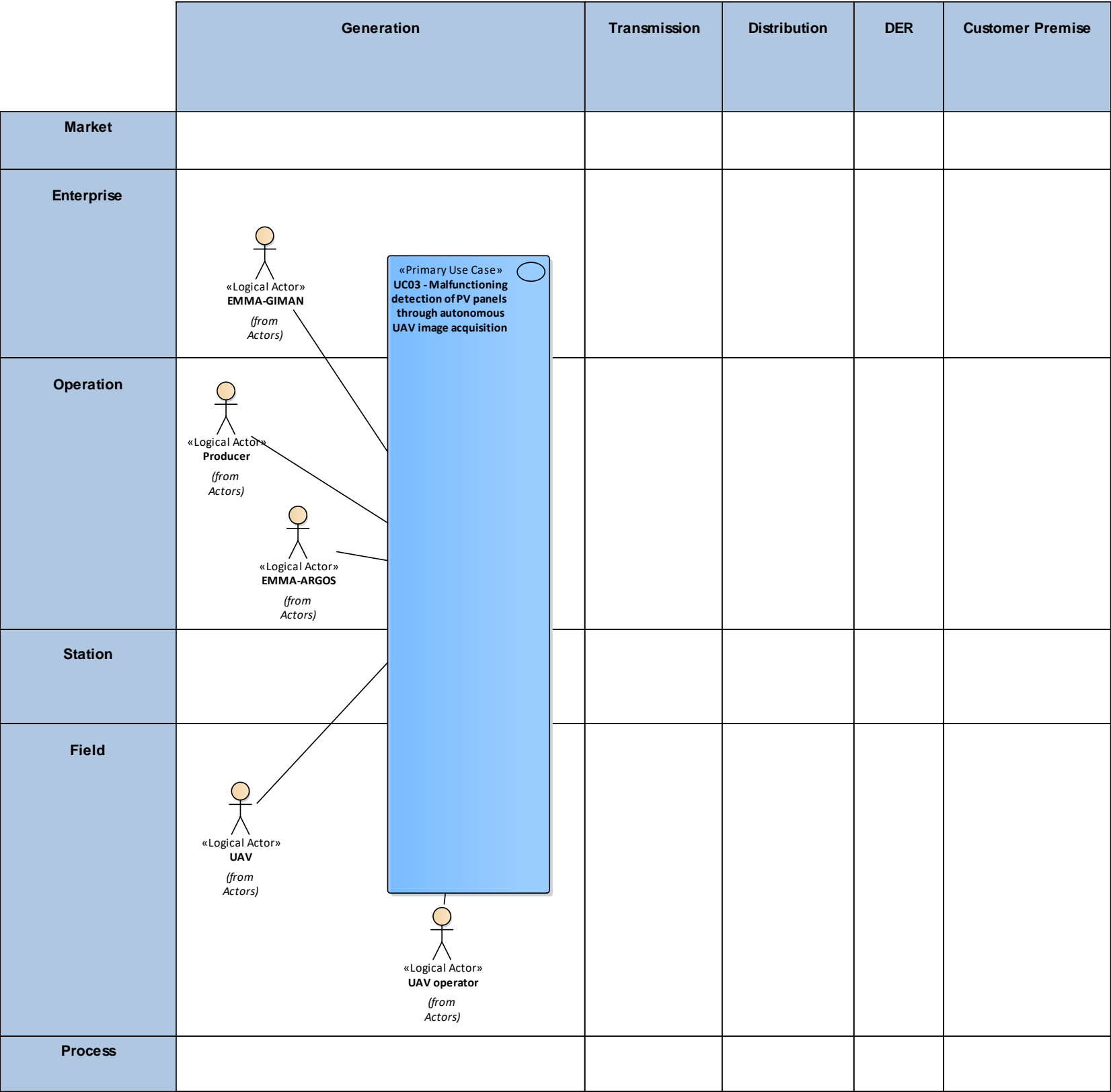


Figure 127 - UC03 Functional Layer

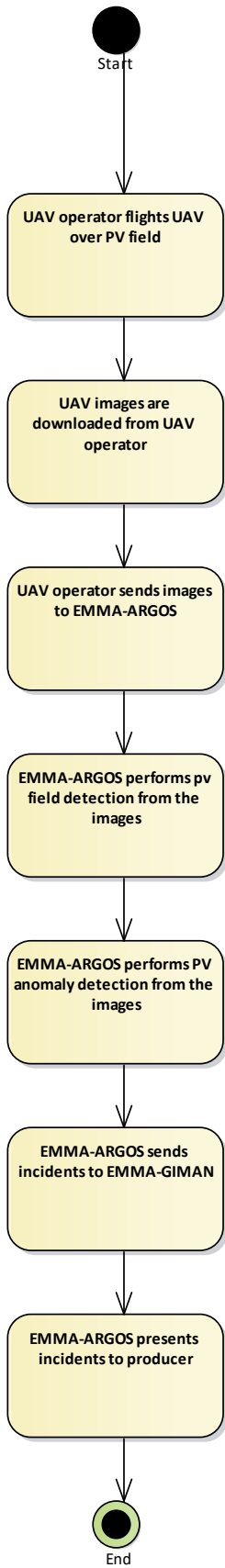


Figure 128 – UC03 Activity Graph

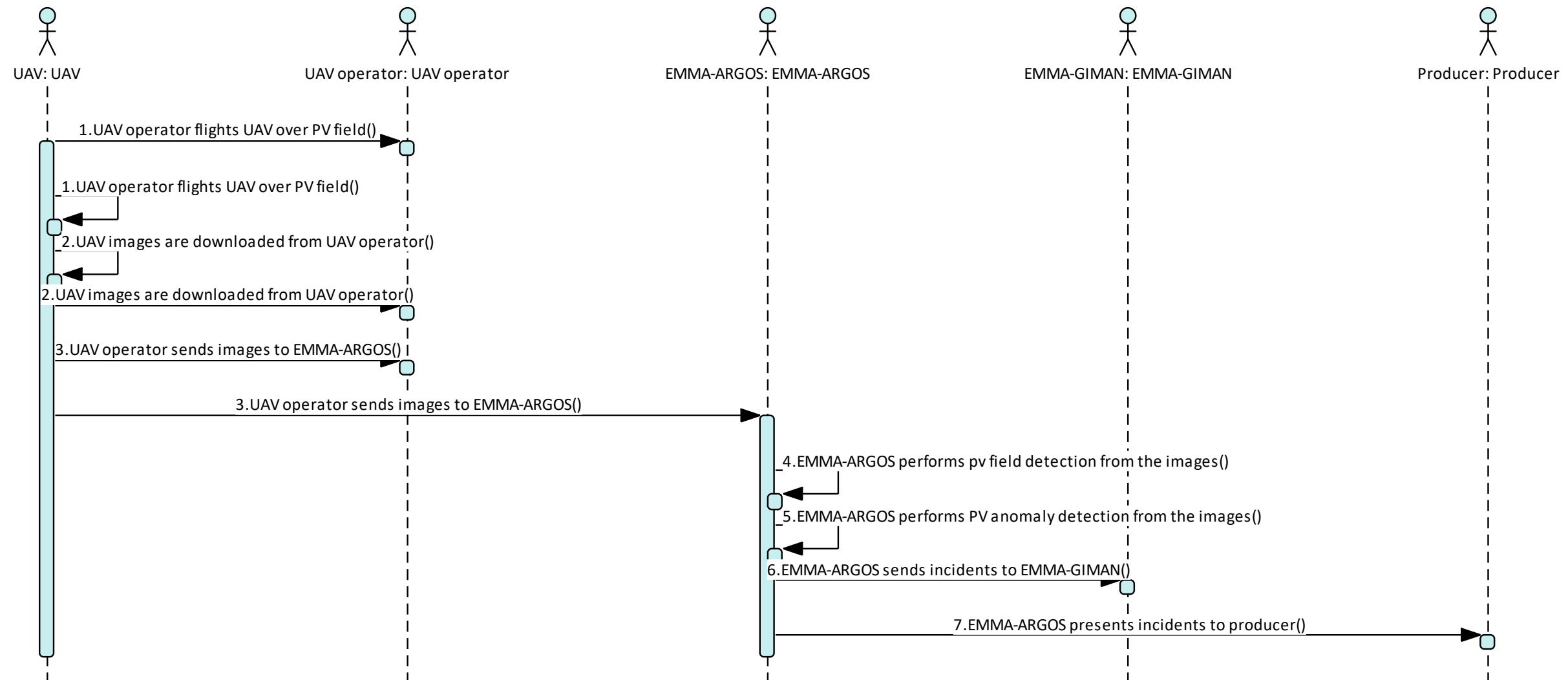


Figure 129 – UC03 Basic Path

UC04 - Detection of NTL through SCADA and AMI data, from a selected portion of the distribution grid

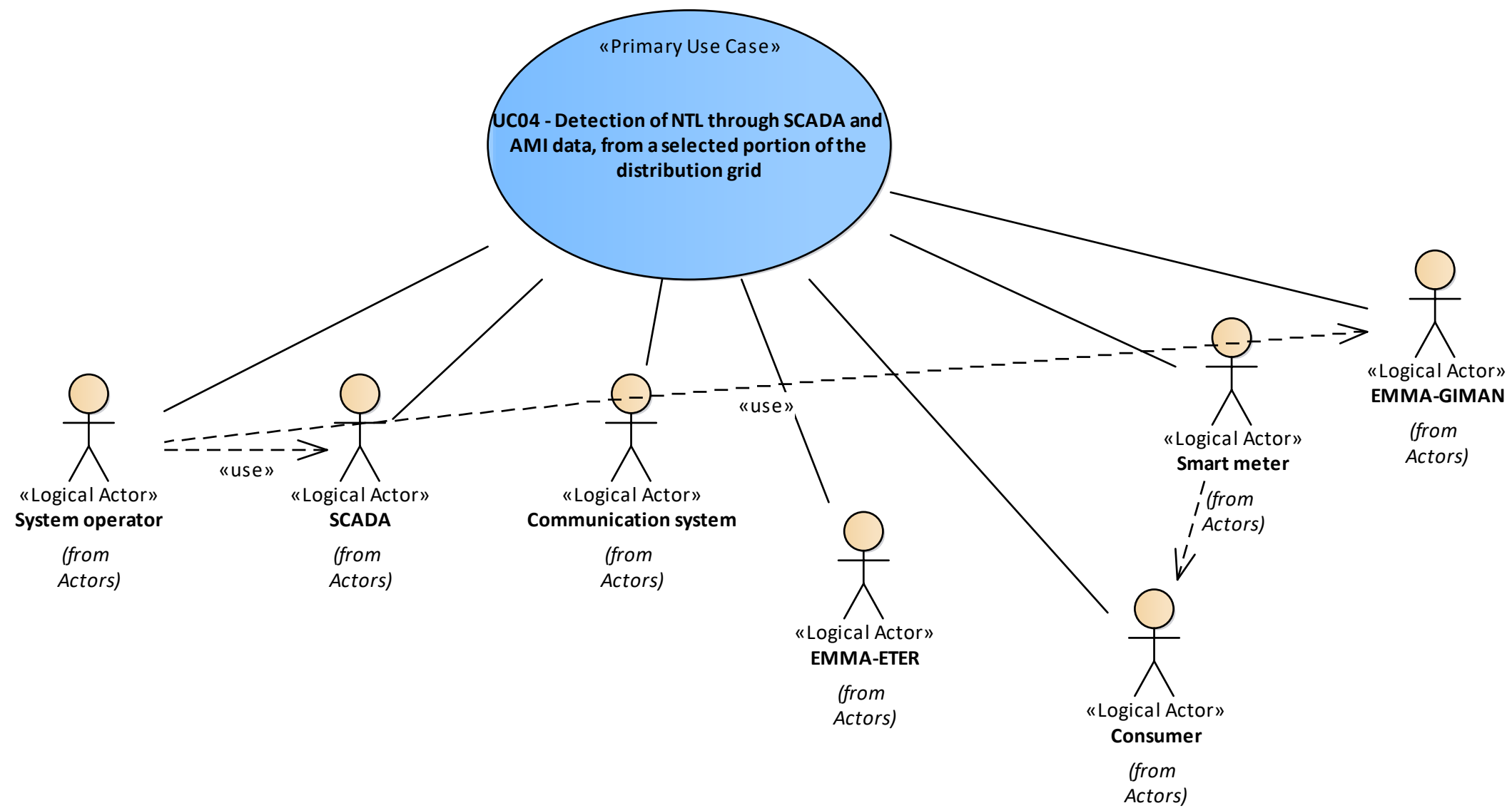


Figure 130 - UC04 Actors Involved

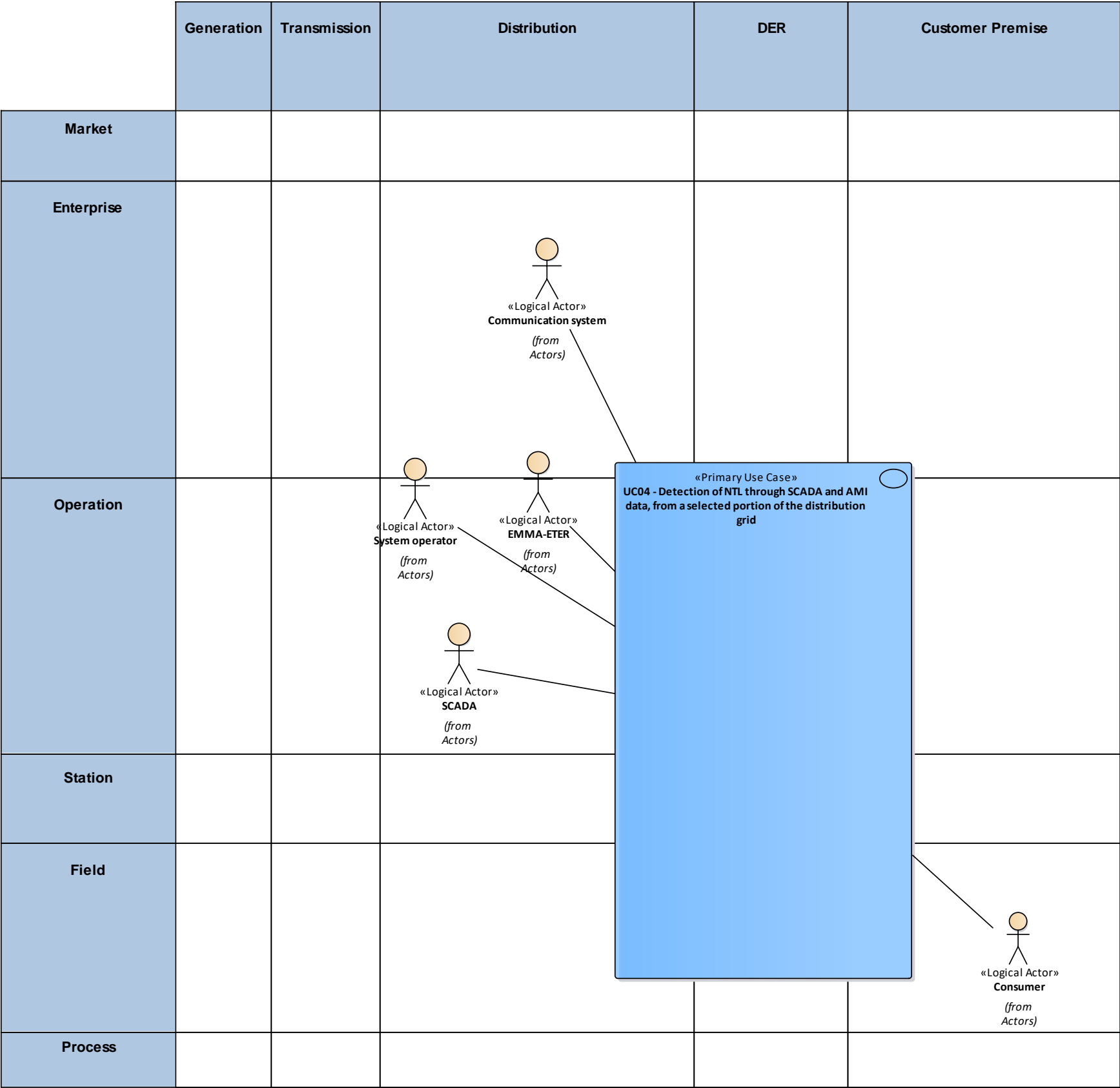


Figure 131 - UC04 Functional Layer

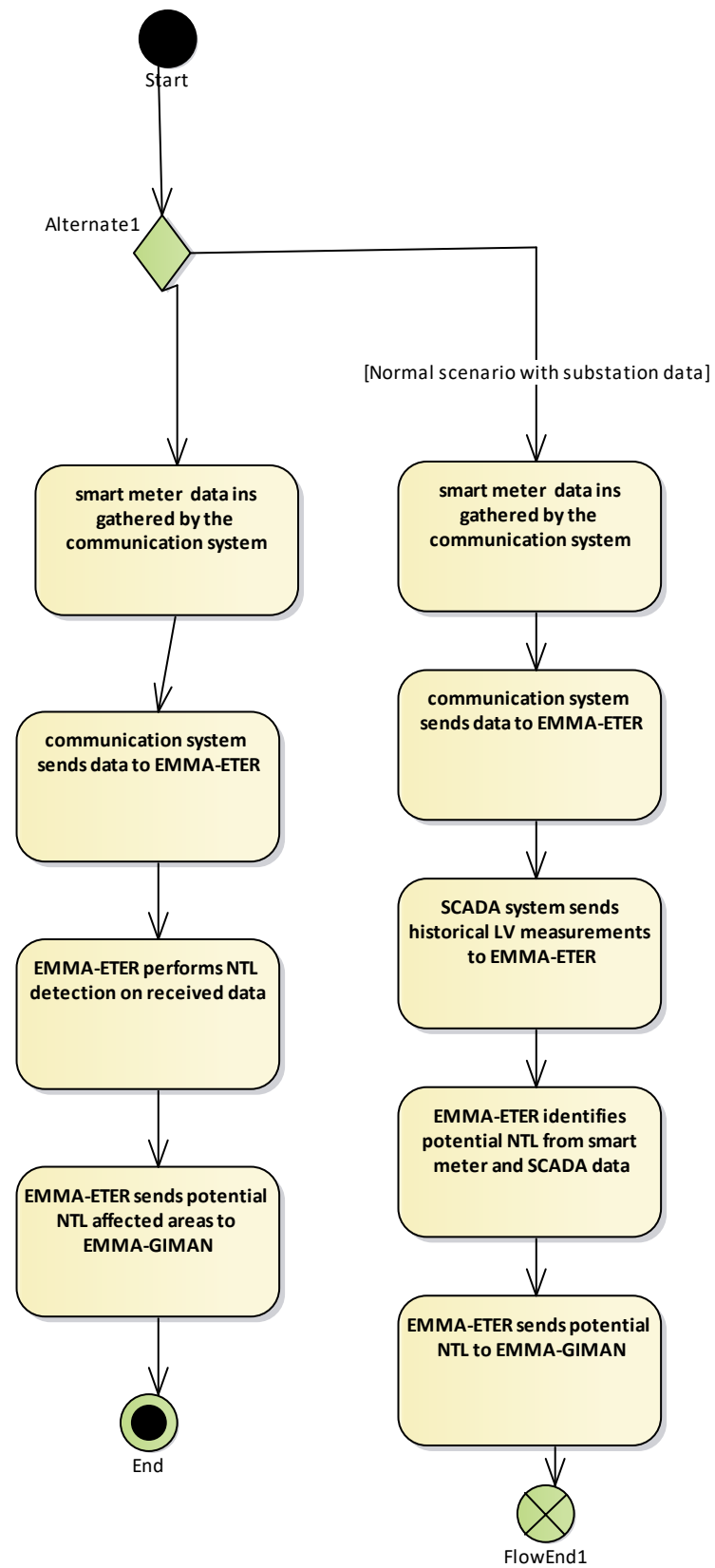


Figure 132 - UC04 Activity Graph

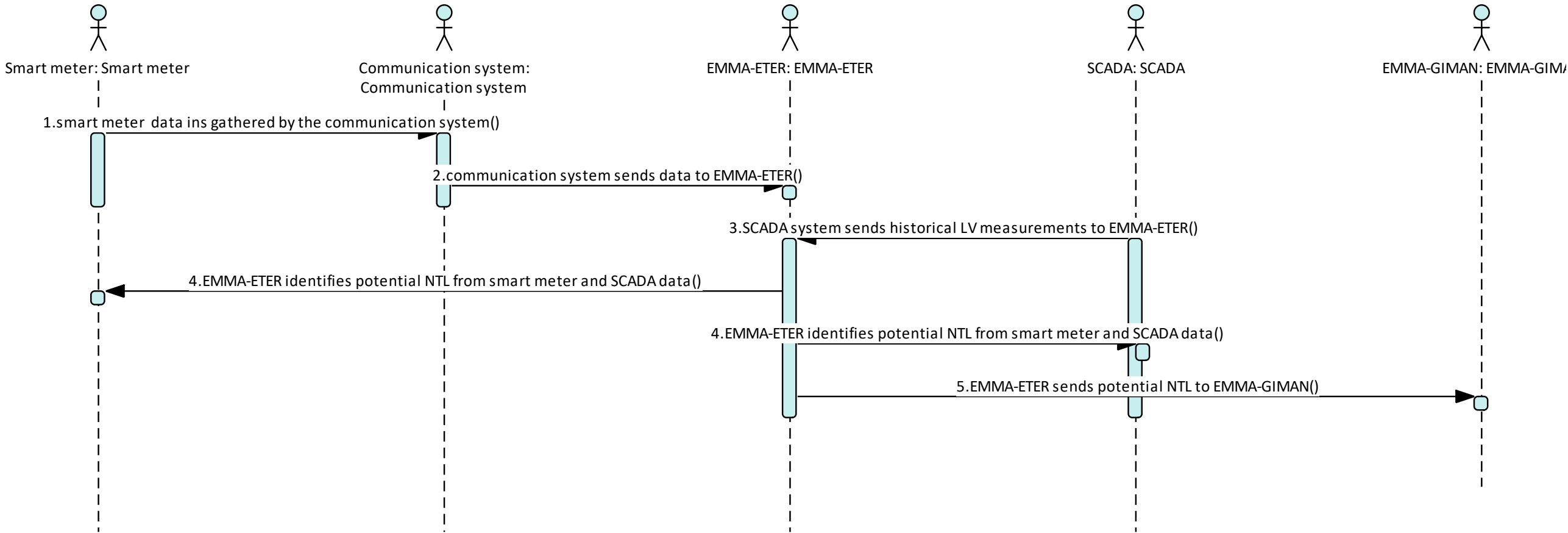


Figure 133 - UC04 Basic Path (1)

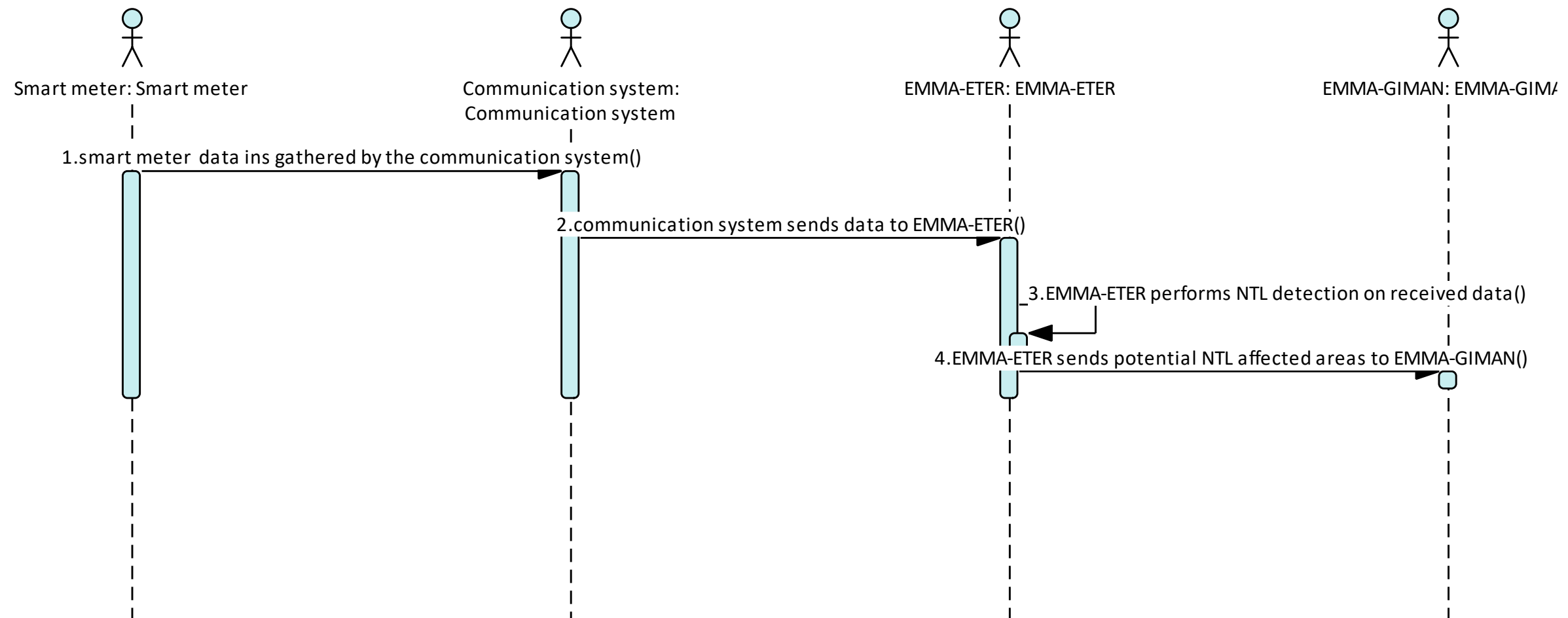


Figure 134 - UC04 Basic Path (2)

UC05 - Automated ranking intervention of assets and optimal scheduling (including routing) of intervention workforce to perform maintenance task

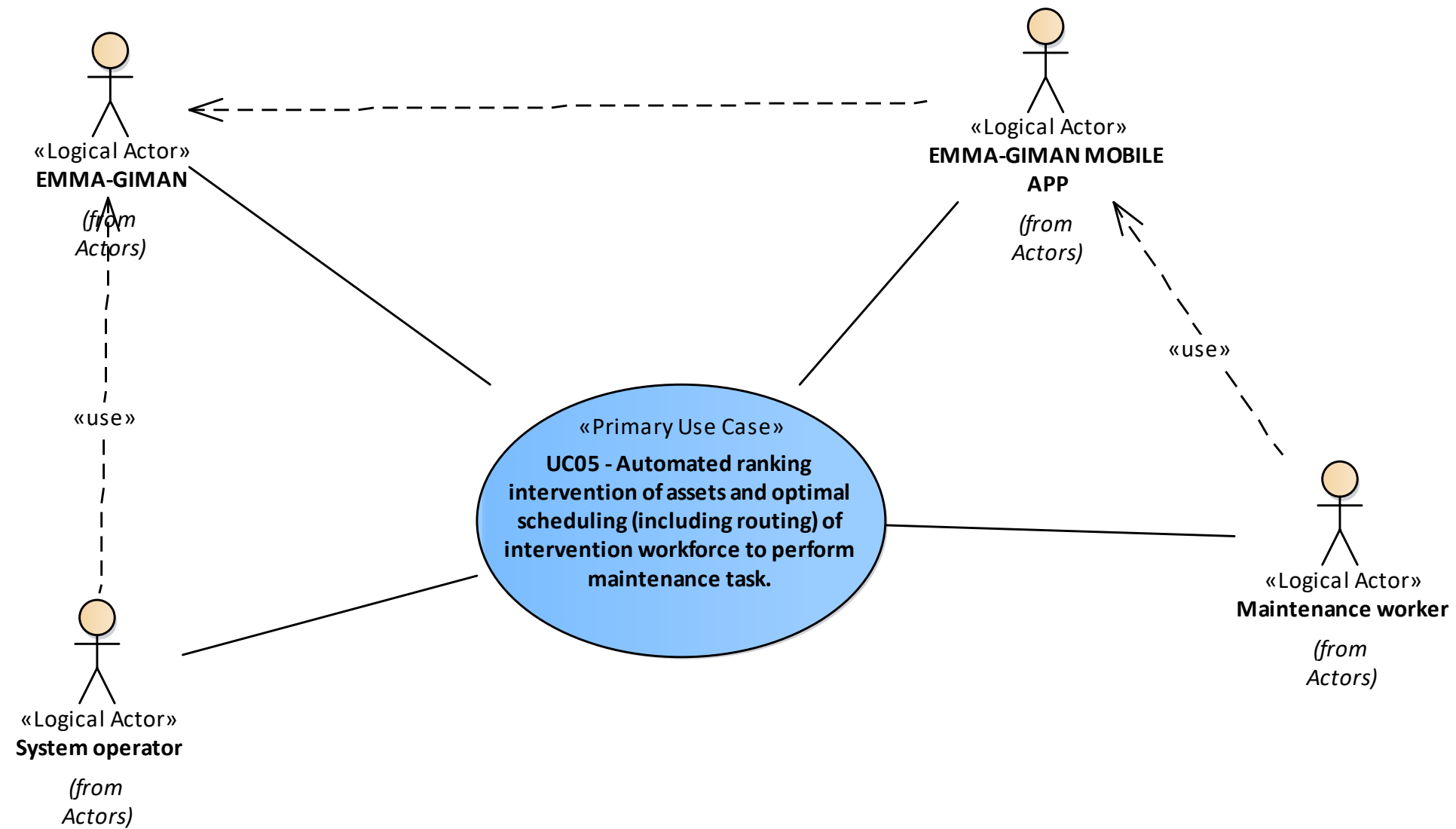


Figure 135 - UC05 Actors Involved

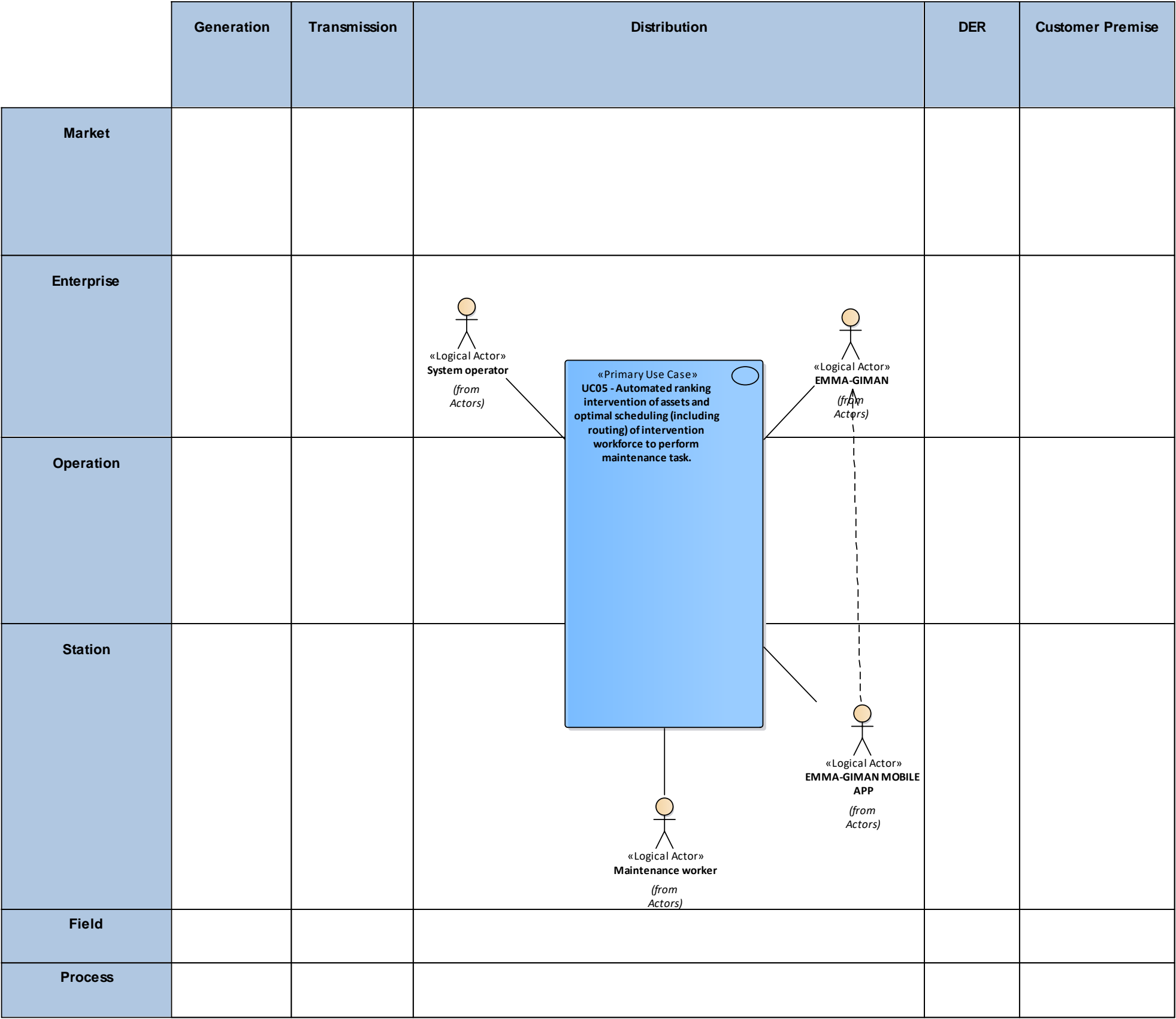


Figure 136 - UC05 Functional Layer

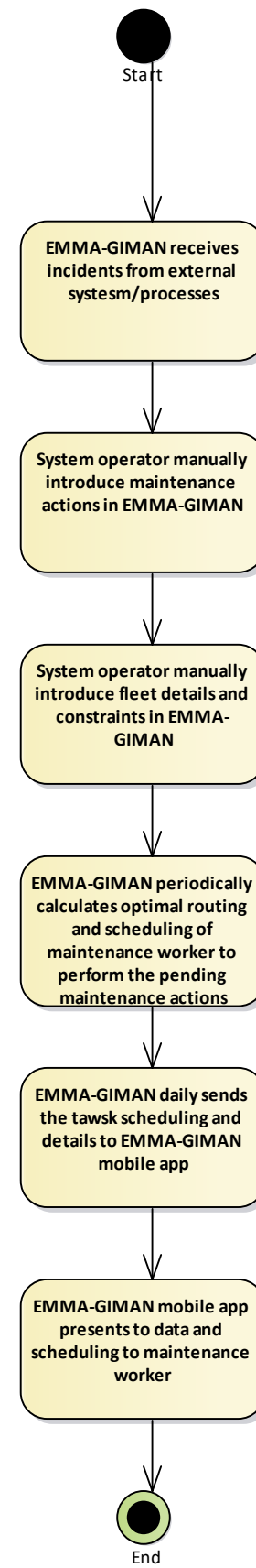


Figure 137 - UC05 Activity Graph

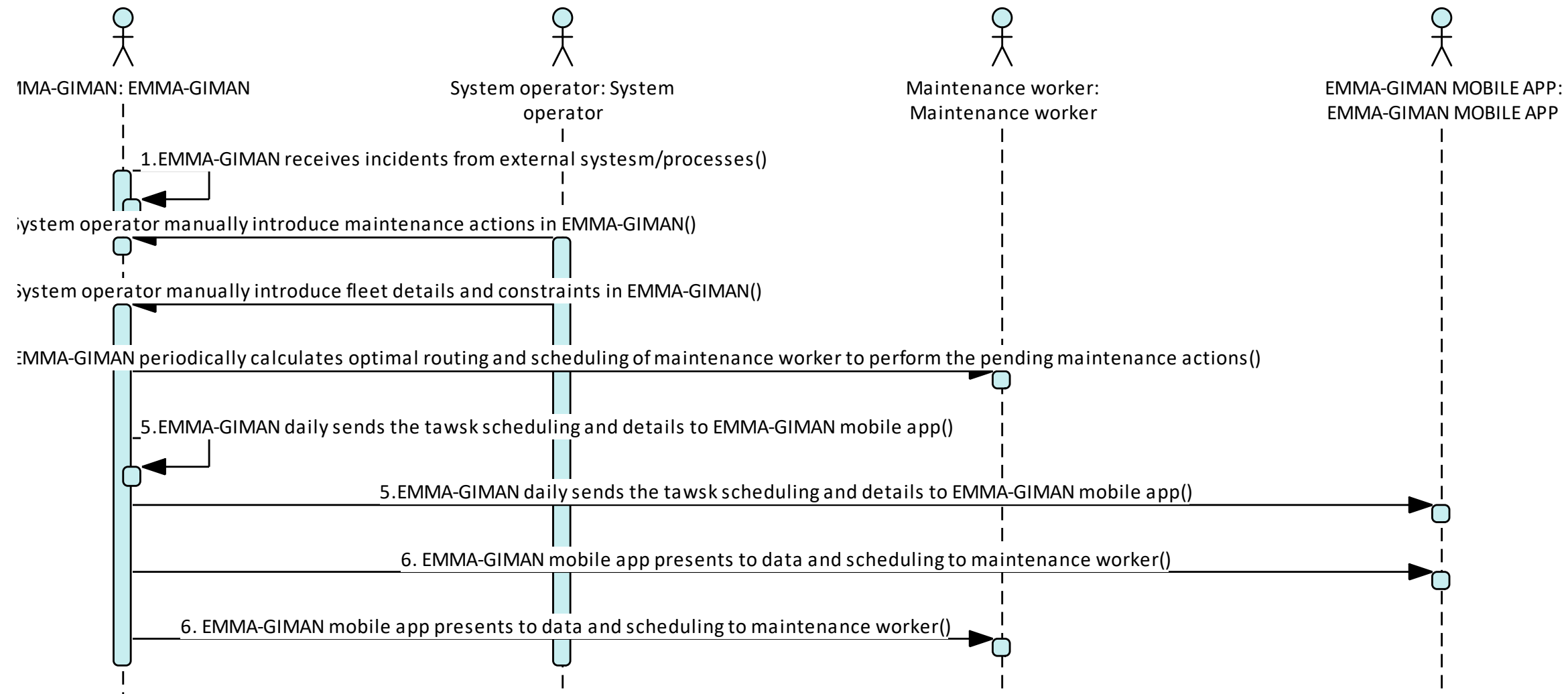


Figure 138 - UC05 Basic Path

UC06 - Substation components degradation detection by analysing images (Conventional & thermal)

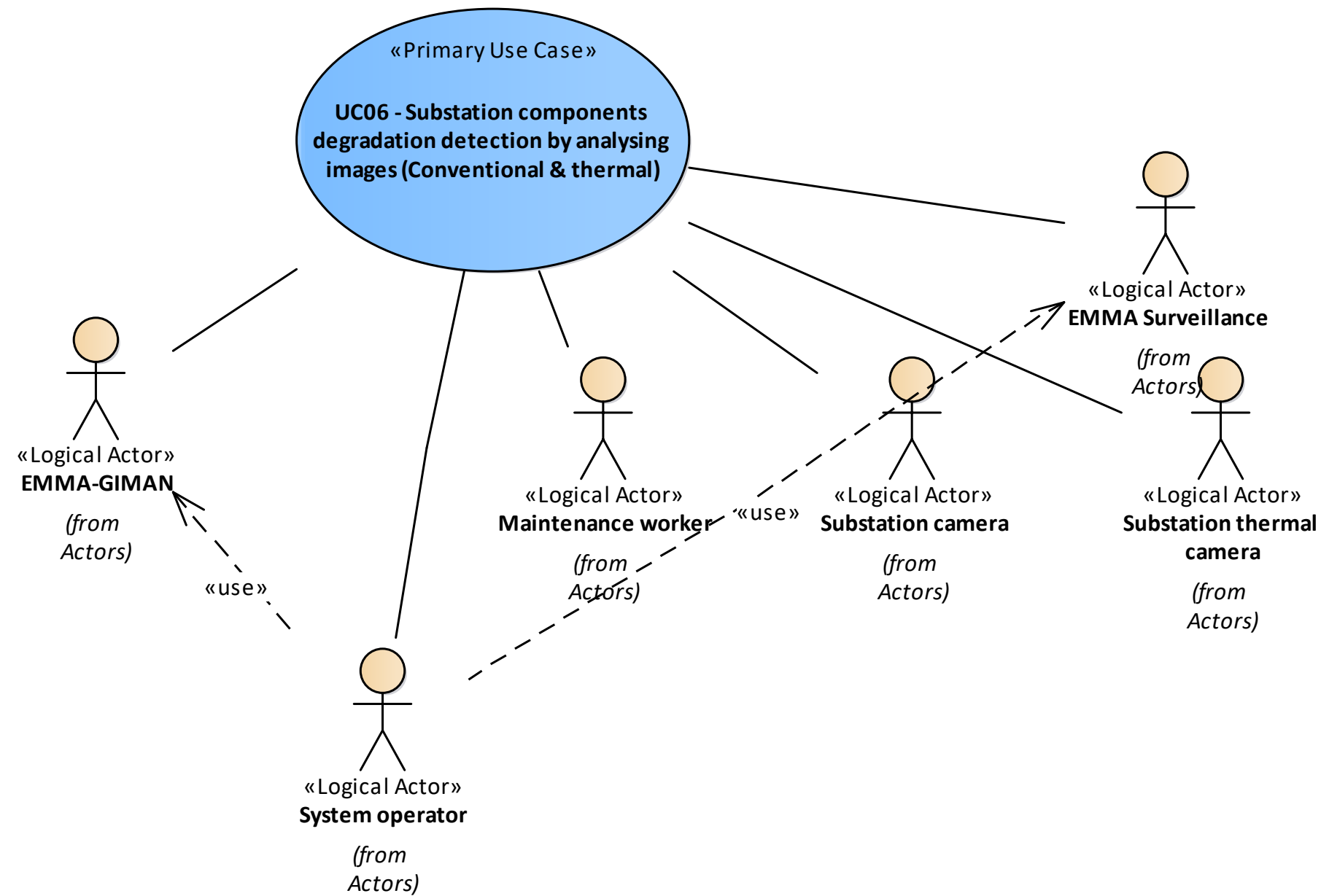


Figure 139 - UC06 Actors Involved

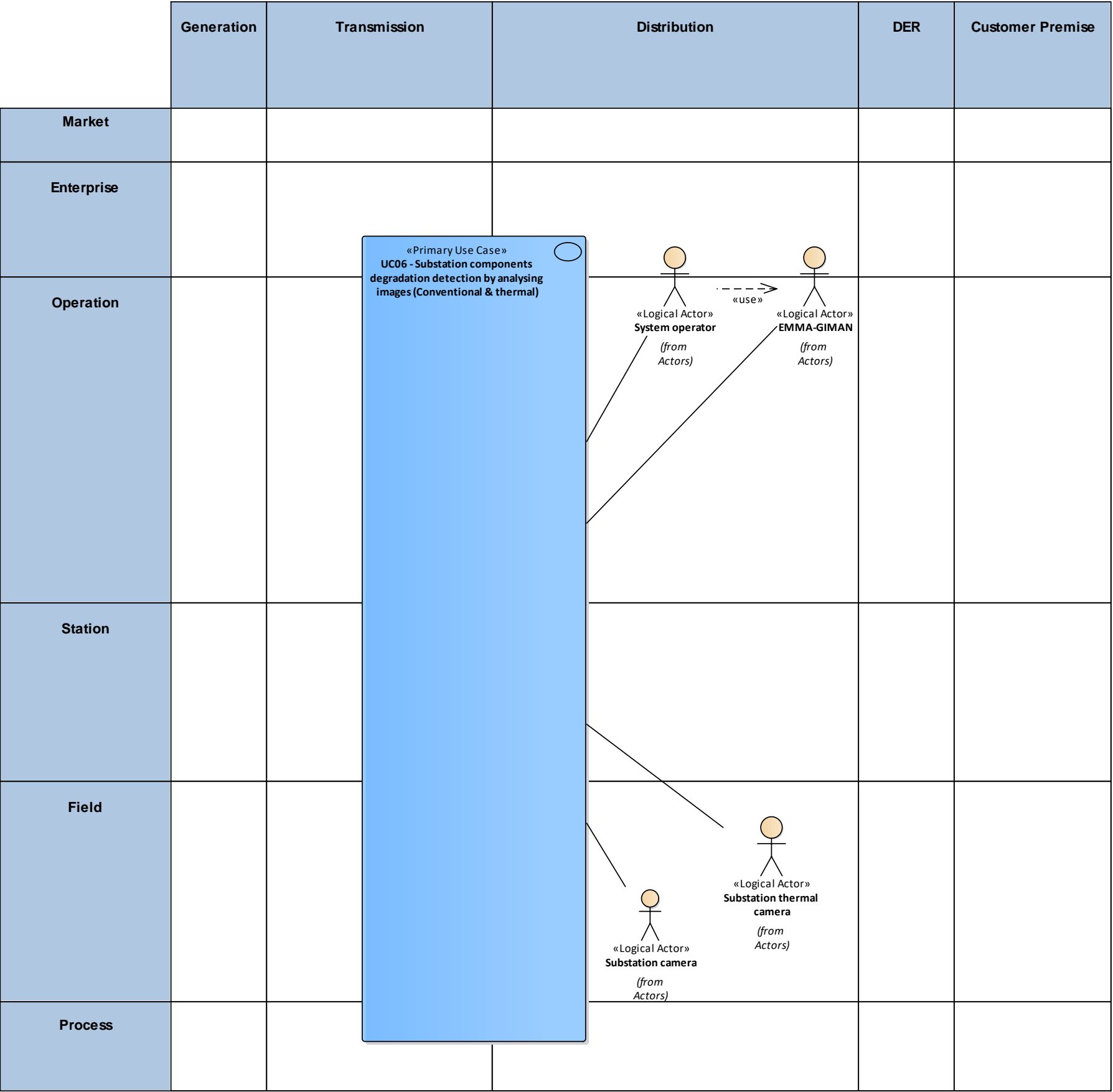


Figure 140 - UC06 Functional Layer

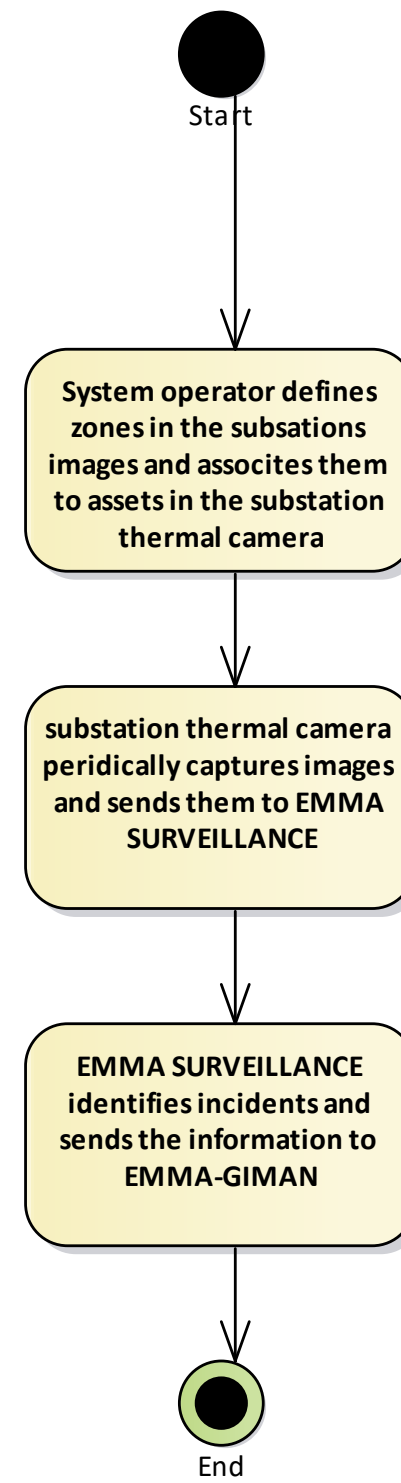


Figure 141 - UC06 Functional Graph

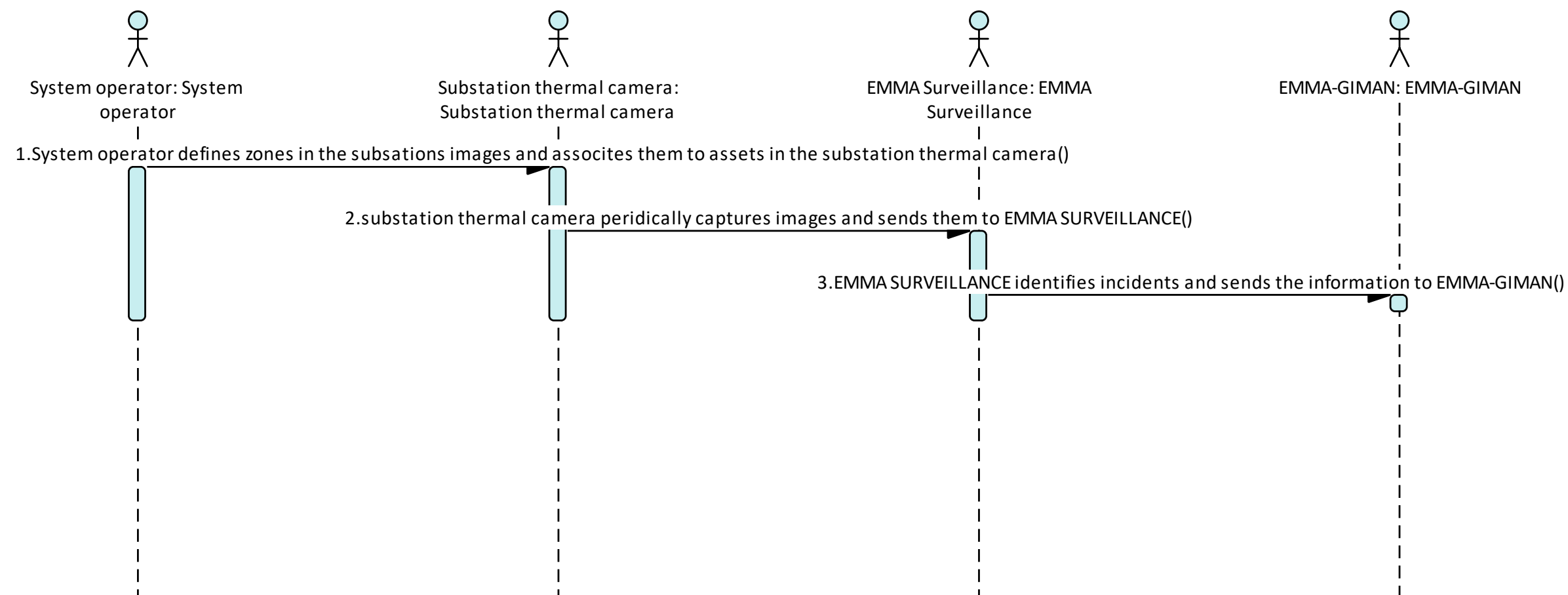


Figure 142 - UC06 Basic Path

UC08 - Outage planning optimization

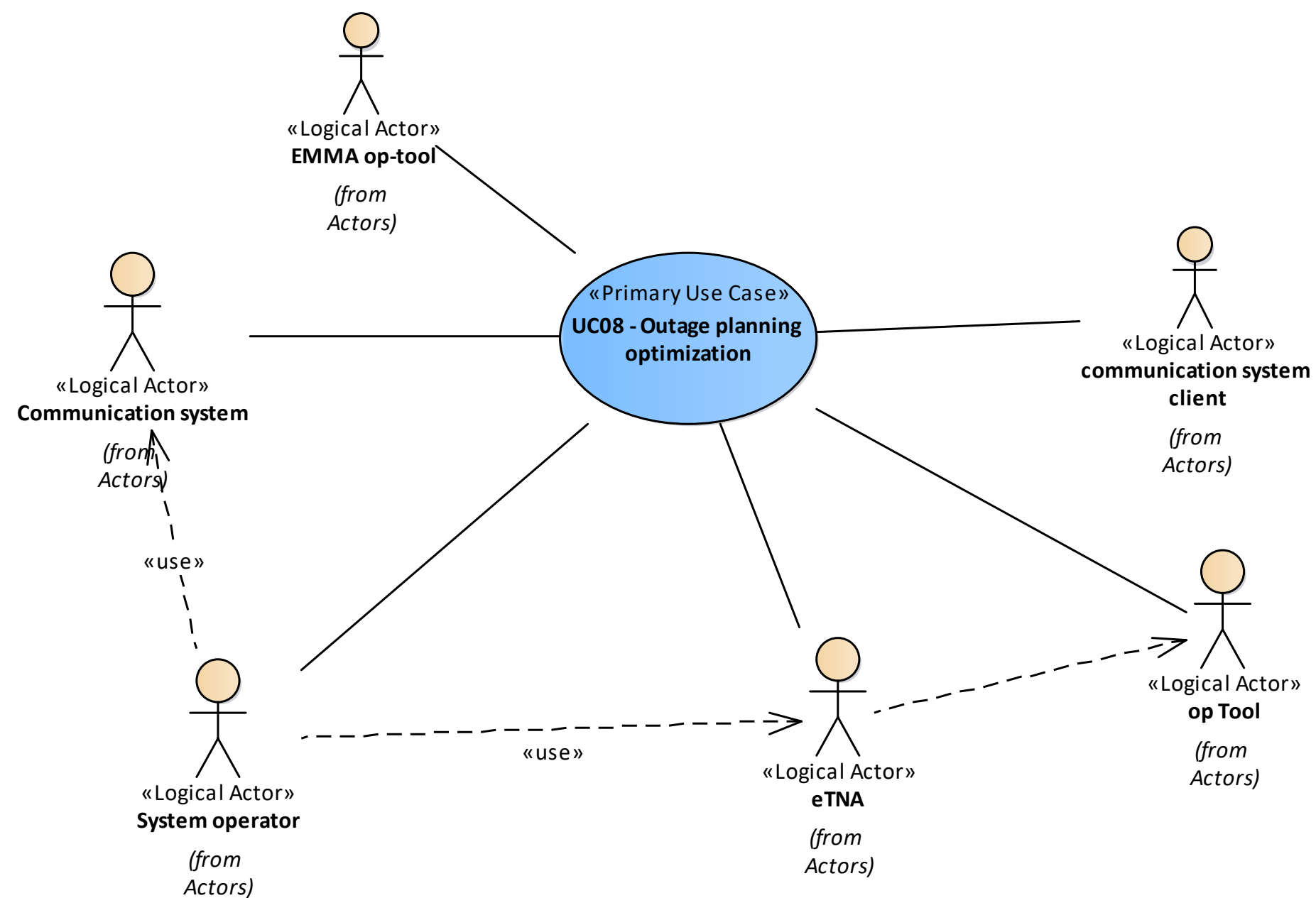


Figure 143 - UC08 Actors Involved

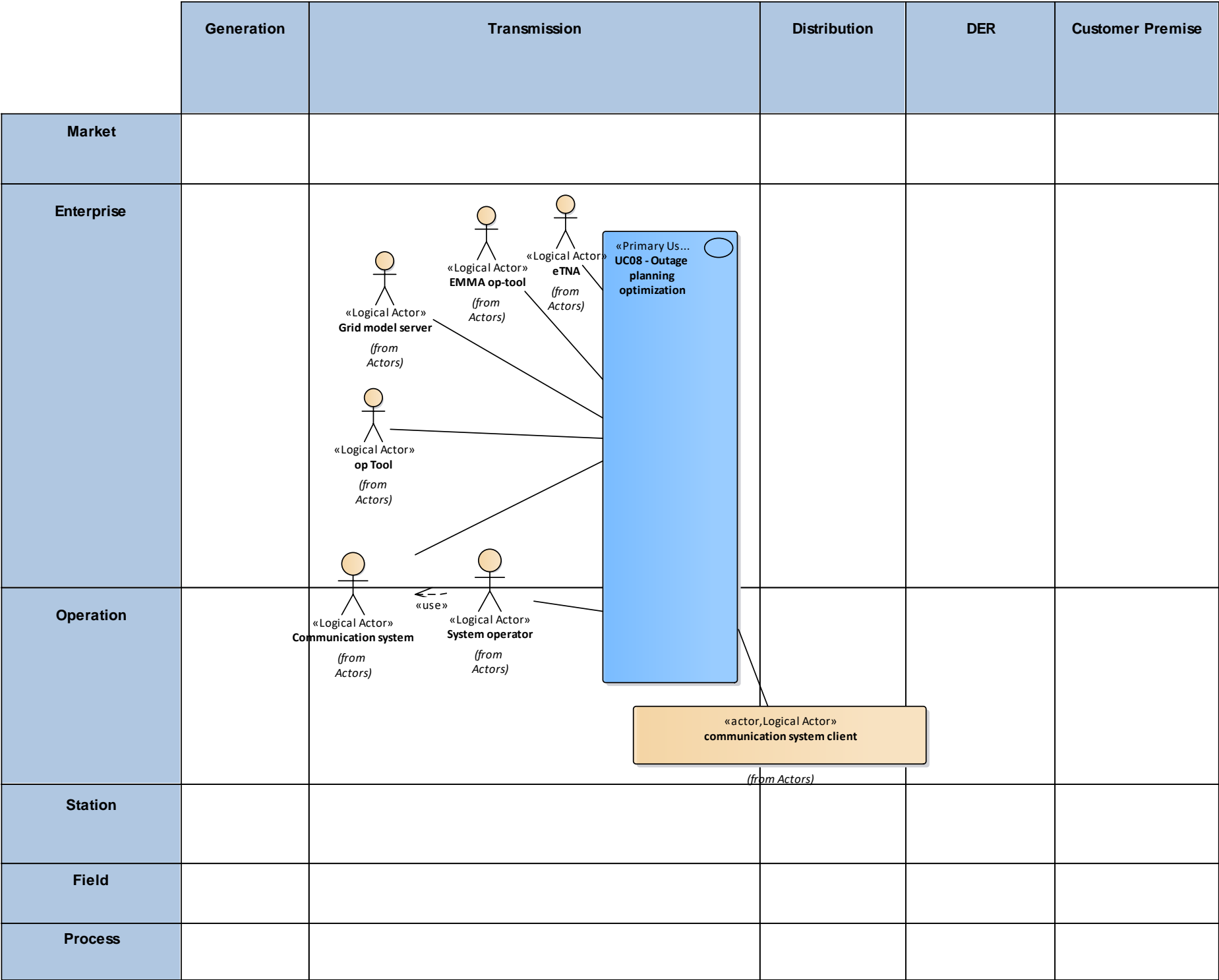


Figure 144 – UC08 Functional Layer

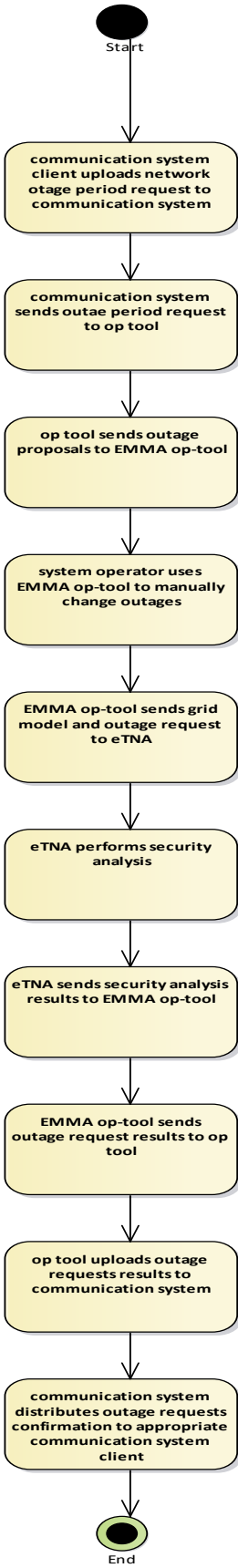


Figure 145 – UC08 Activity Graph

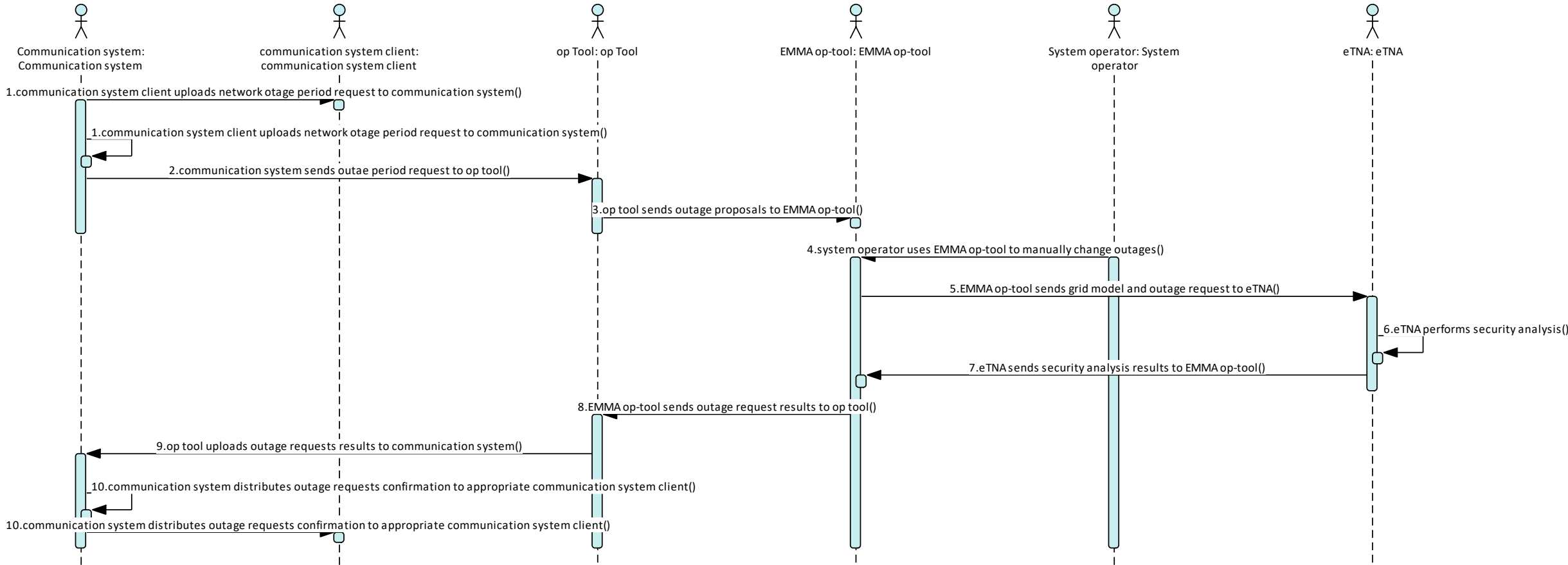


Figure 146 - UC08 Basic Path

UC09 - Automation of power quality parameters emission levels calculation

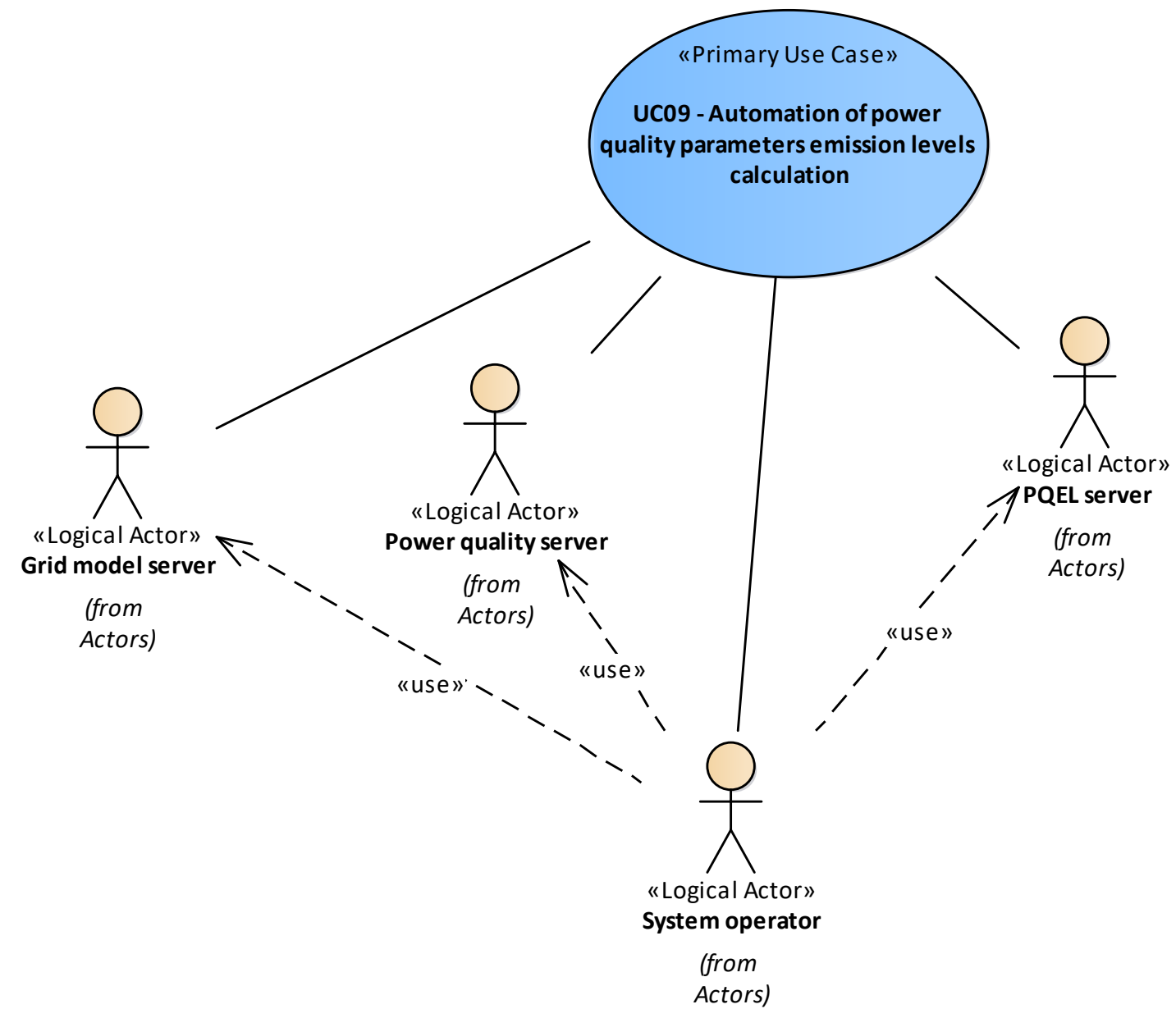


Figure 147 - UC09 Actors Involved

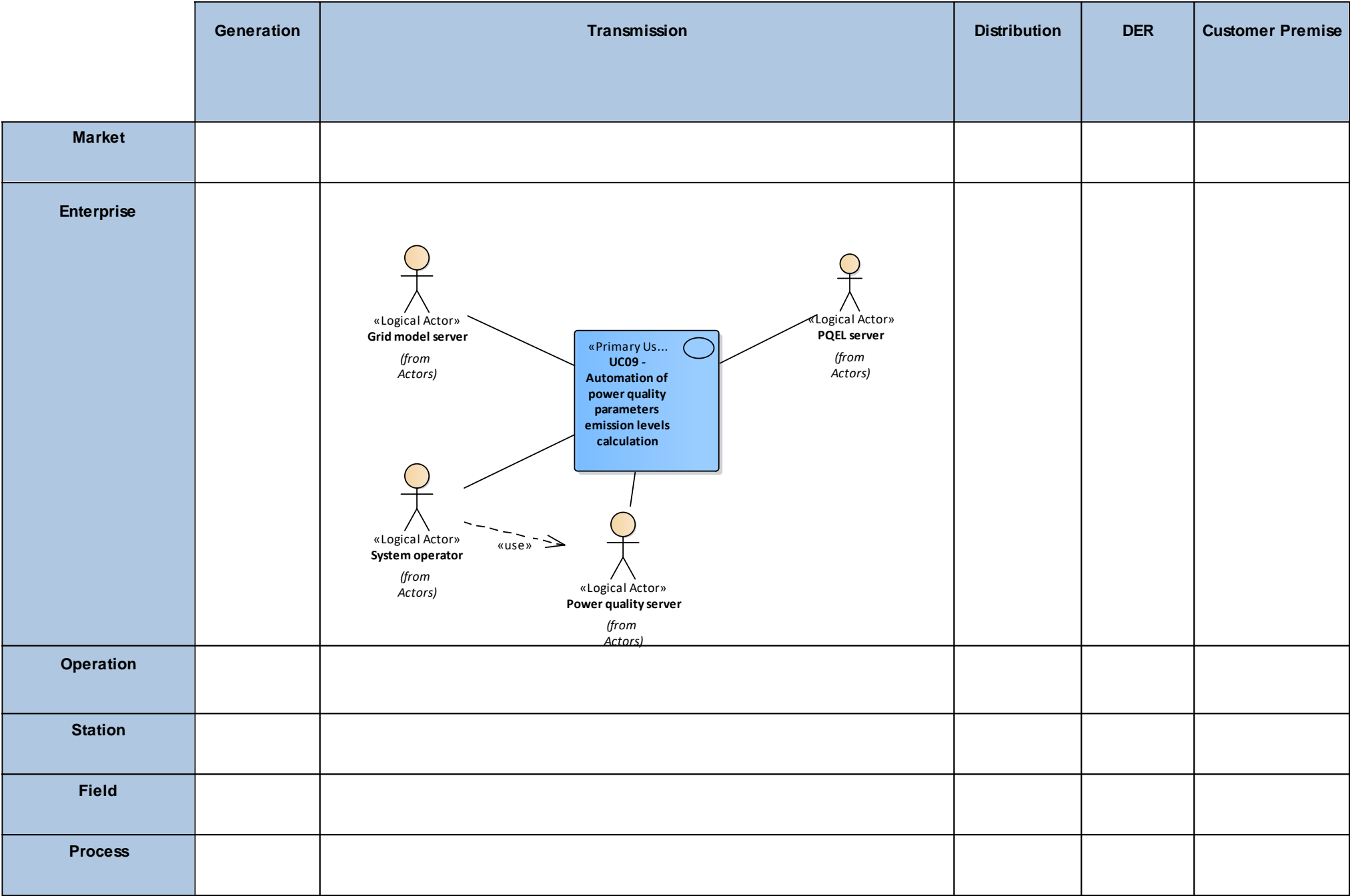


Figure 148 - UC09 Functional Layer

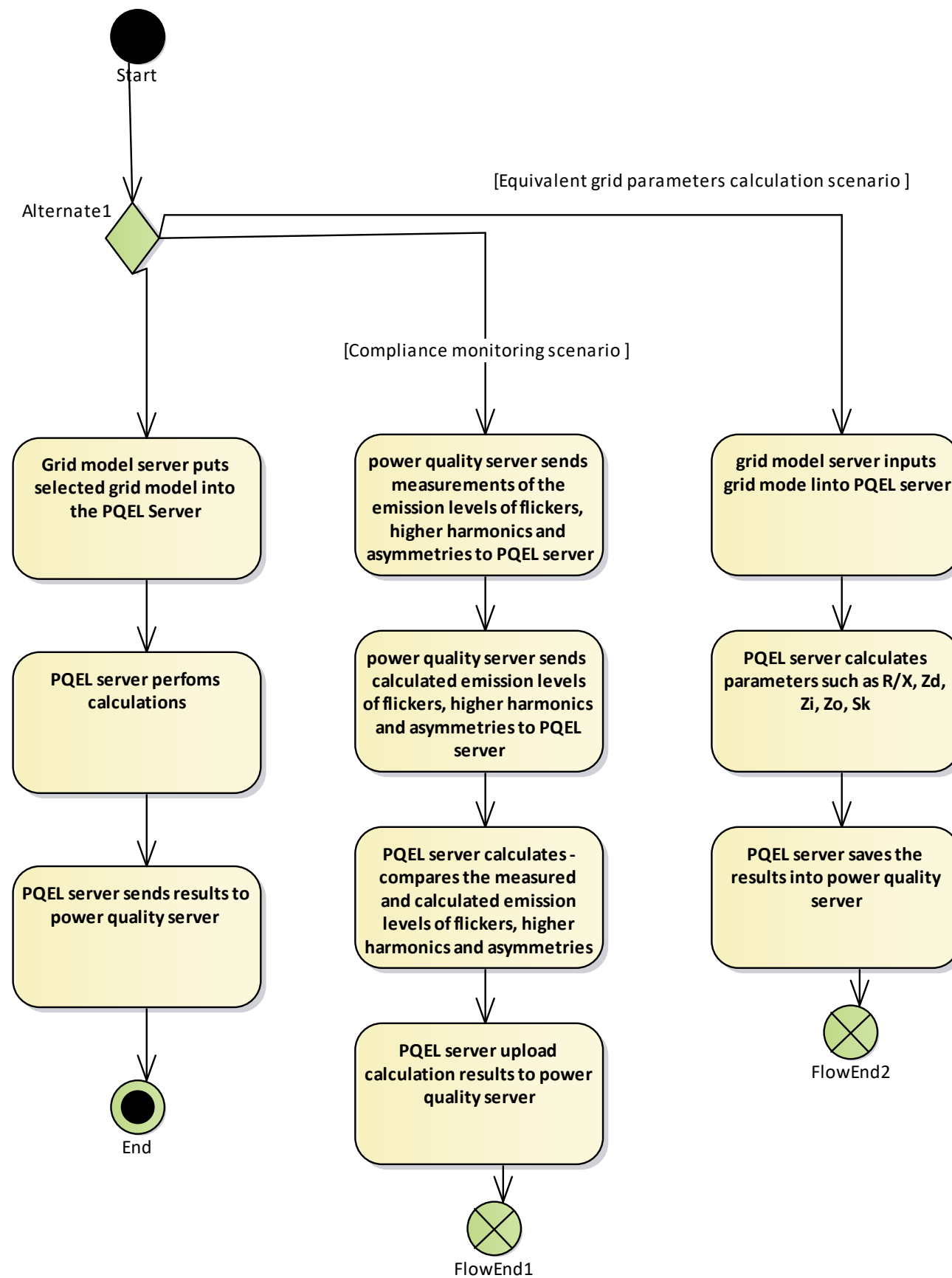


Figure 149 - UC09 Activity Graph

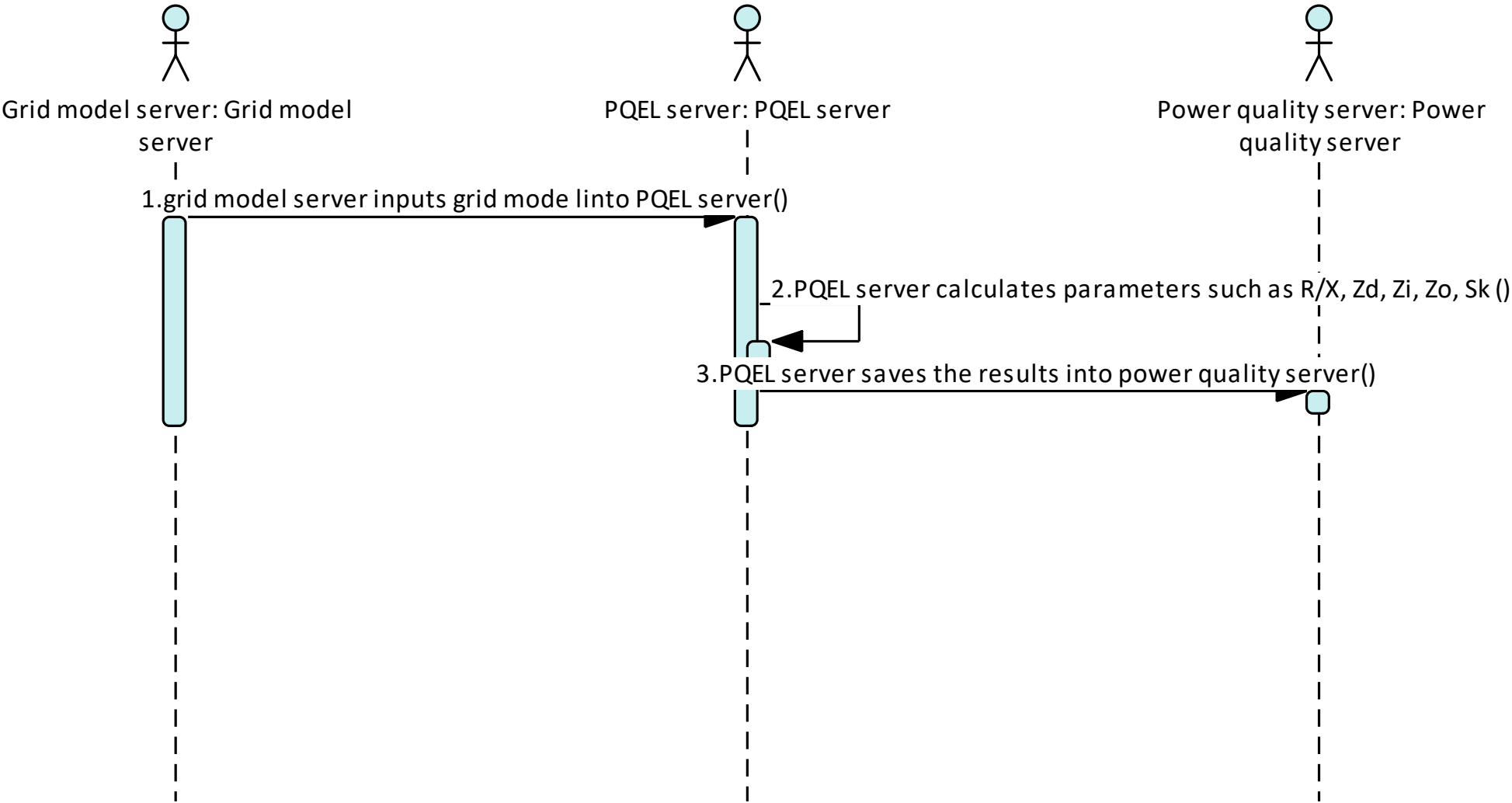


Figure 150 - UC09 Basic Path (1)

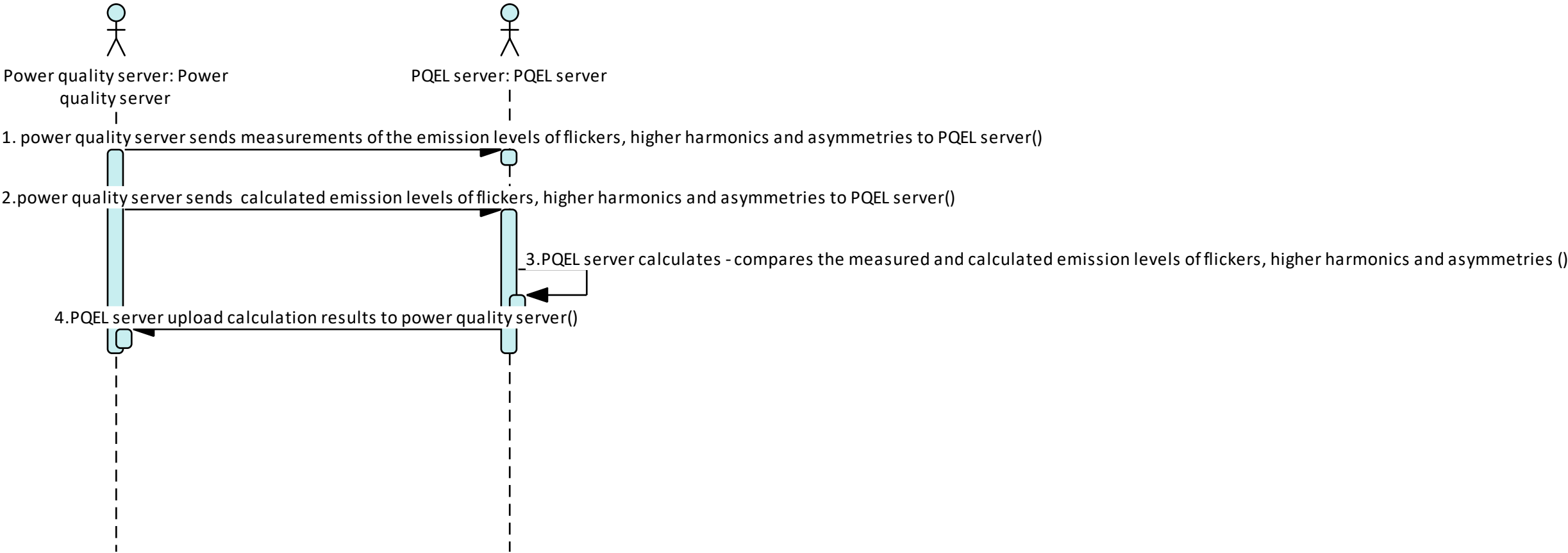


Figure 151 - UC09 Basic Path (2)

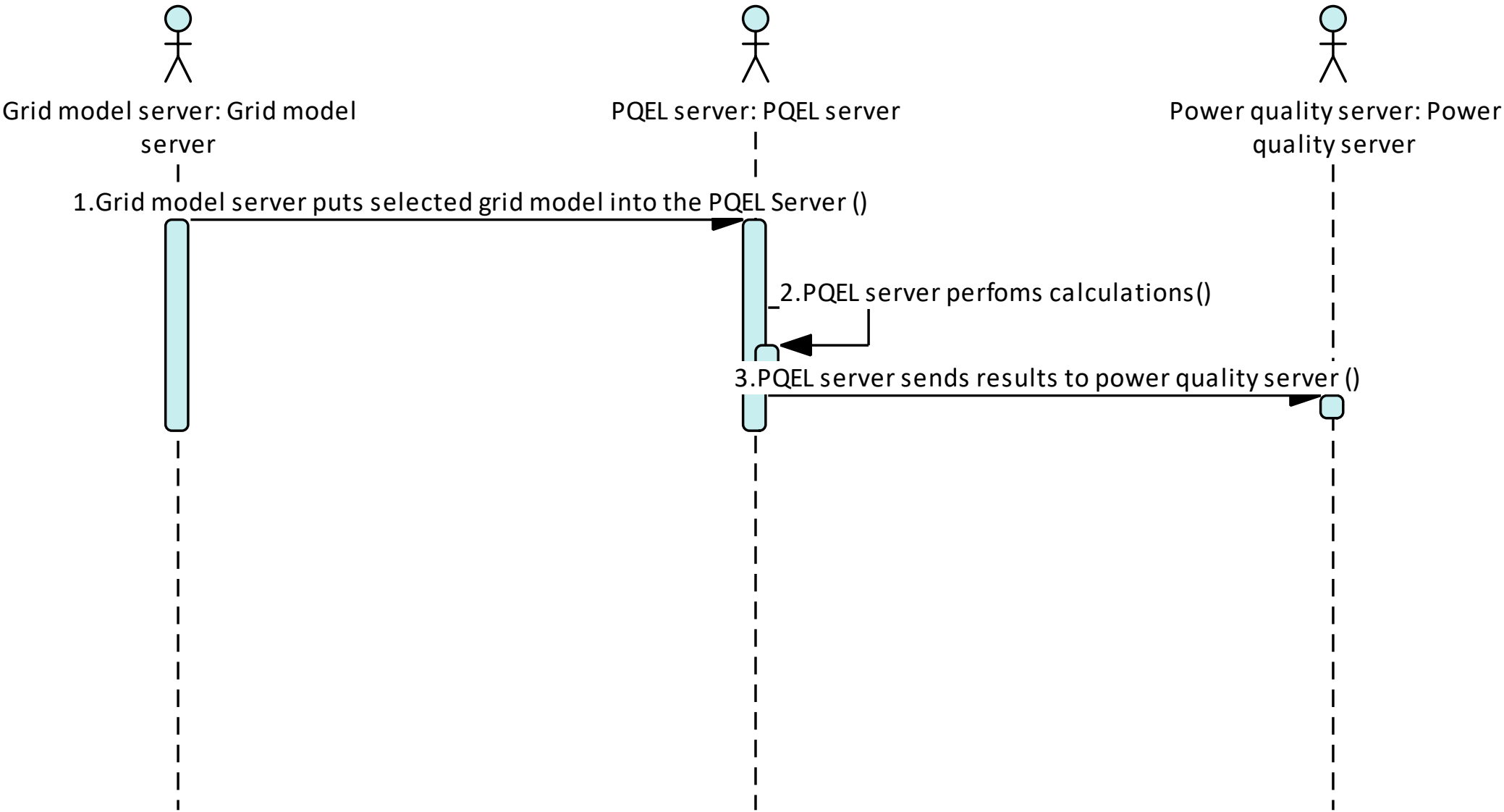


Figure 152 - UC09 Basic Path (3)

UC13 - Cost sharing of remedial actions with cross-border impact

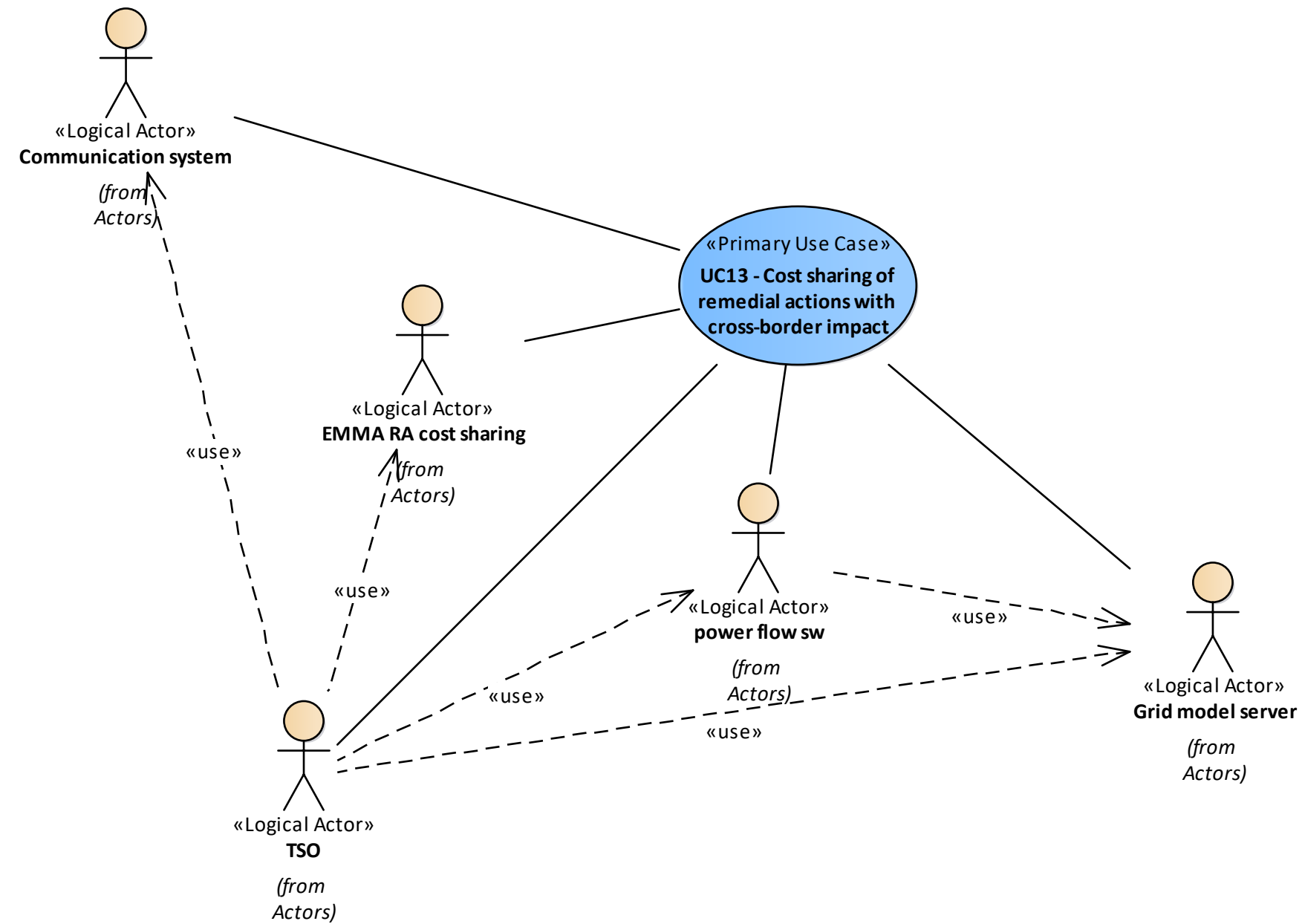


Figure 153 - UC13 Actors Involved

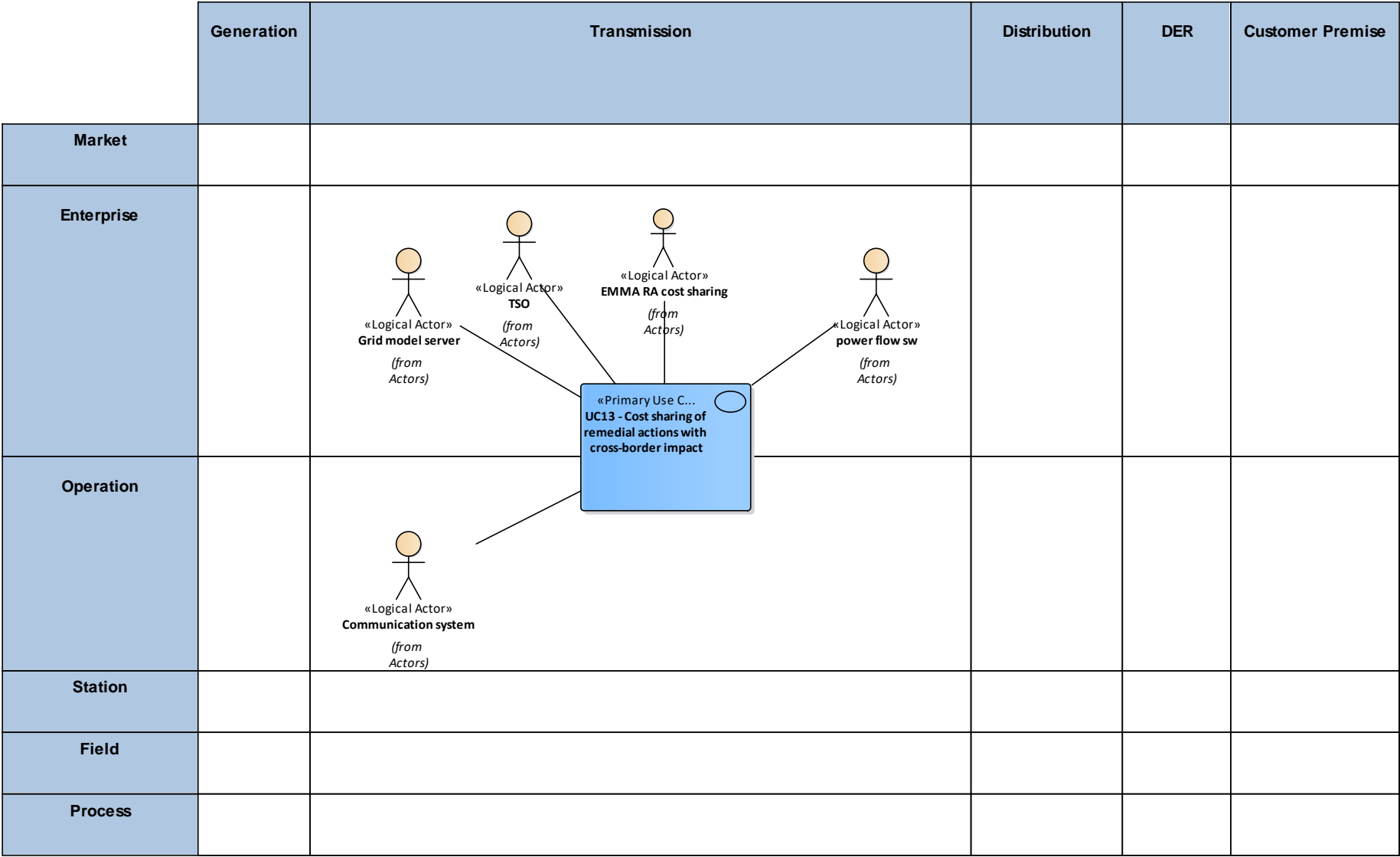


Figure 154- UC13 Functional Layer

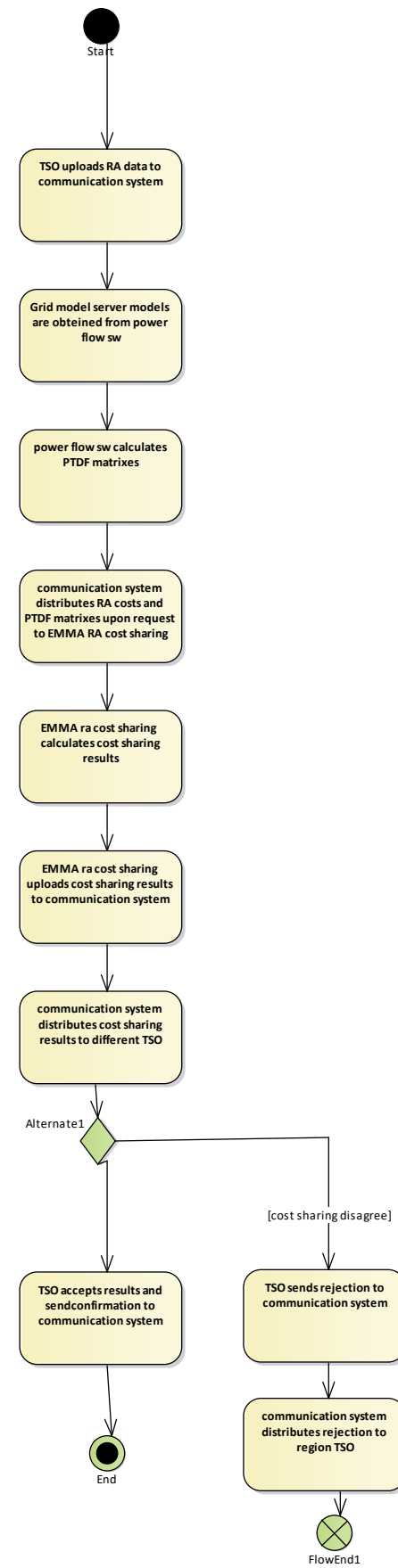


Figure 155 - UC13 Activity Graph

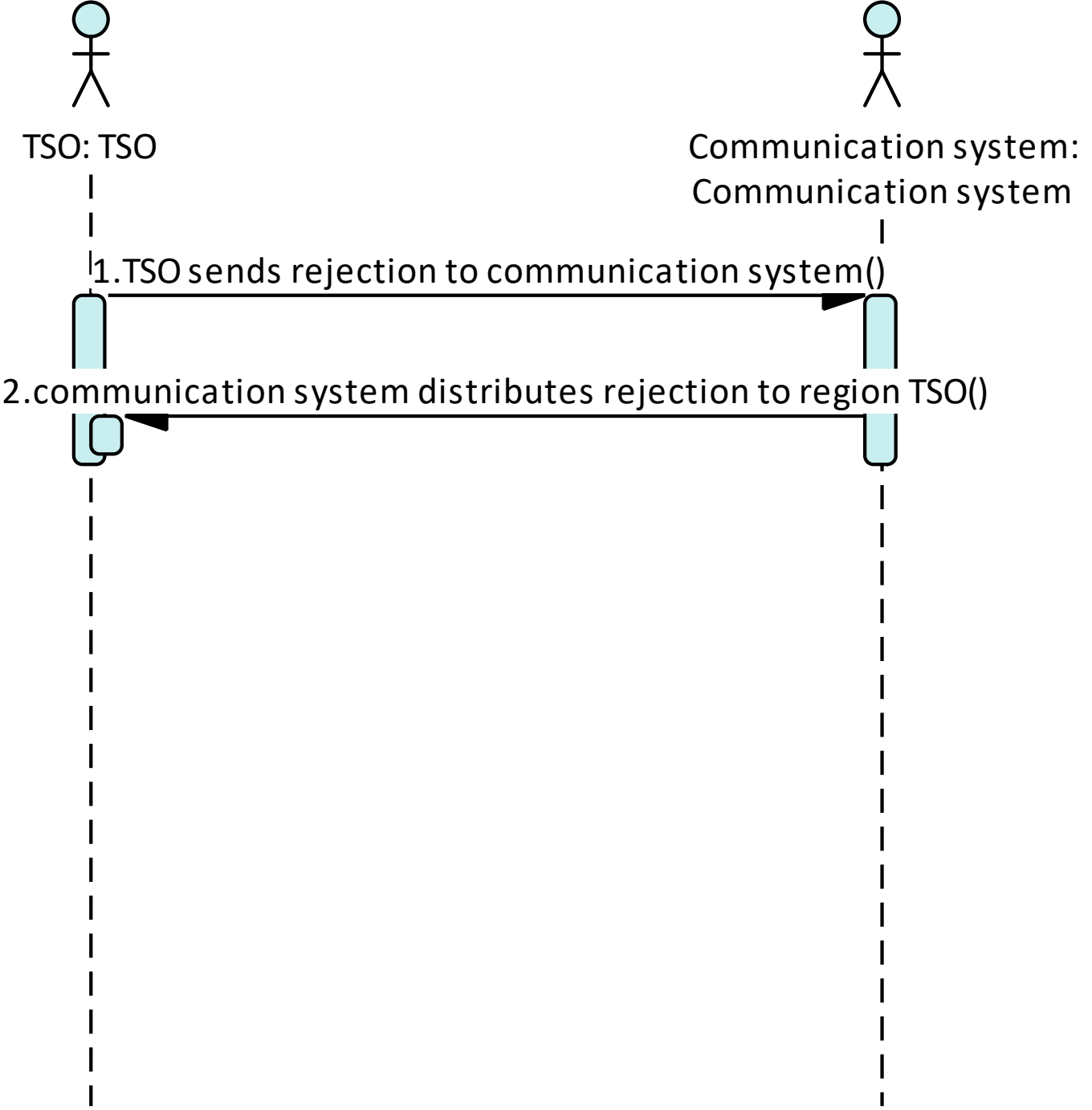


Figure 156 - UC13 Basic Path (1)

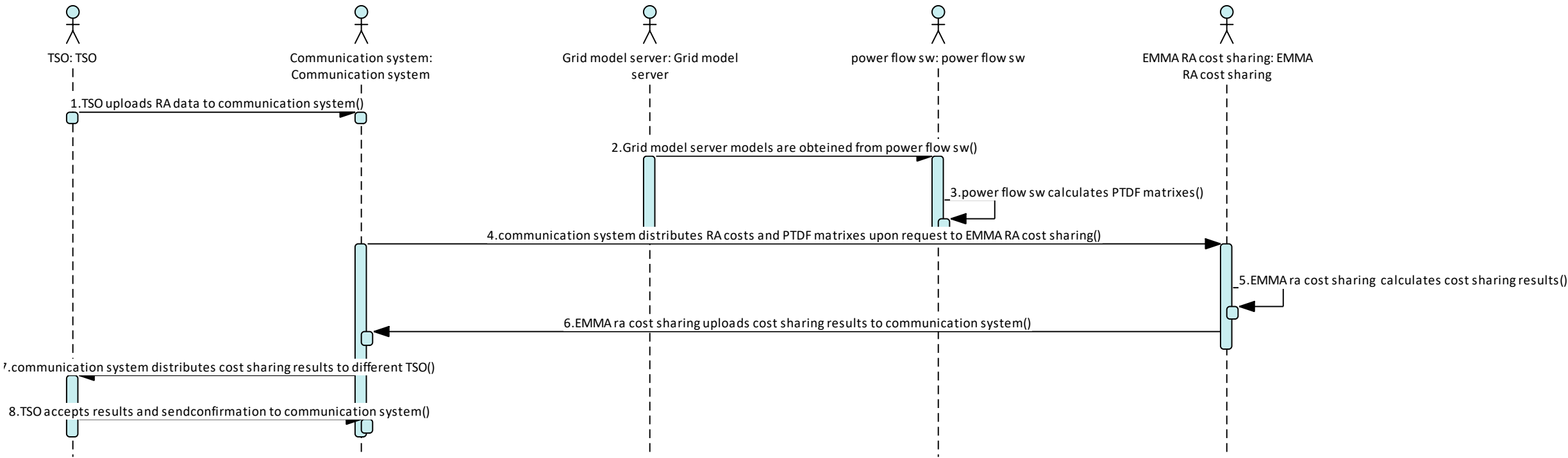


Figure 157 - UC13 Basic Path (2)

UC14 - Automation of transient stability calculations for operation planning purposes

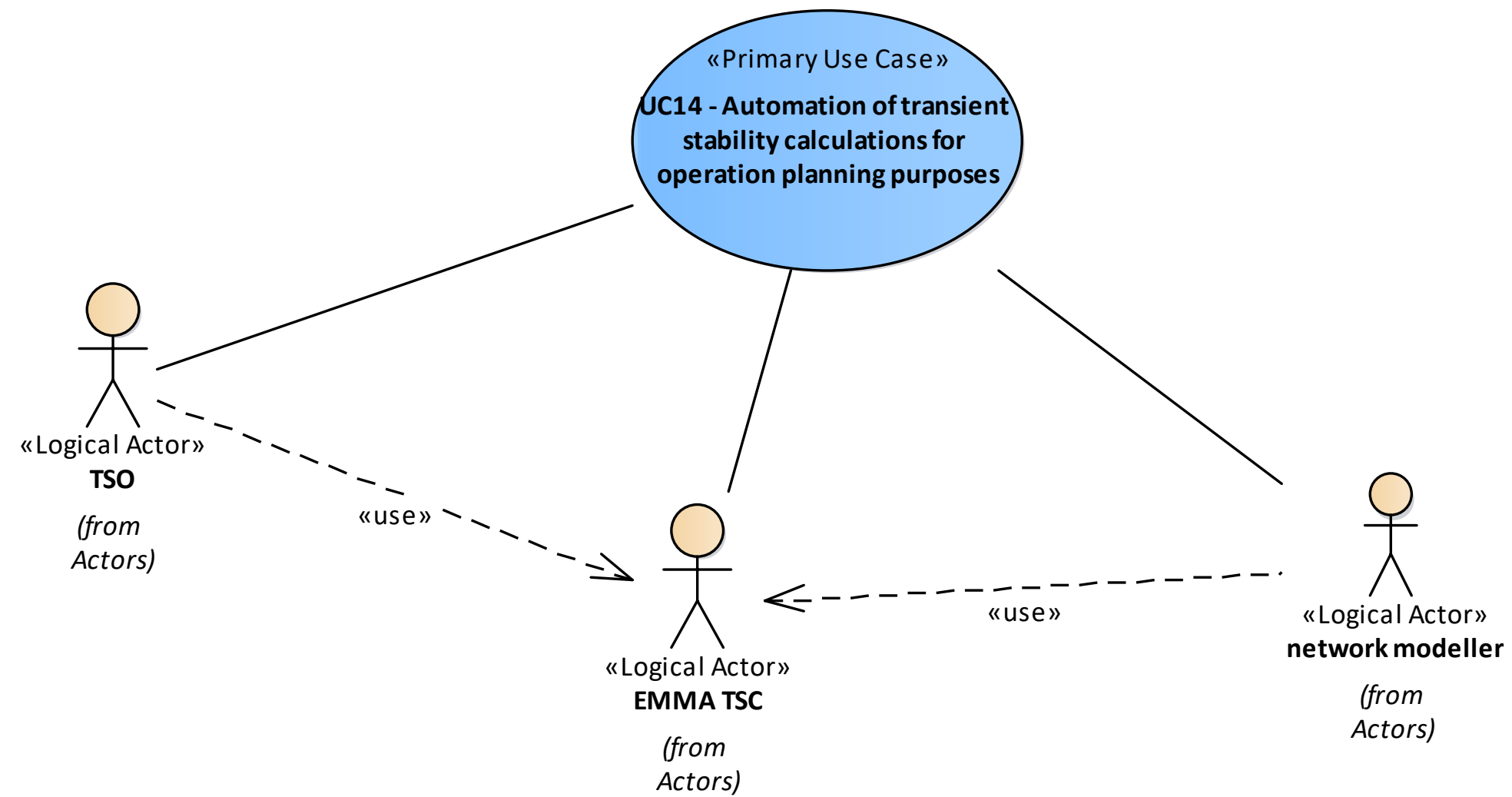


Figure 158 - UC14 Actors Involved



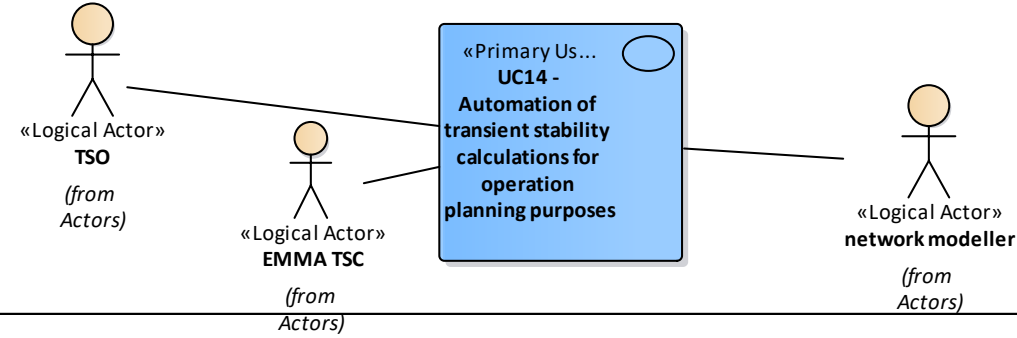
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 159 - UC14 Functional Layer

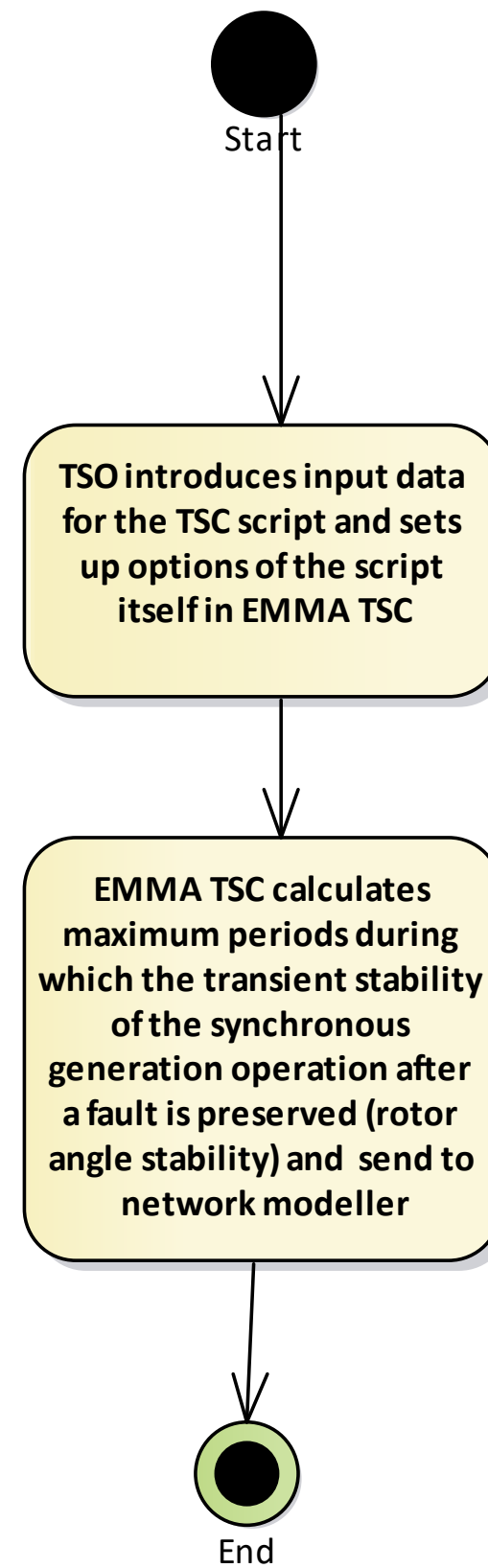


Figure 160 - UC14 Activity Graph

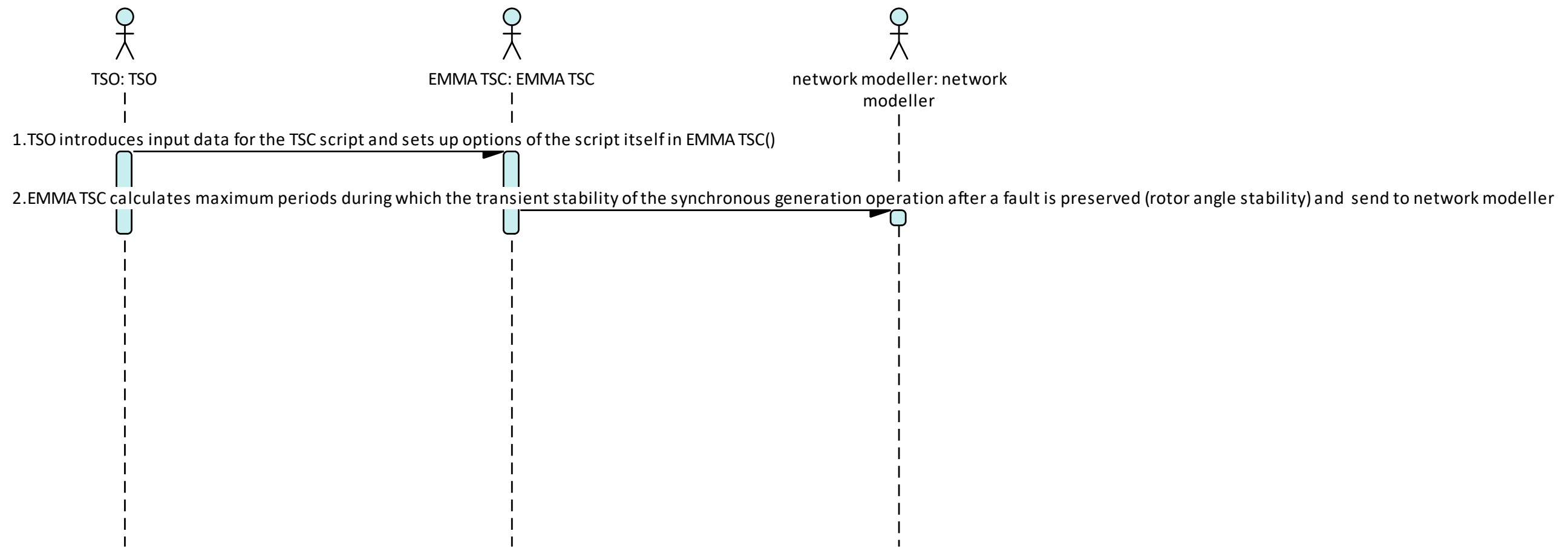


Figure 161 - UC14 Basic Path



UC17 -Outage coordination and automated creation of topology files for Individual Grid Models

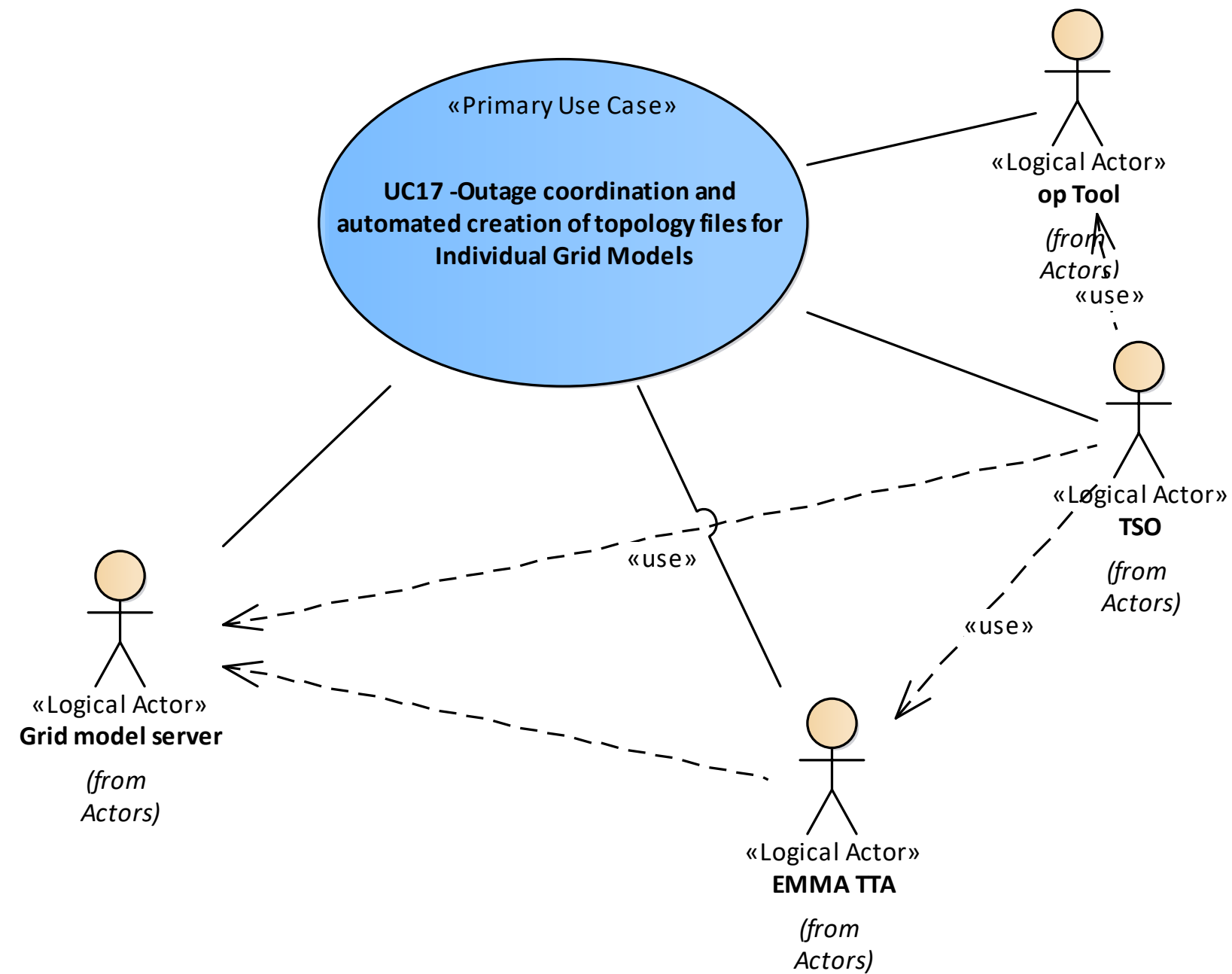


Figure 162 - UC17 Actors Involved



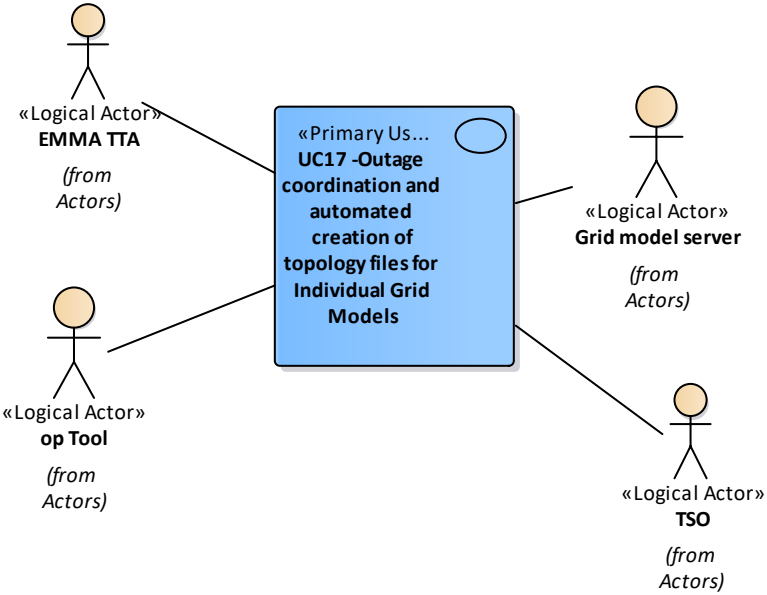
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 163 - UC17 Functional Layer

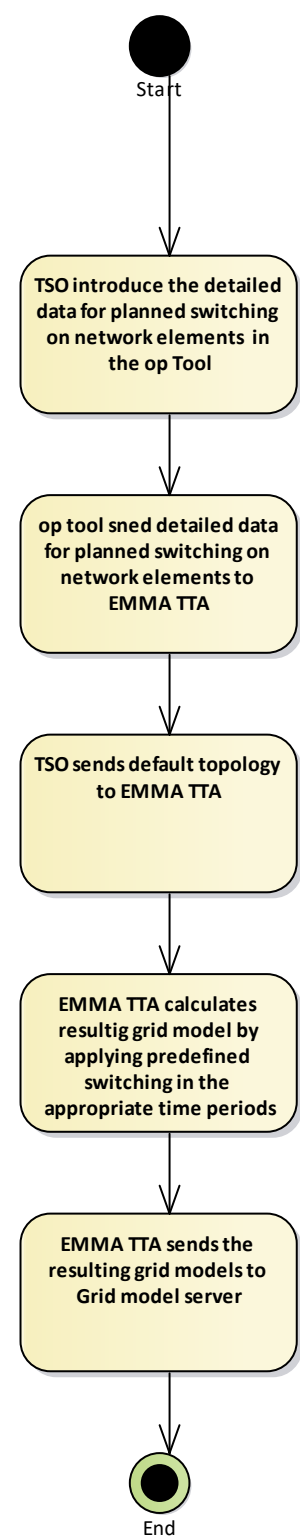


Figure 164 – UC17 Activity Graph

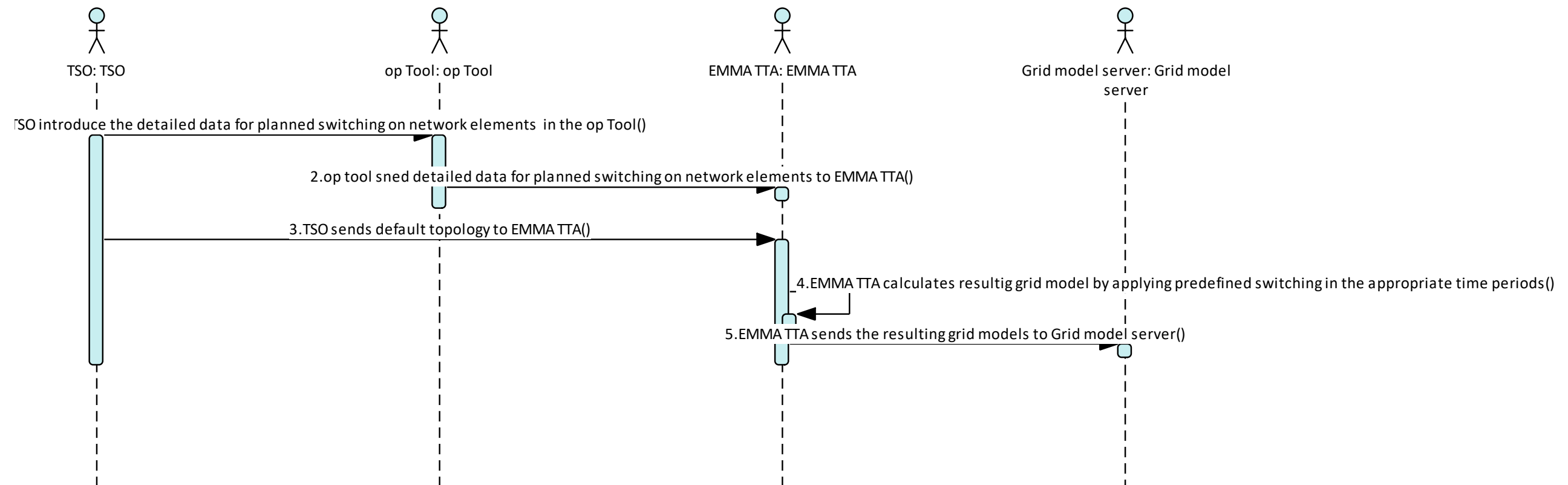


Figure 165 - UC17 Basic Path

UC20 - Physical security enhancement in core network components (Primary Substations)

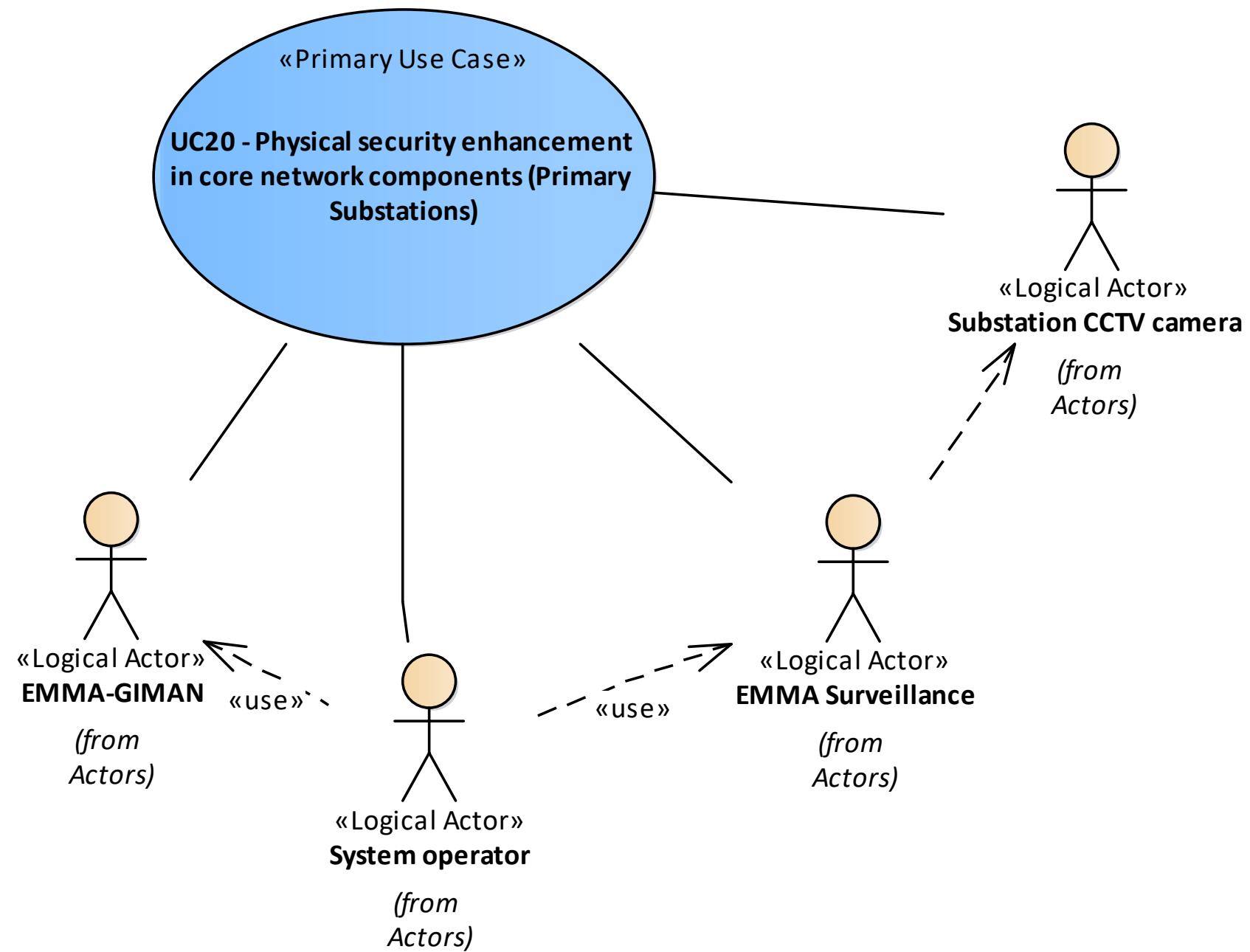


Figure 166 - UC20 Actors Involved

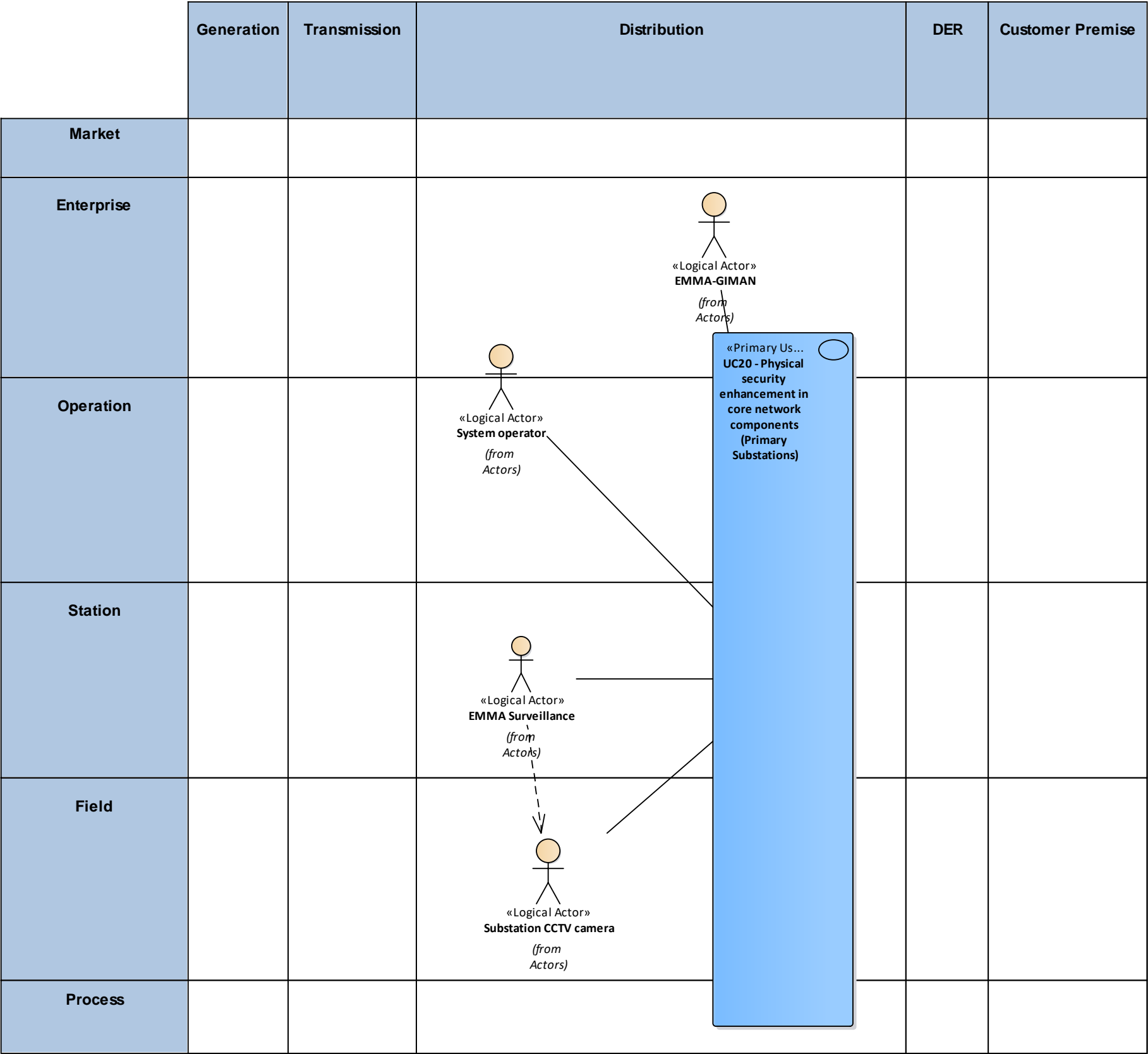


Figure 167 – UC20 Functional Layer

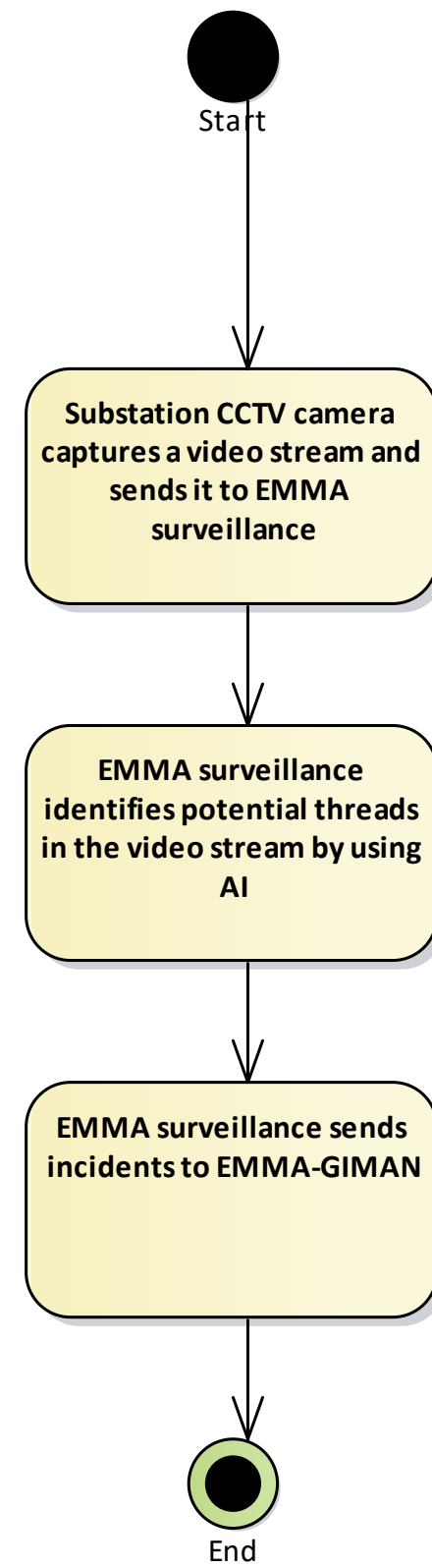


Figure 168 – UC20 Activity Graph

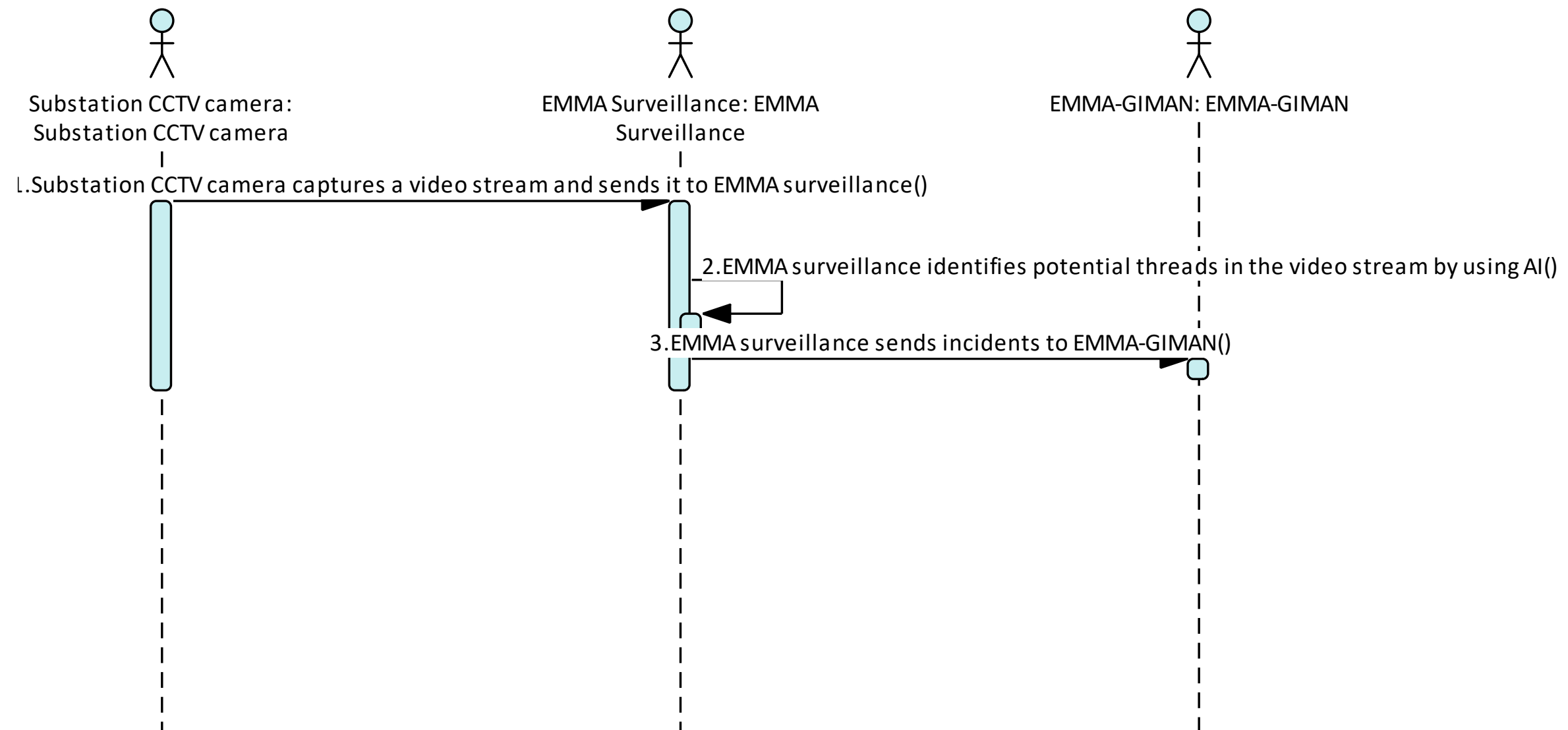


Figure 169 - UC20 Basic Path



UC31 - DLR integration with IGMs and SCADA/EMS

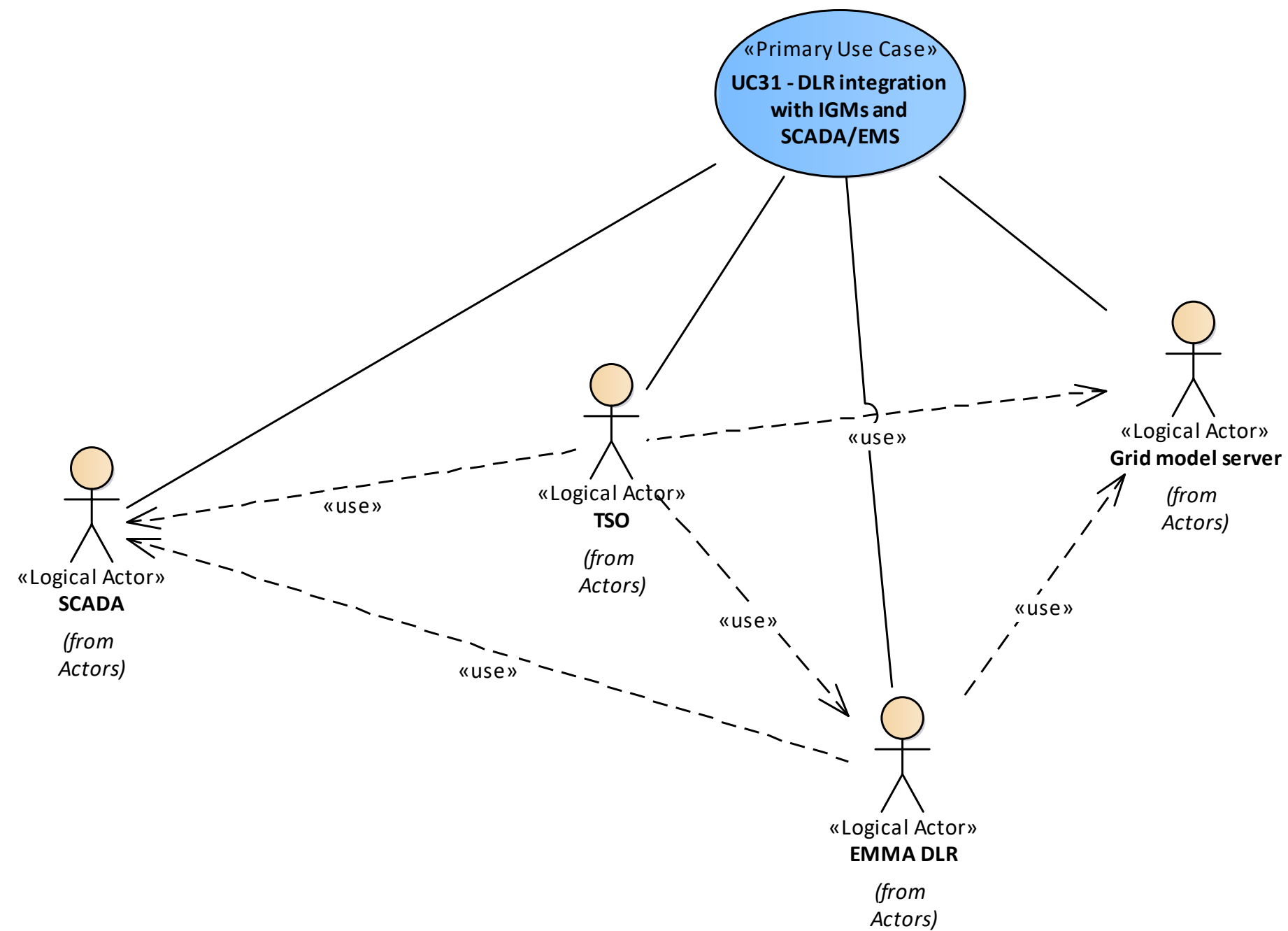


Figure 170 - UC31 Actors Involved



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 171 - UC31 Functional Layer

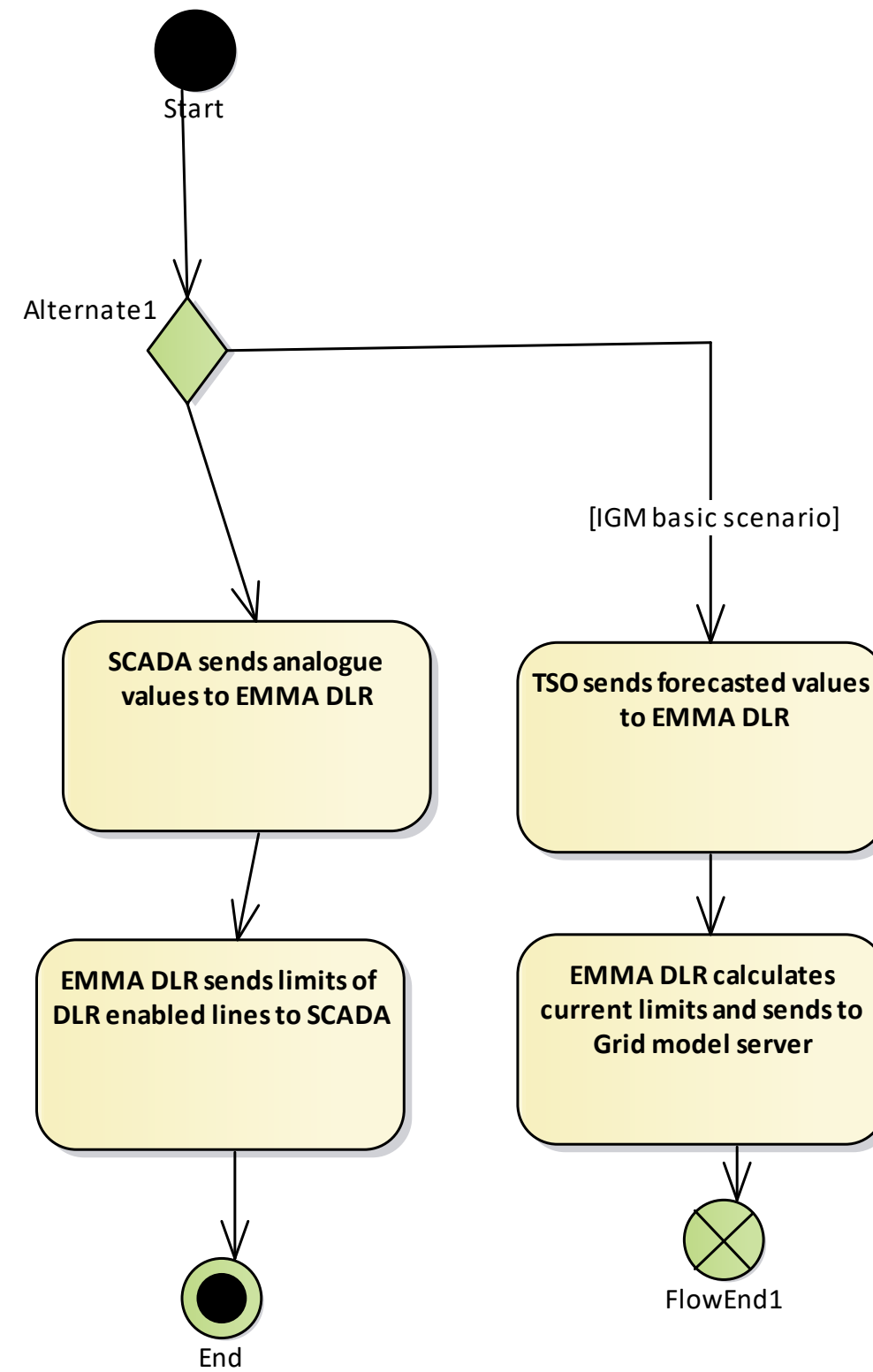


Figure 172 - UC31 Activity Graph

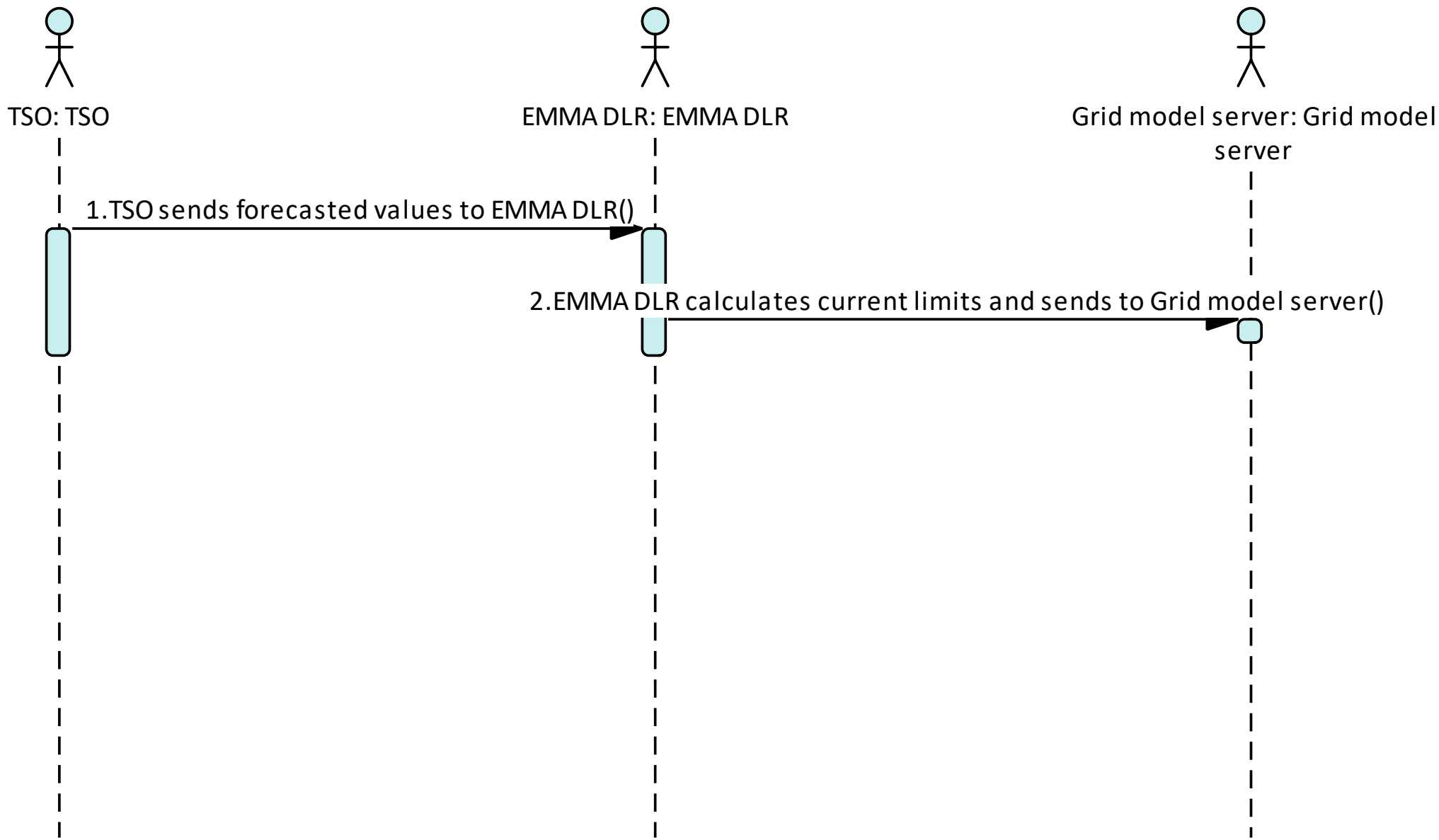


Figure 173 - UC31 Basic Path (1)

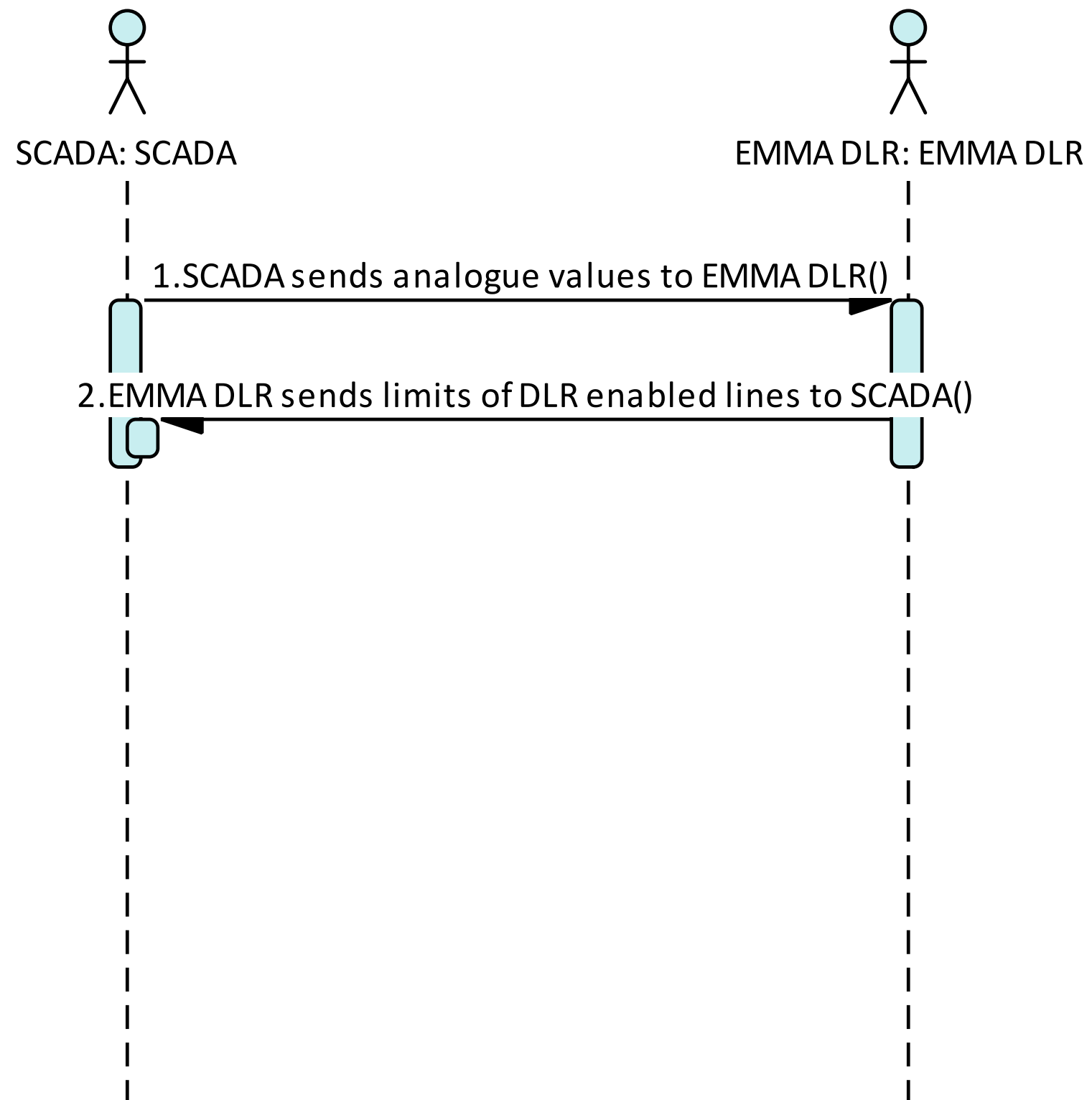


Figure 174 - UC31 Basic Path (2)



13.2 SGAM INFORMATION LAYER

13.2.1 Business Context View

13.2.1.1 WP3-C3PO

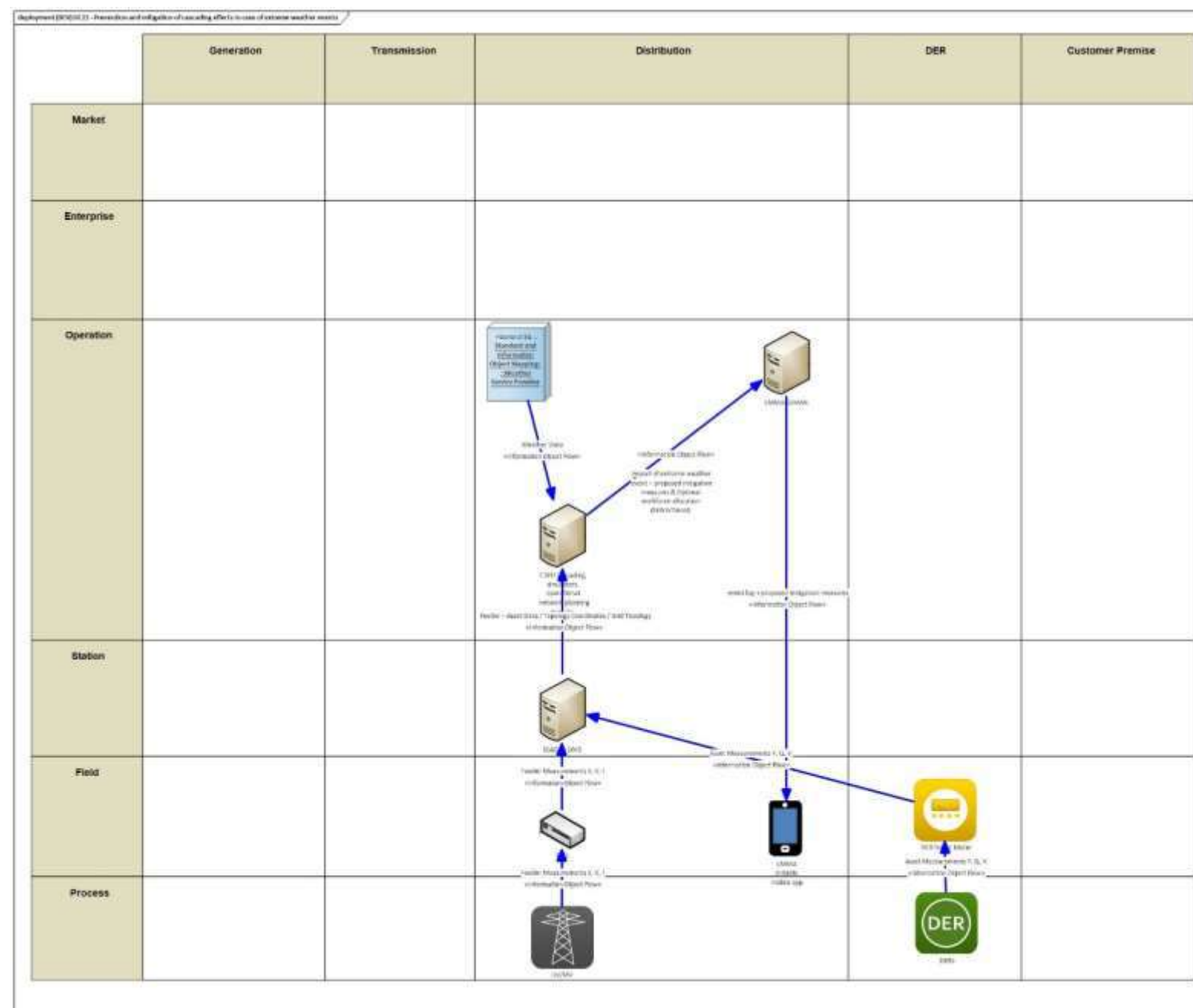


Figure 175 - UC22 Business Layer

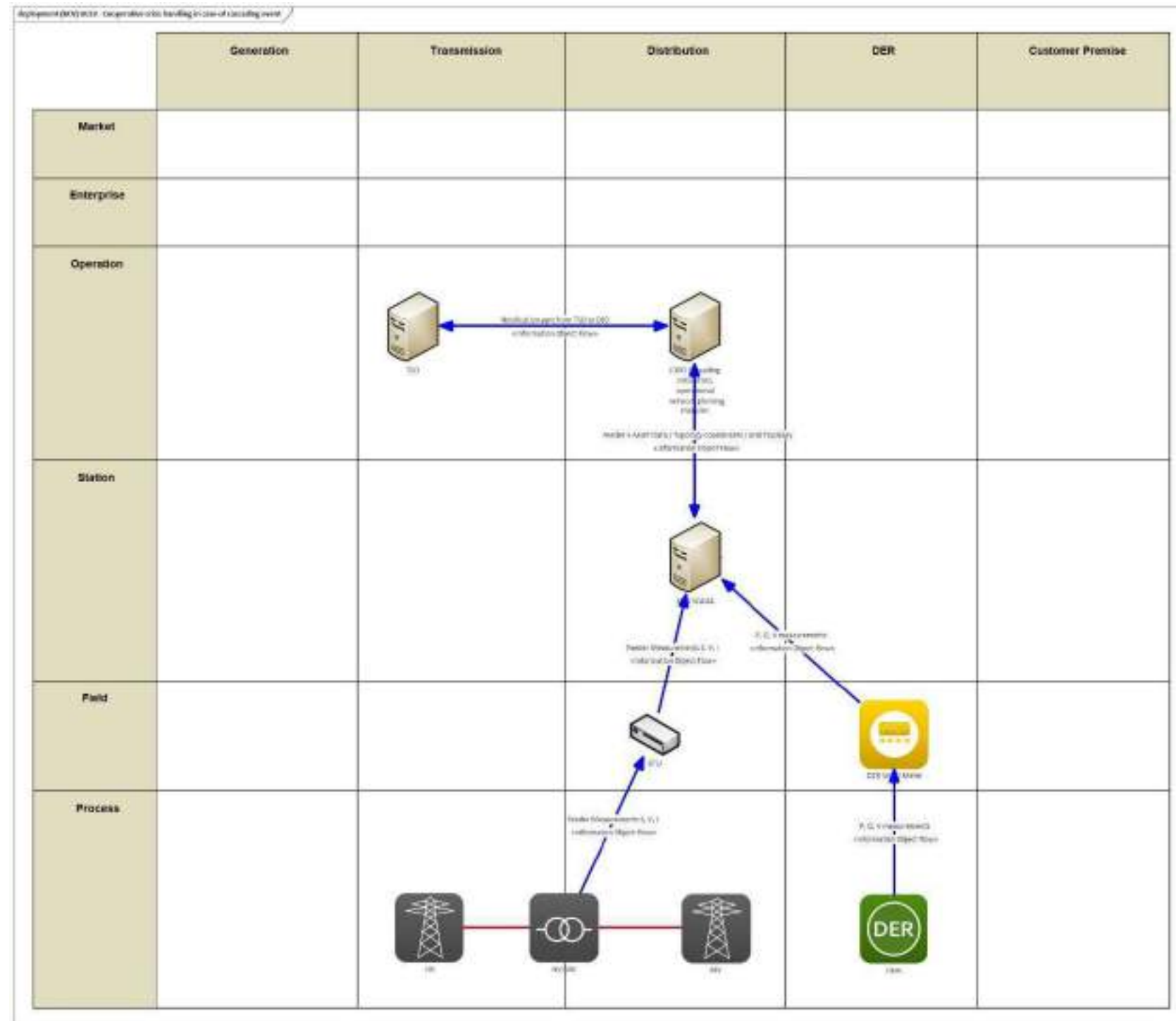


Figure 176 - UC23 Business Layer

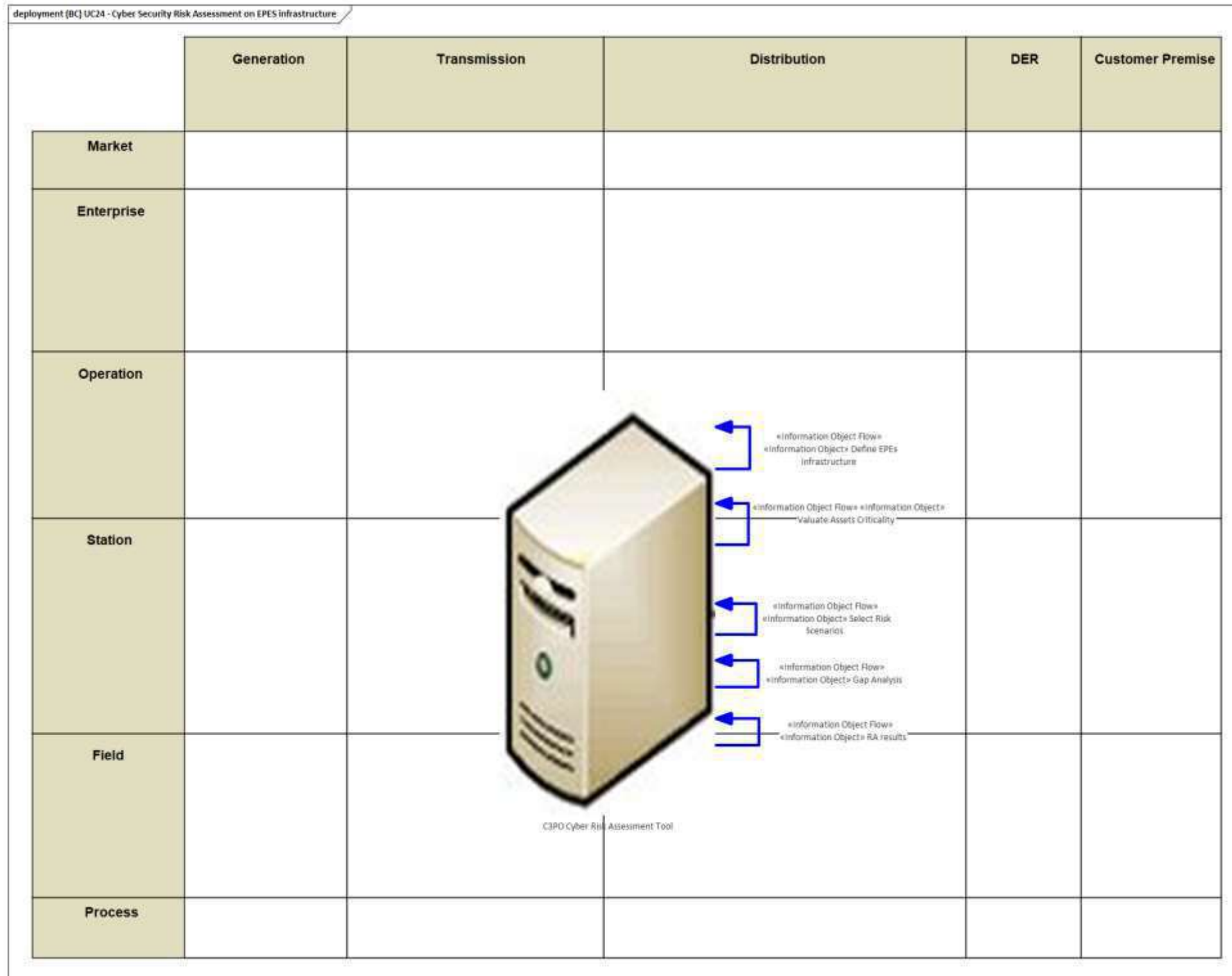


Figure 177 - UC24 Business Layer

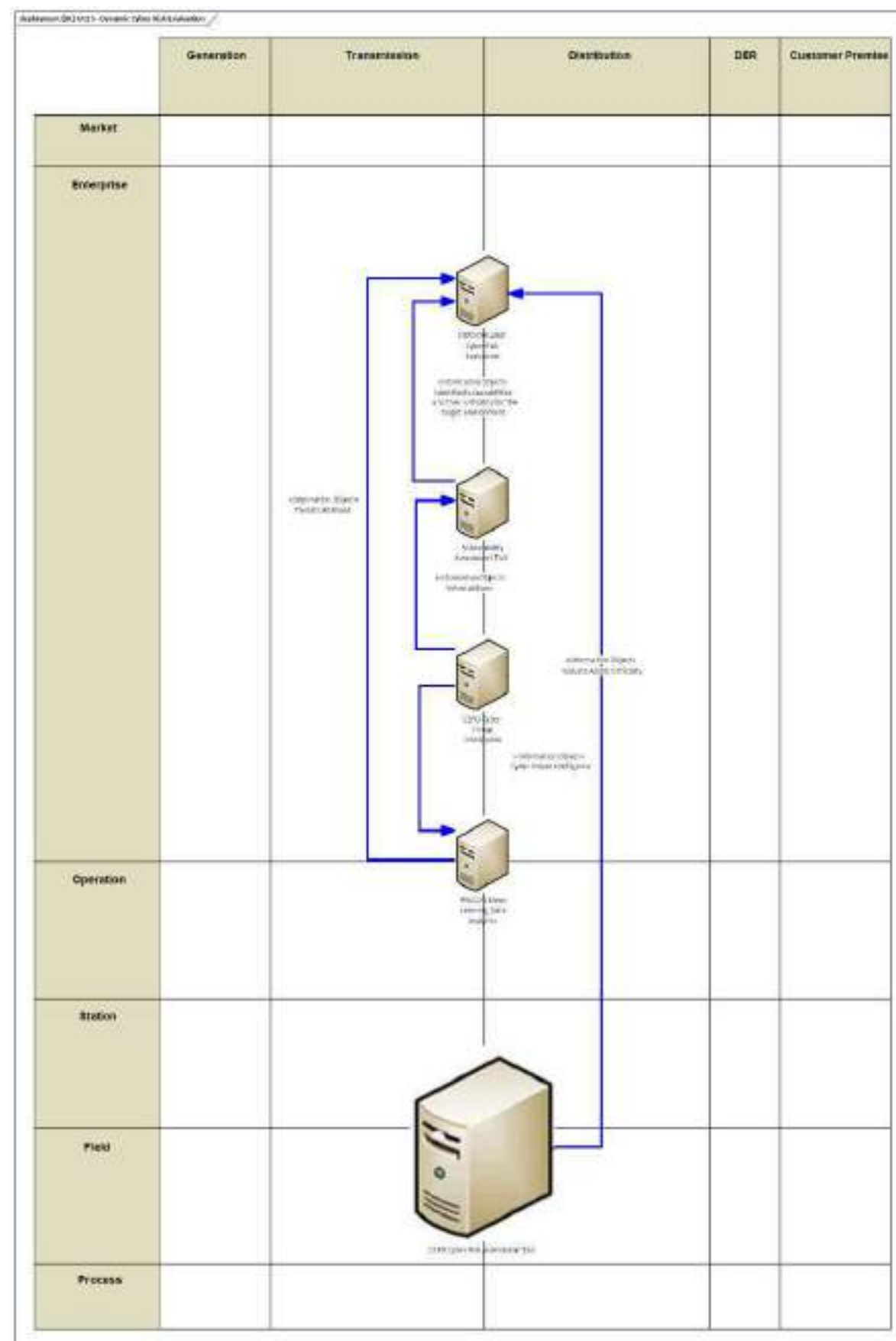


Figure 178 - UC25 Business Layer

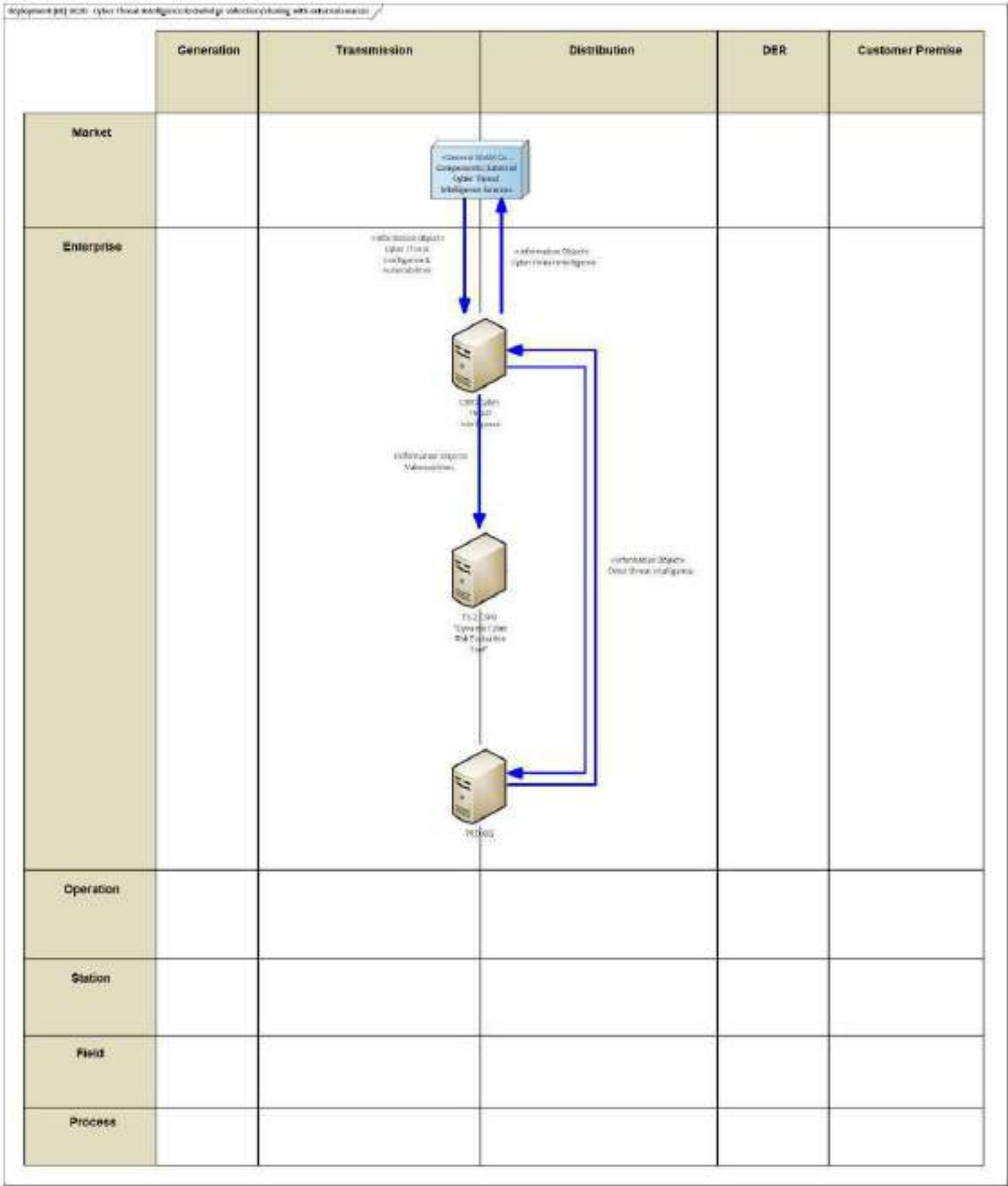


Figure 179 - UC26 Business Layer

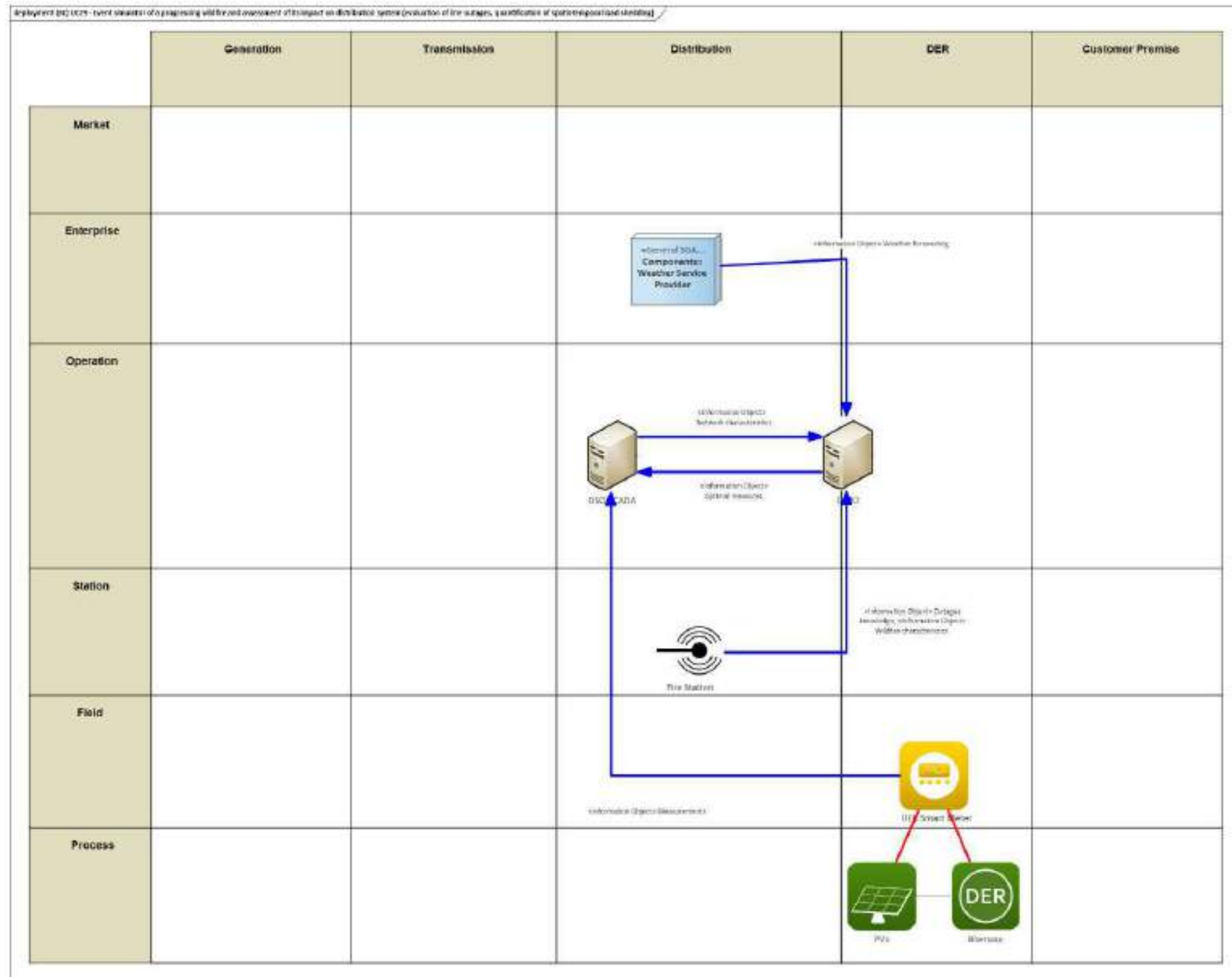


Figure 180 - UC29 Business Layer

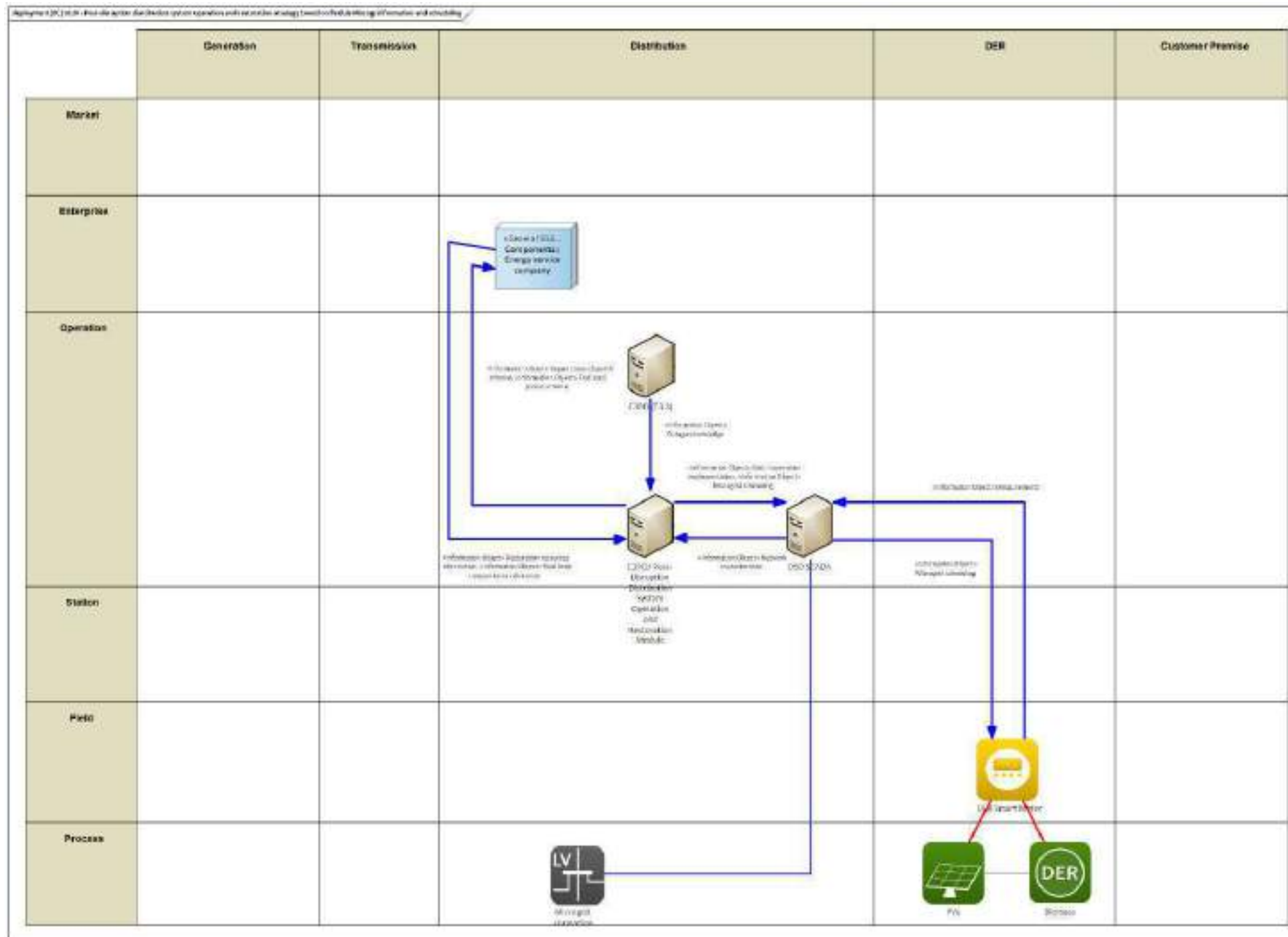


Figure 181 - UC30 Business Layer

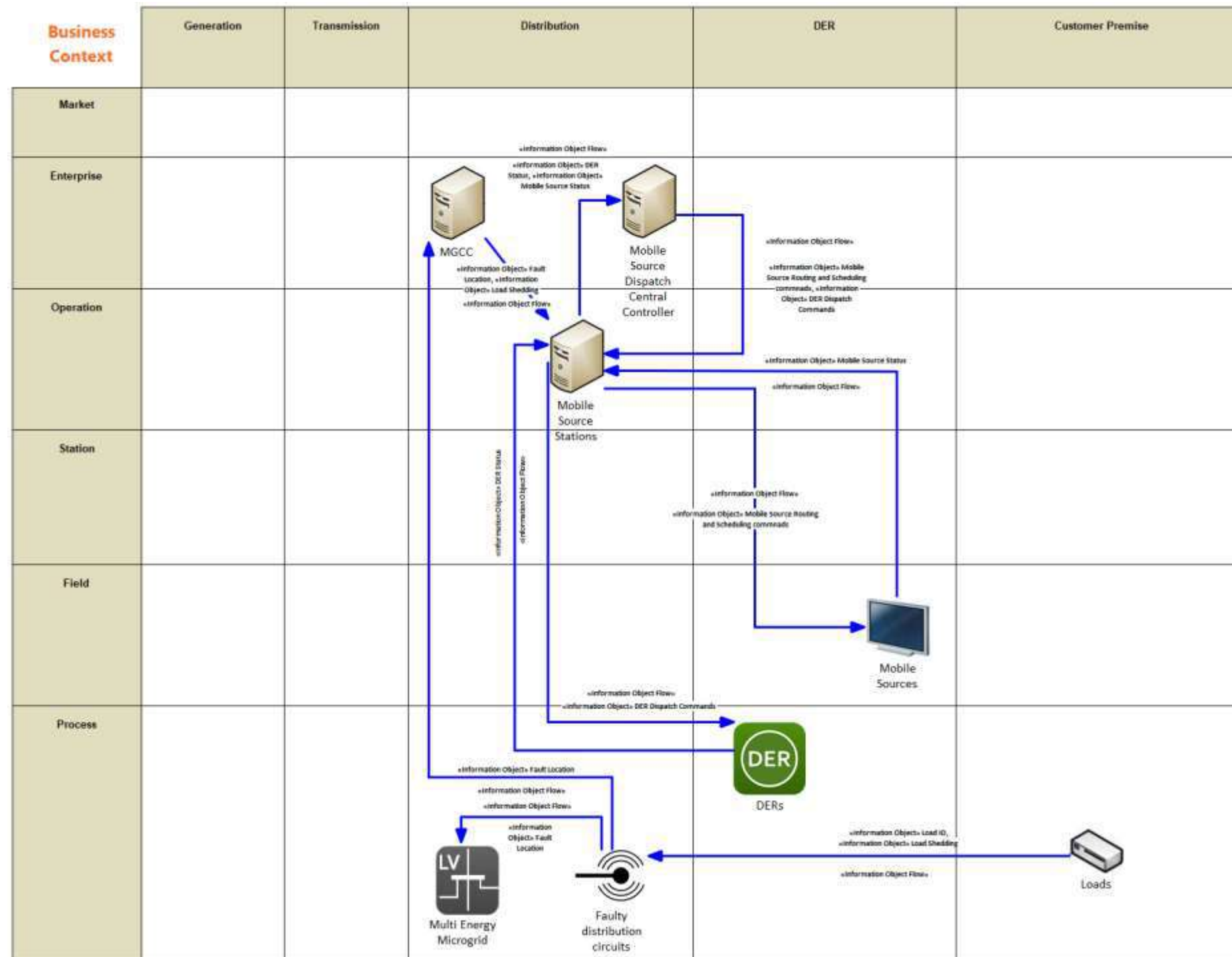


Figure 182 - UC32 Business Layer

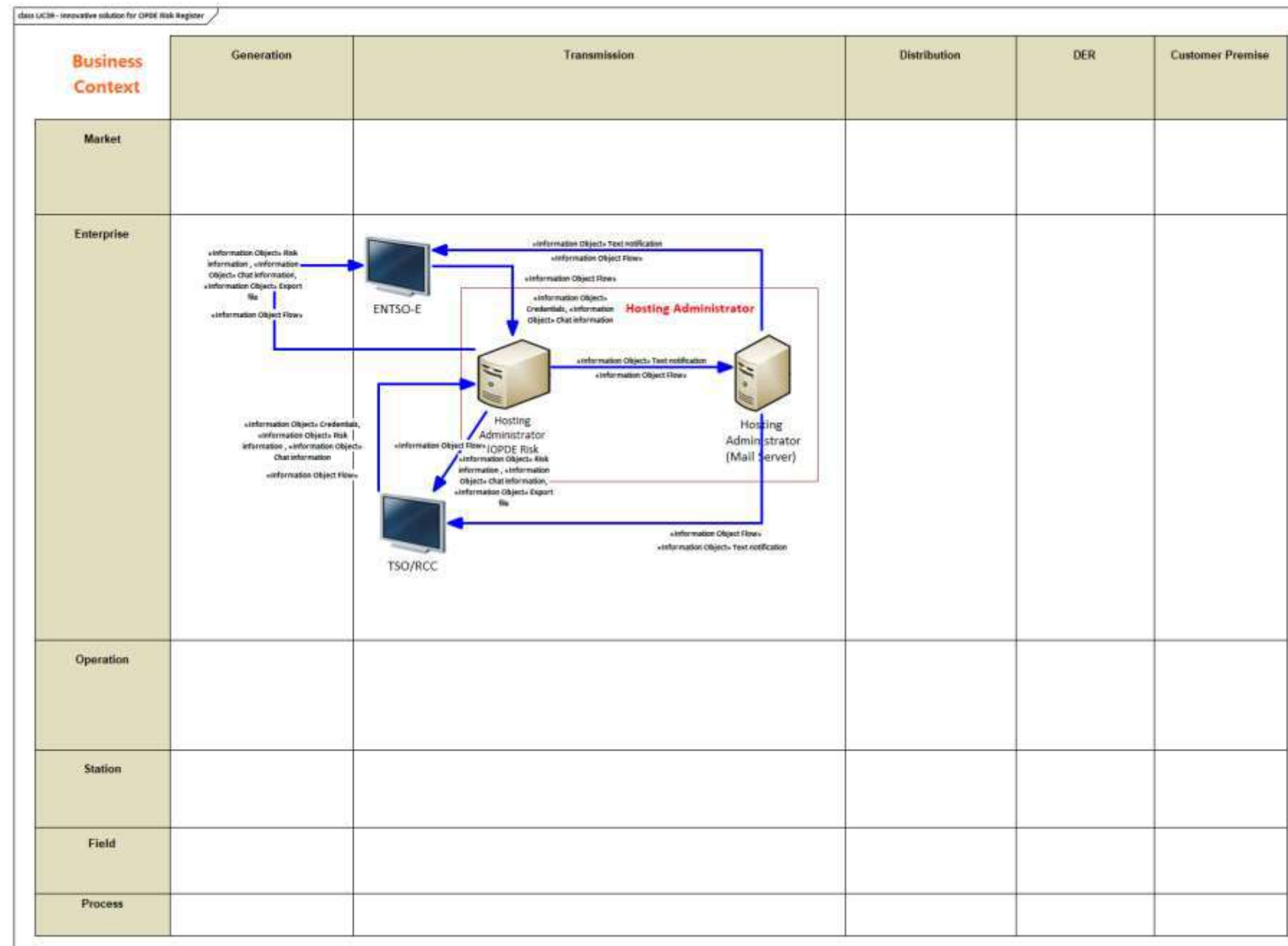


Figure 183 - UC39 Business Layer

13.2.1.2 WP4-IRIS

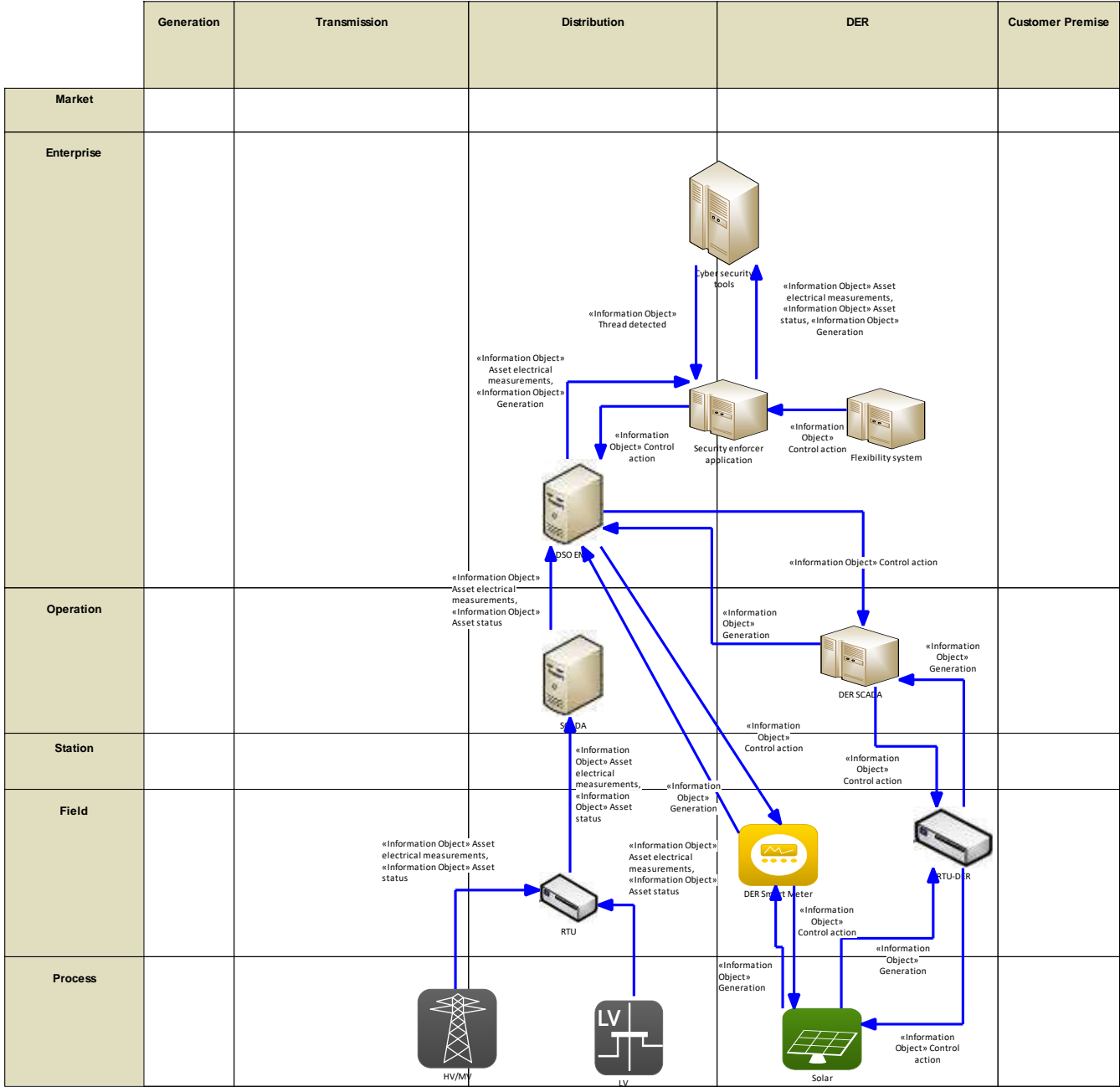


Figure 184 - UC07 Business Layer

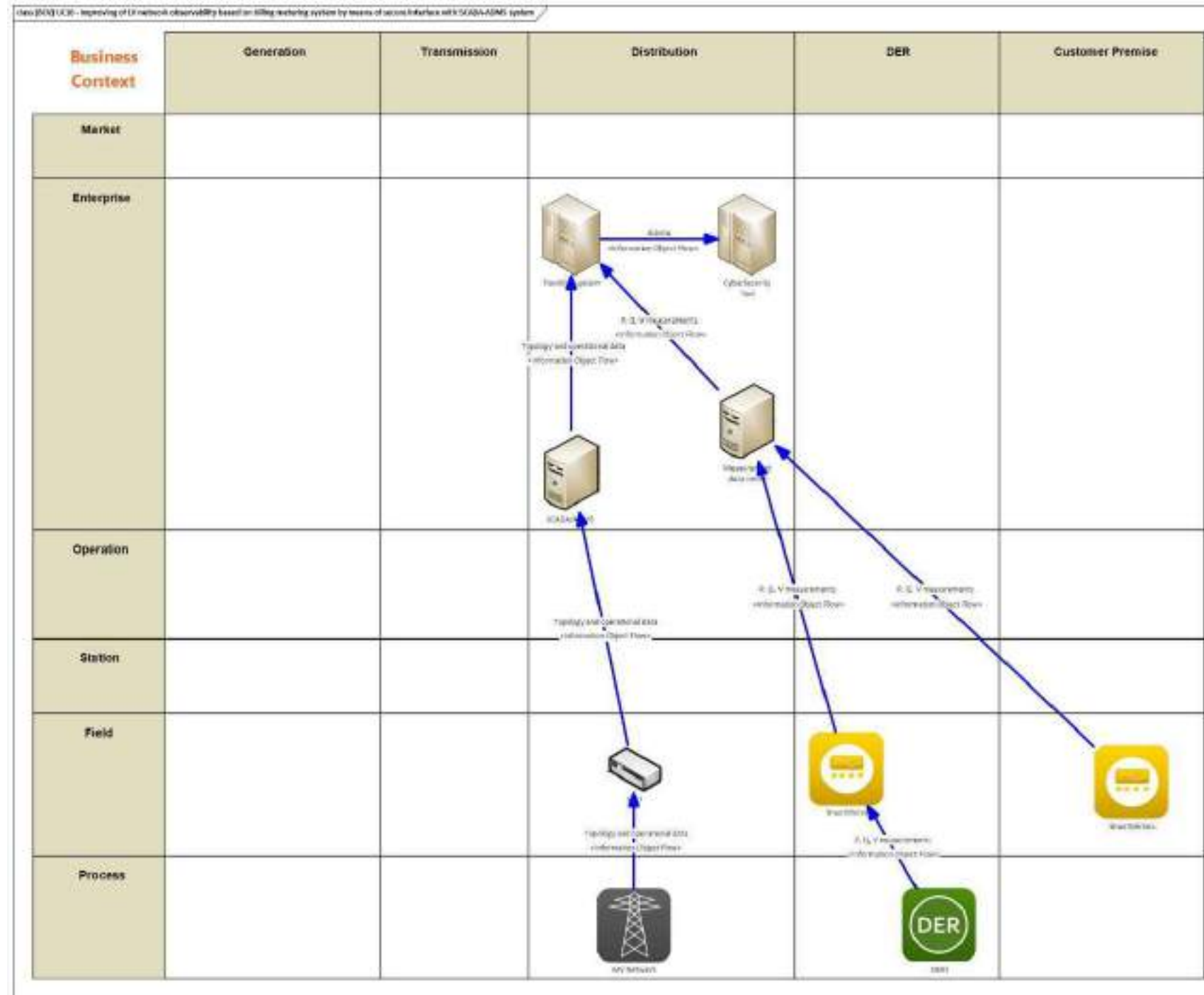


Figure 185 - UC10 Business Layer

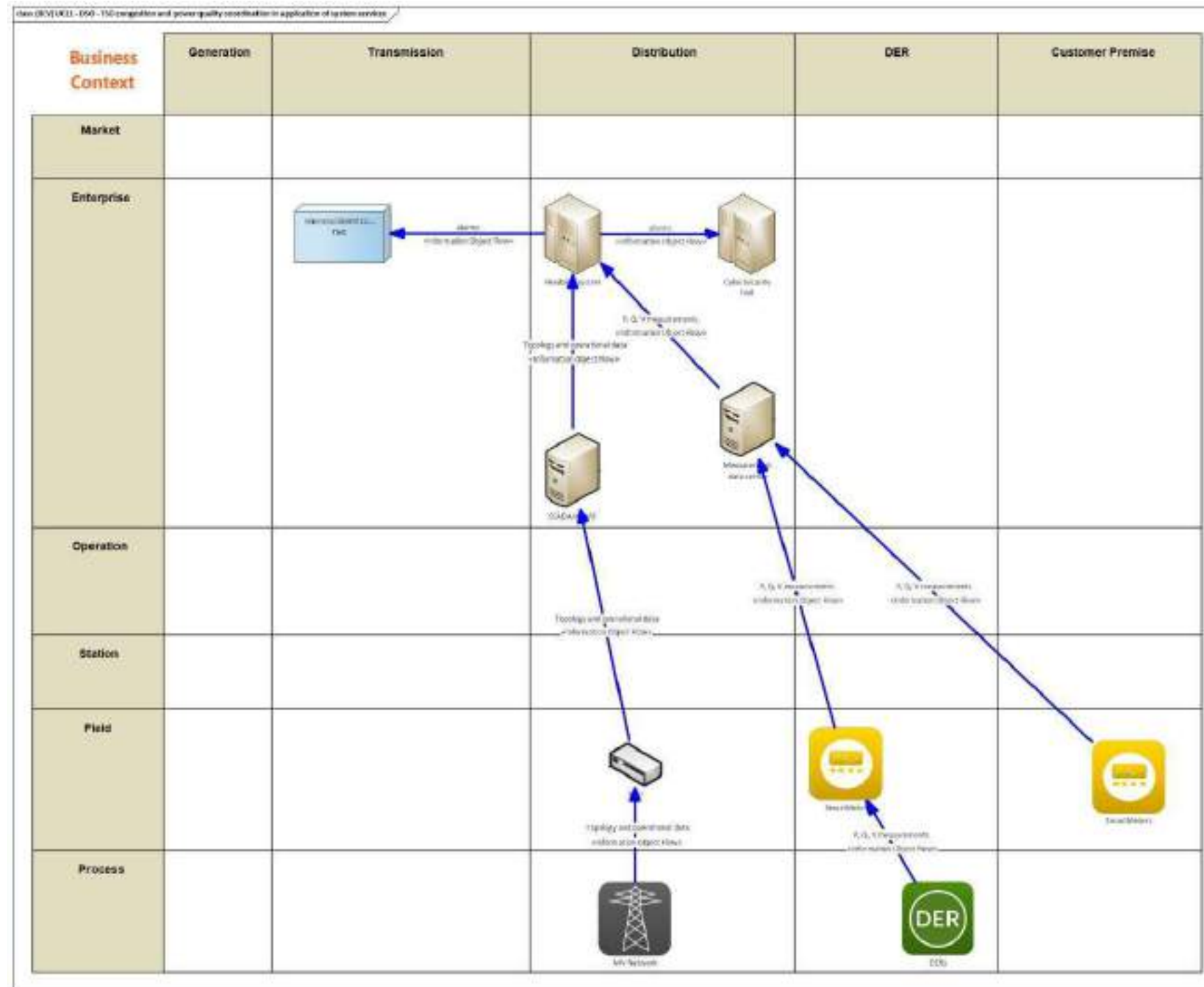


Figure 186 - UC11 Business Layer

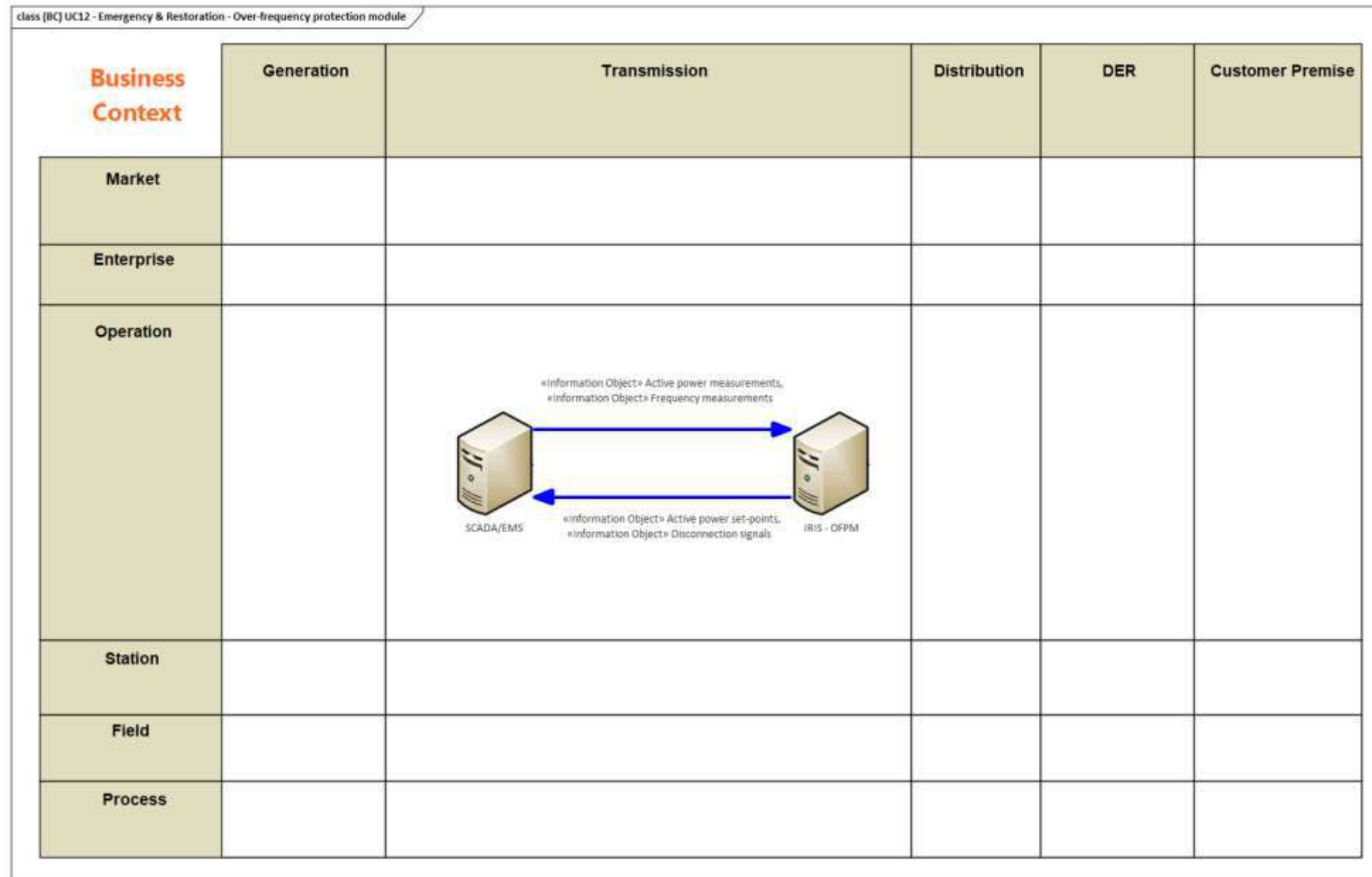


Figure 187 – UC12 Business Layer

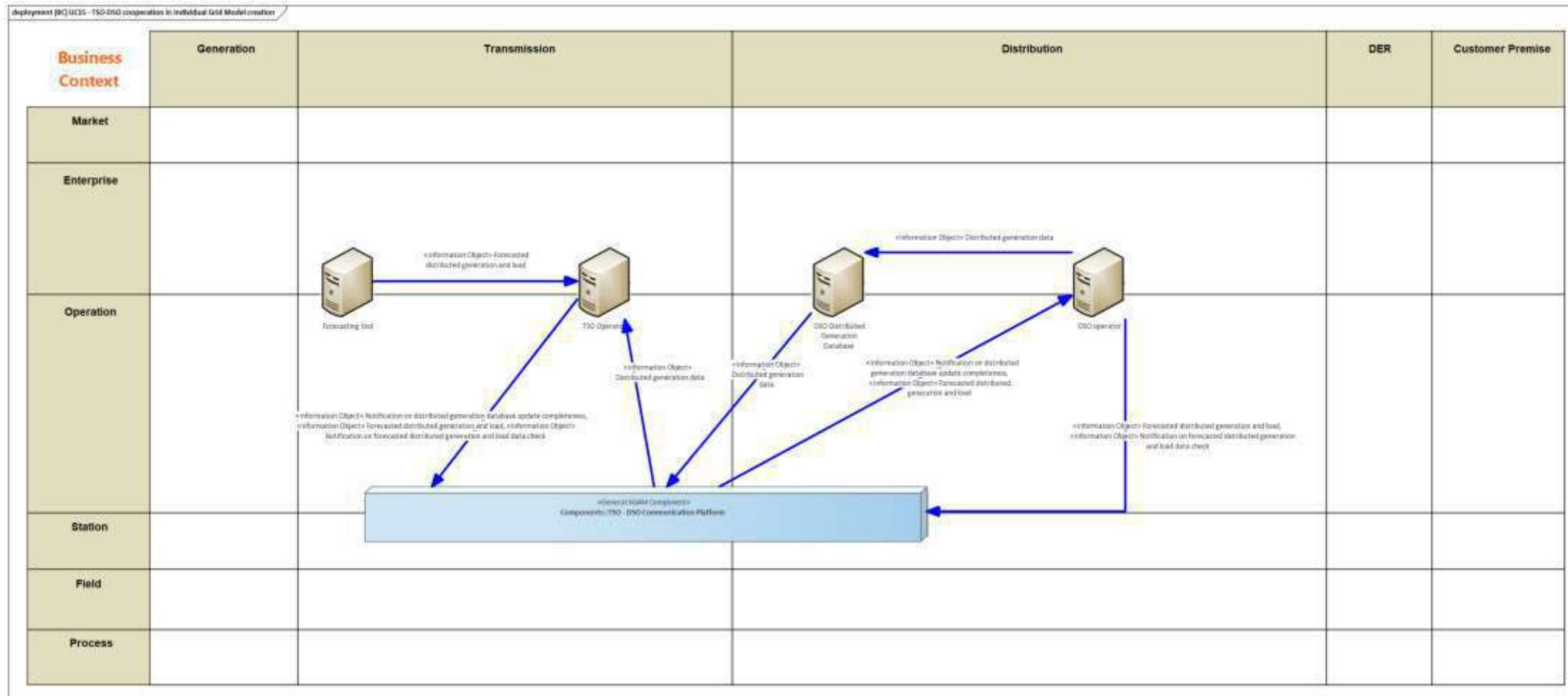


Figure 188 - UC15 Business Layer

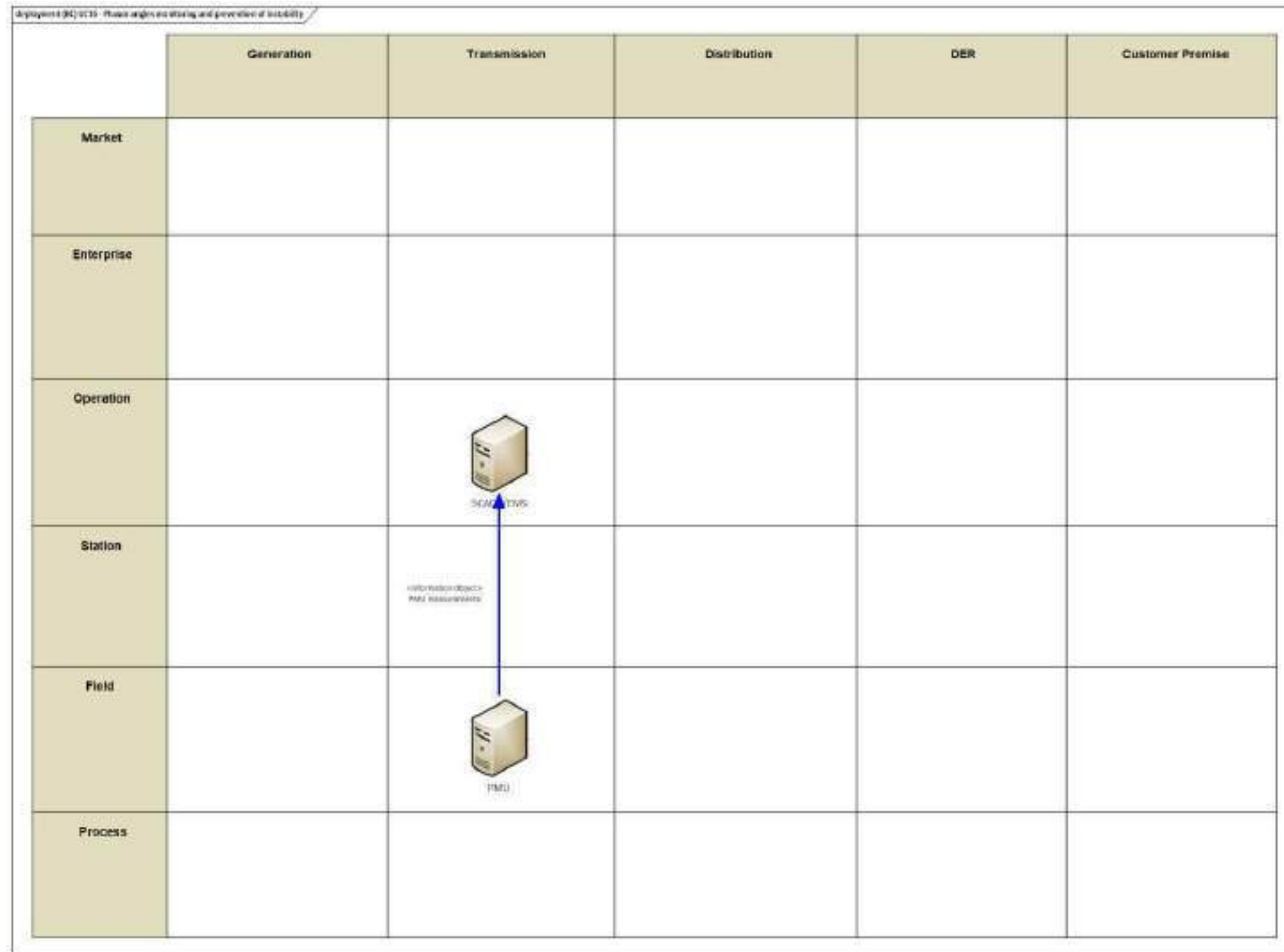


Figure 189 - UC16 Business Layer

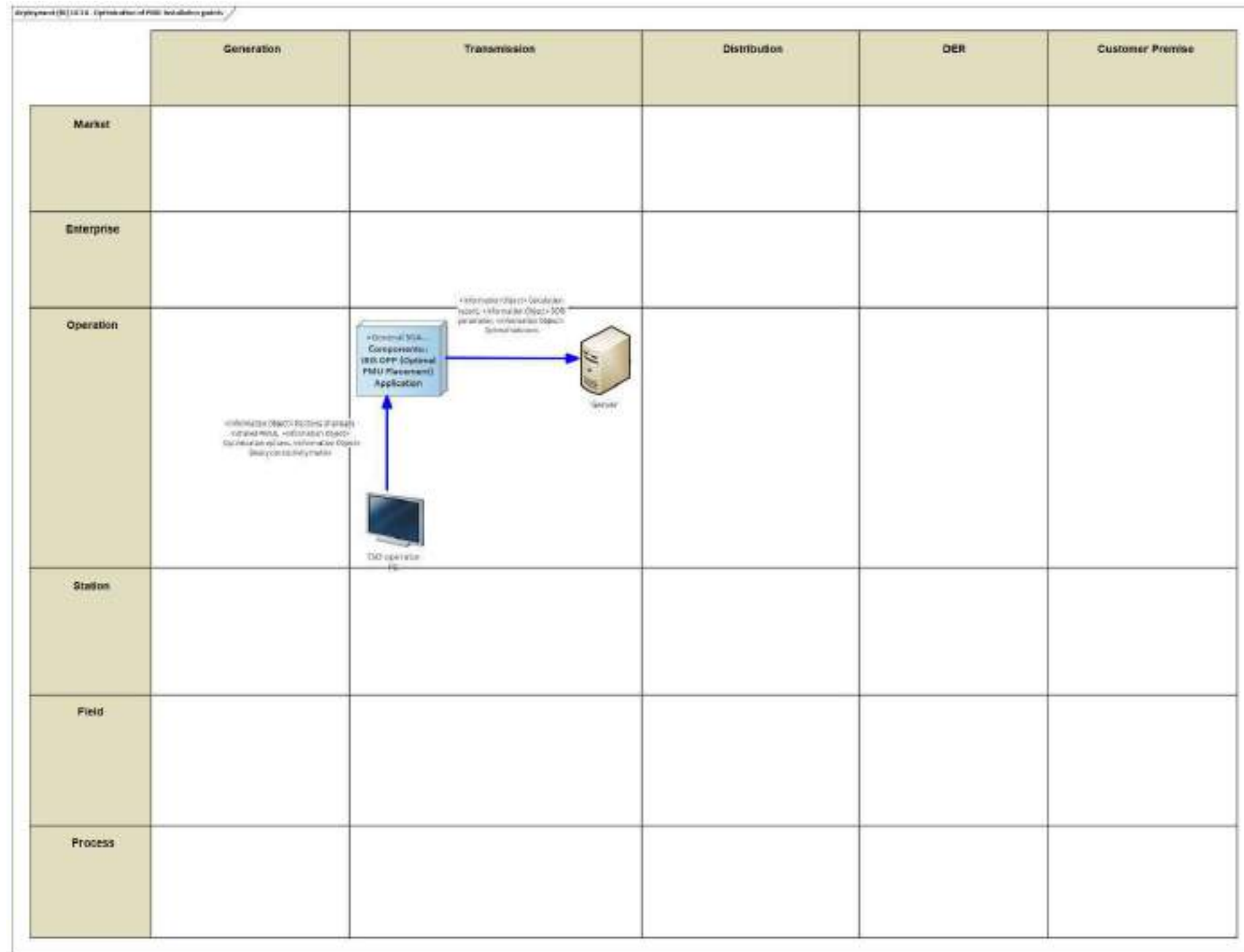


Figure 190 - UC18 Business Layer

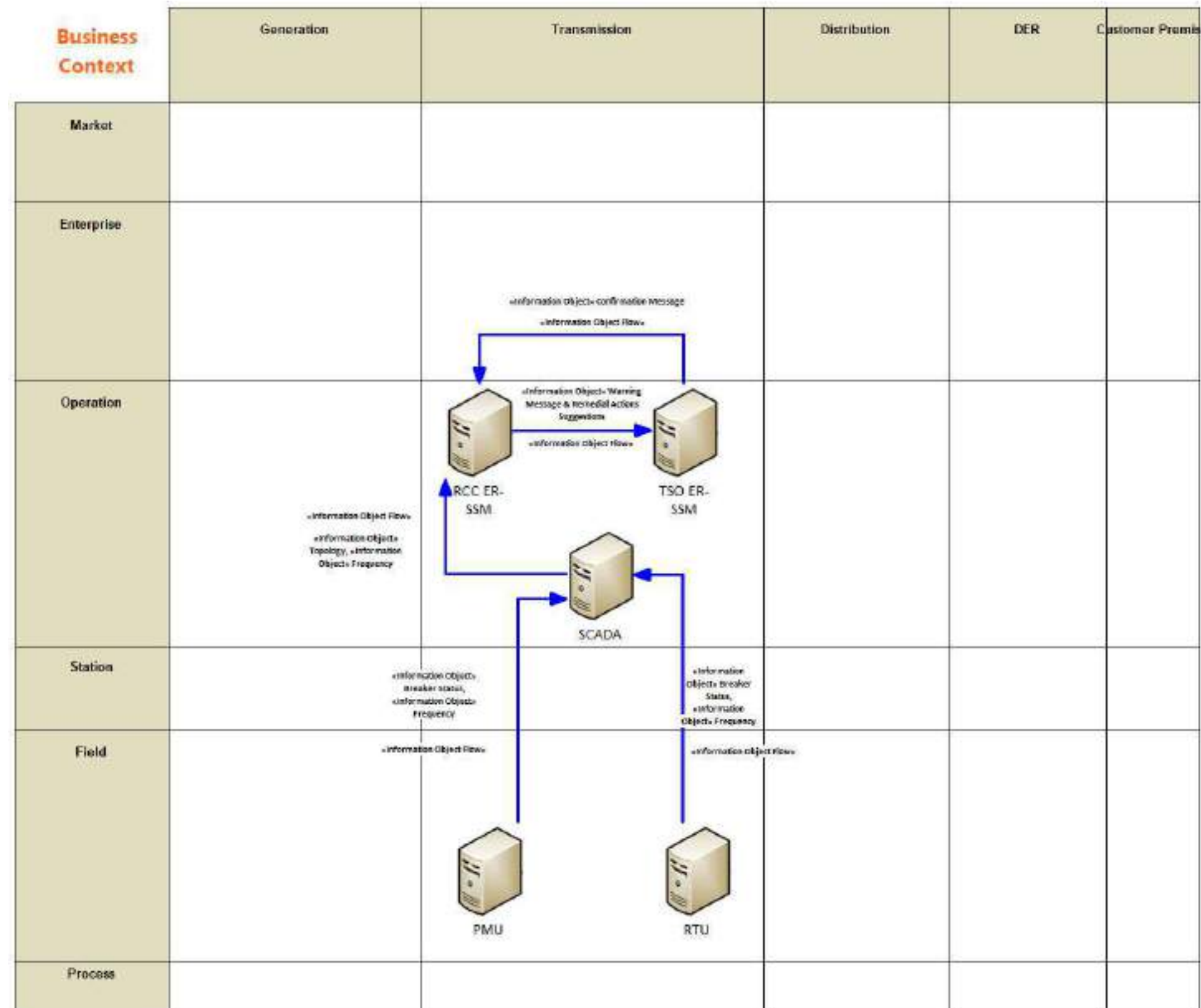


Figure 191 - UC19 Business Layer

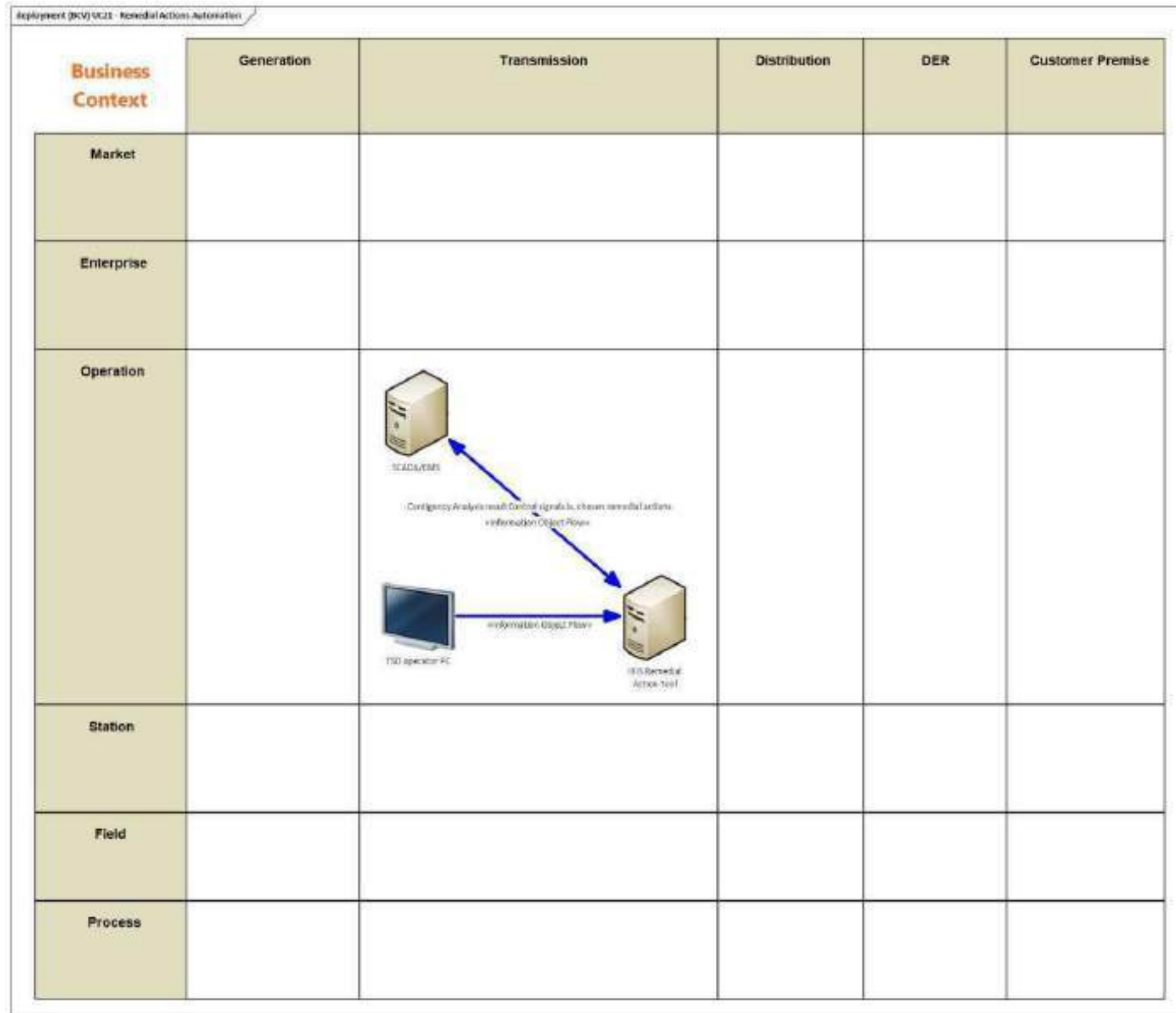


Figure 192 - UC21 Business Layer

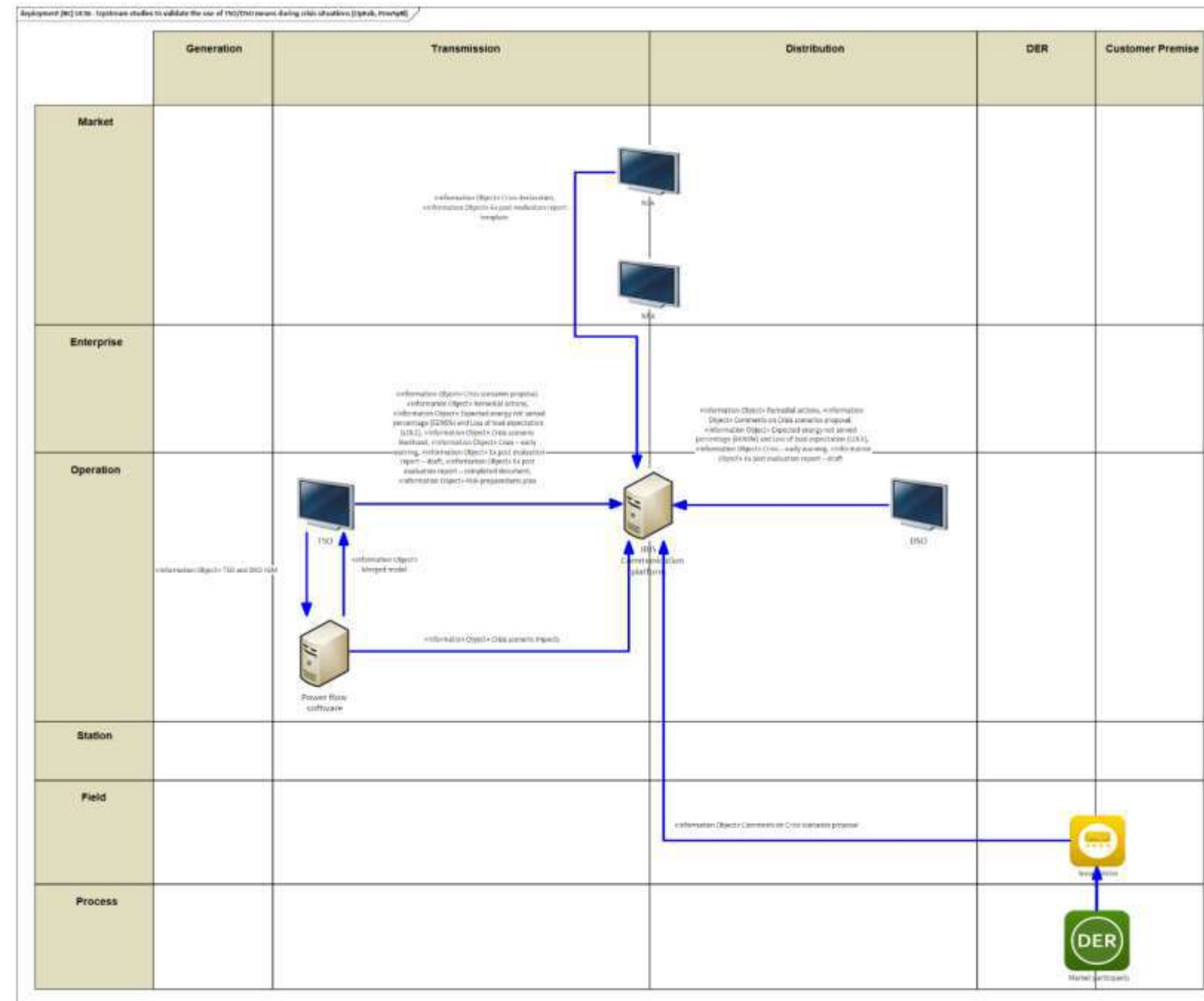


Figure 193 - UC35 Business Layer



13.2.1.3 WP5-PRECOG

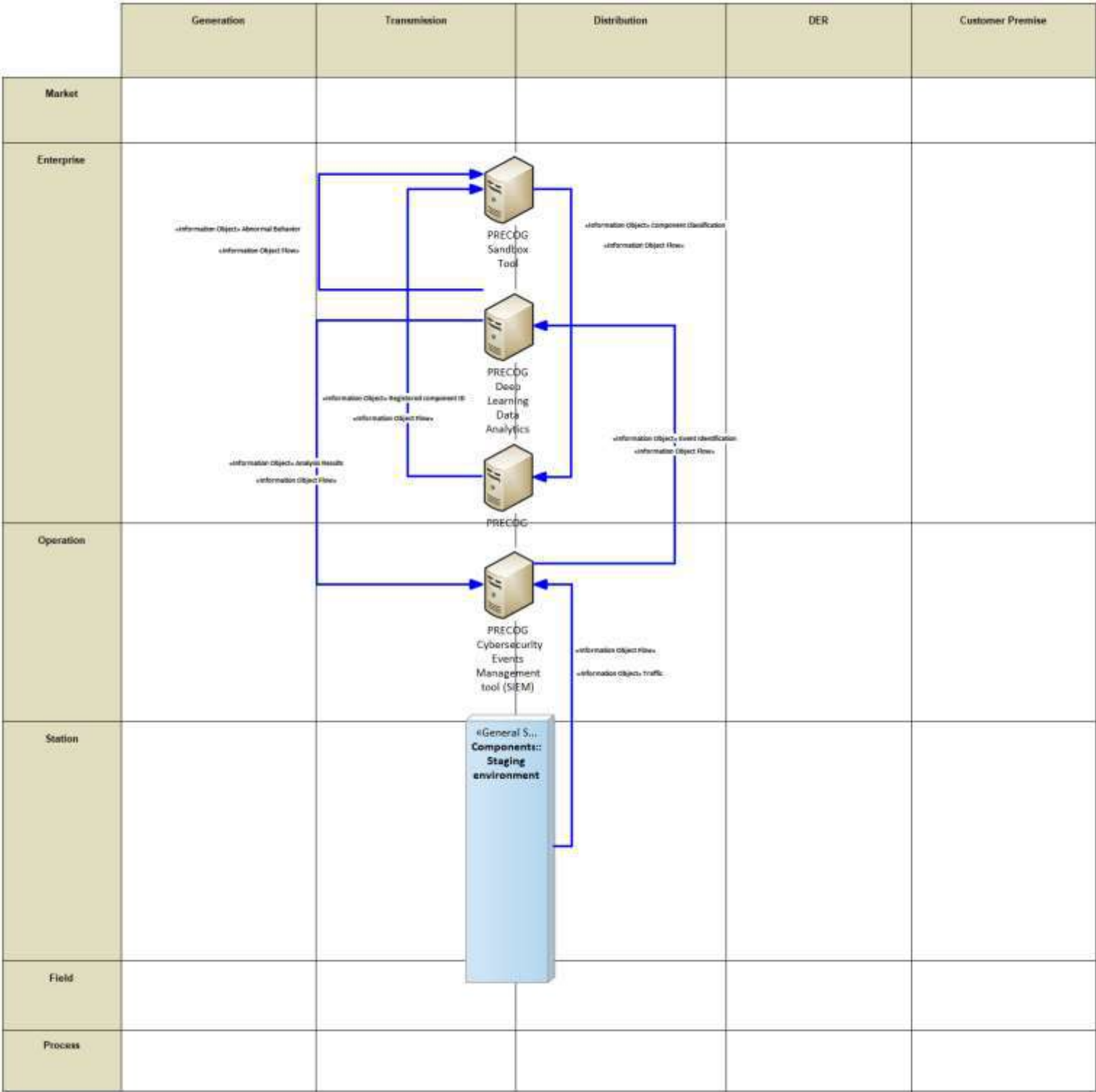


Figure 194 - UC27 Business Layer

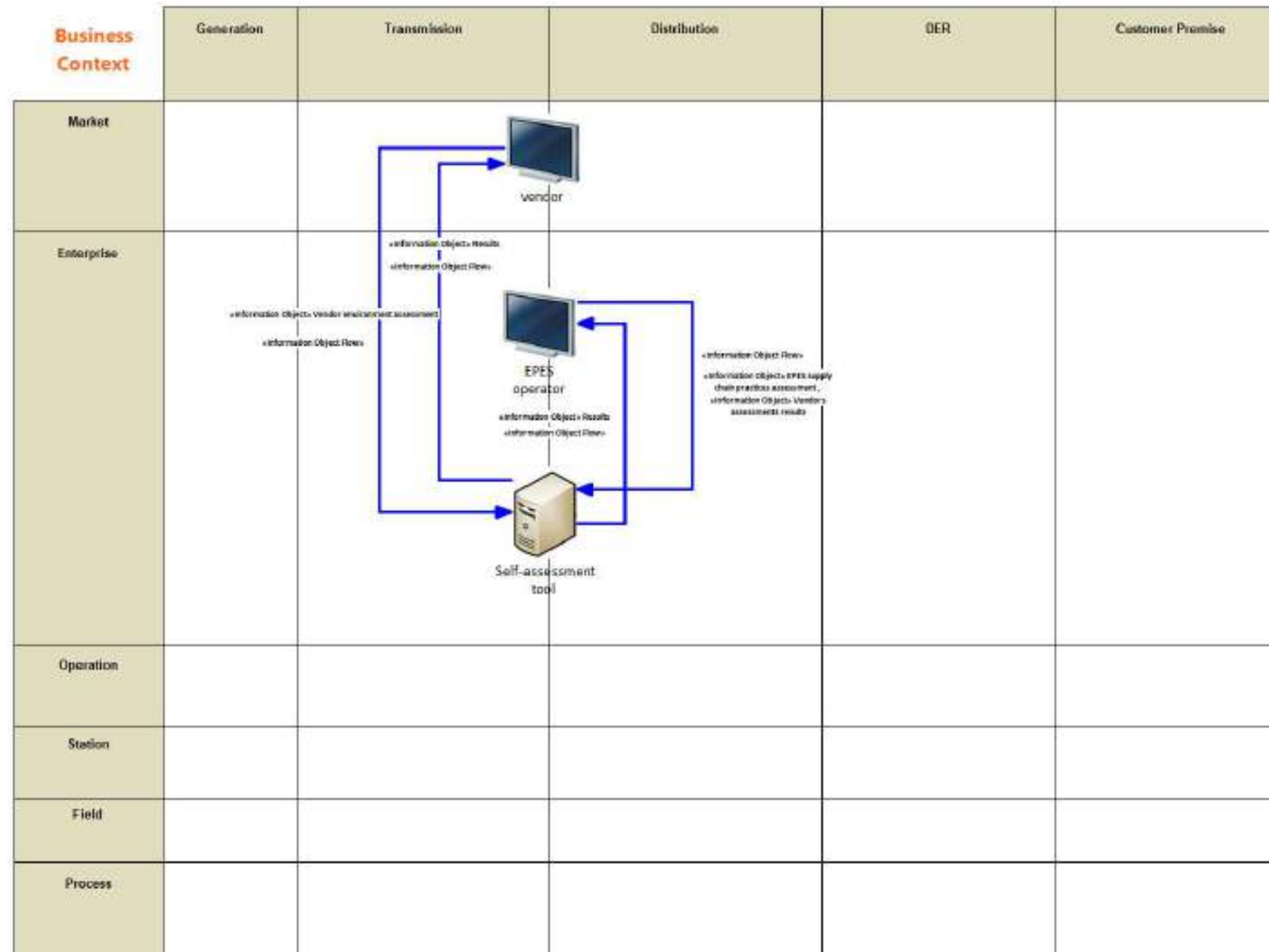


Figure 195 - UC28 Business Layer

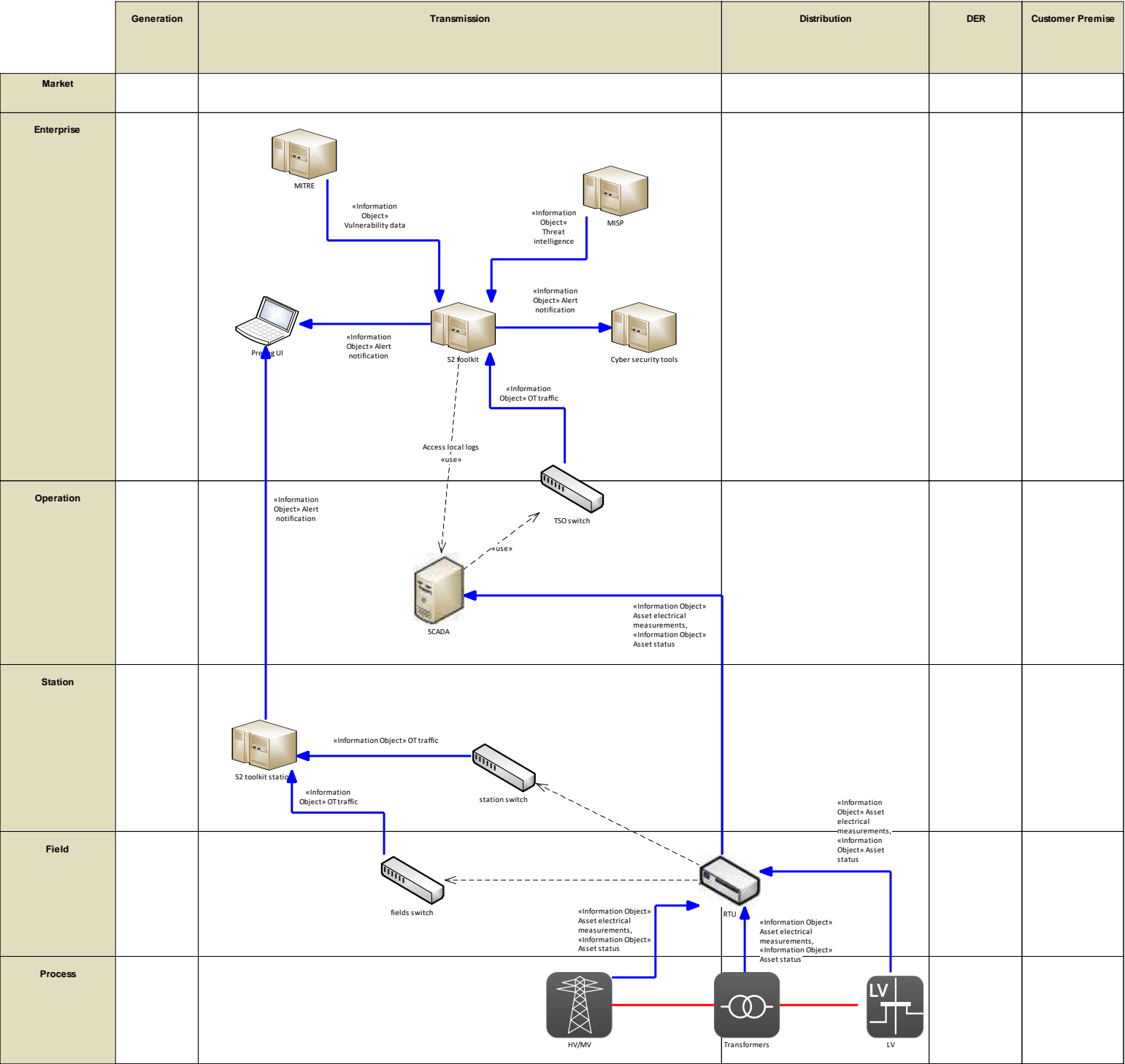


Figure 196 - UC33 Business Layer

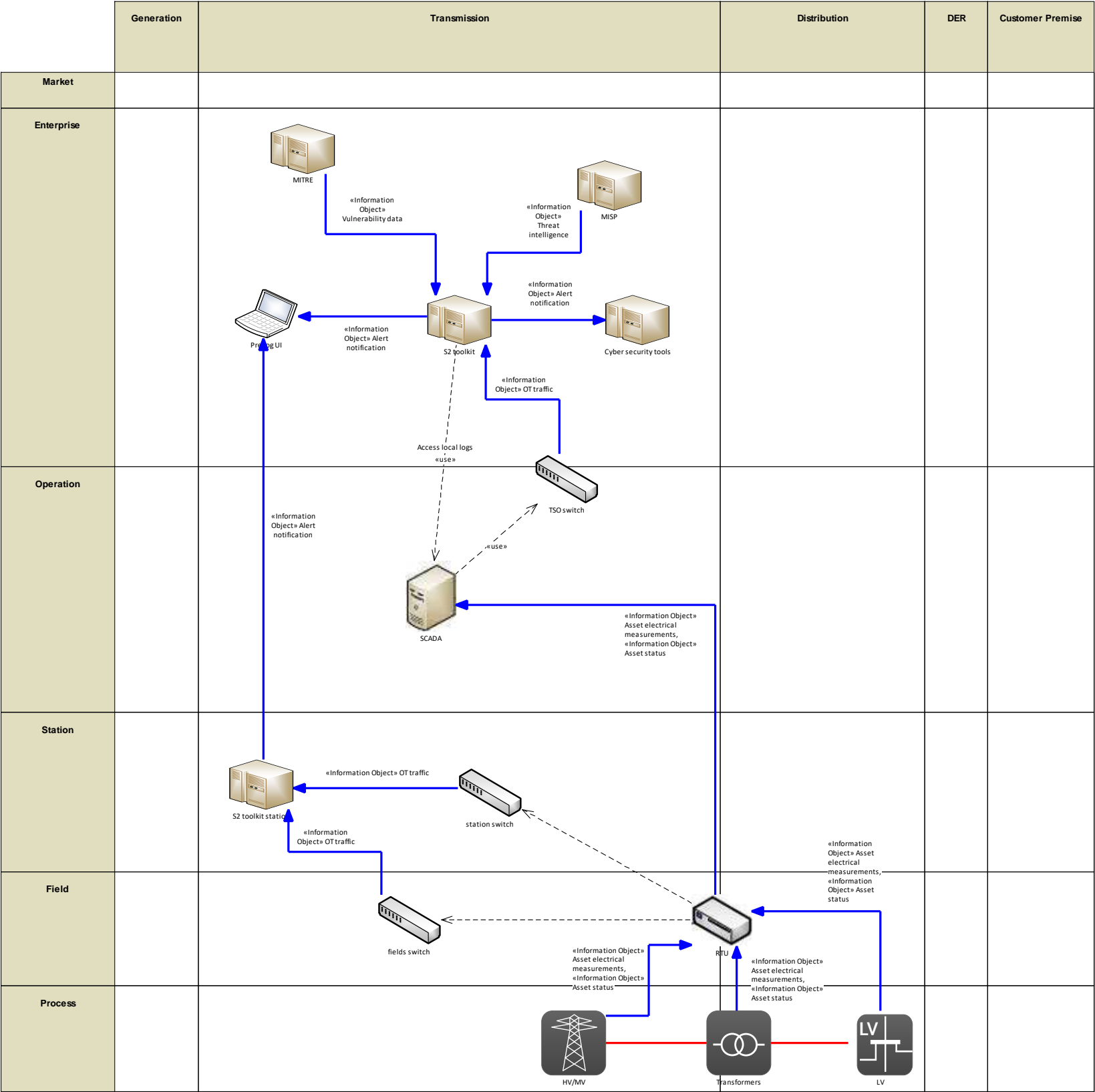


Figure 197 - UC34 Business Layer

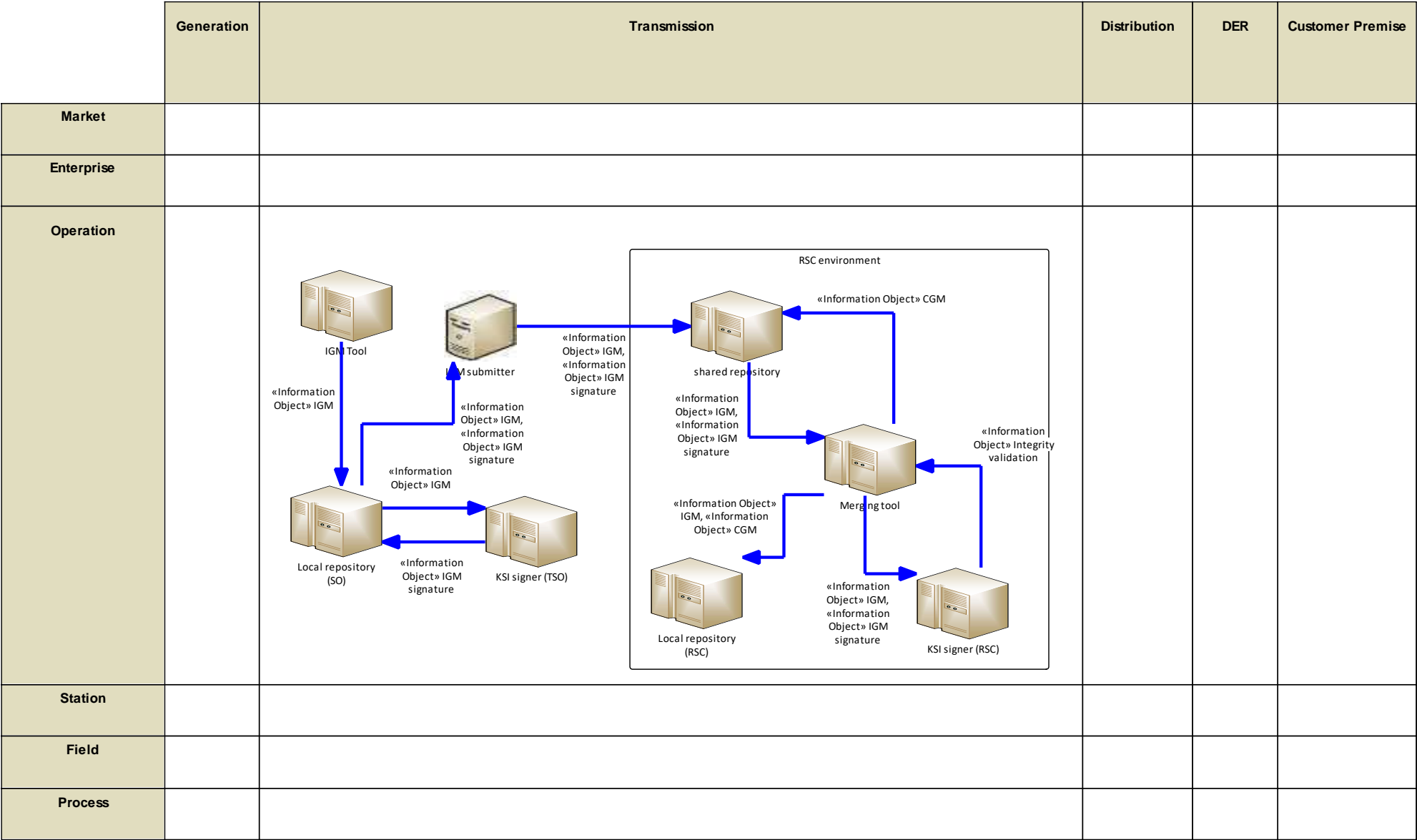


Figure 198 - UC36 Business Layer

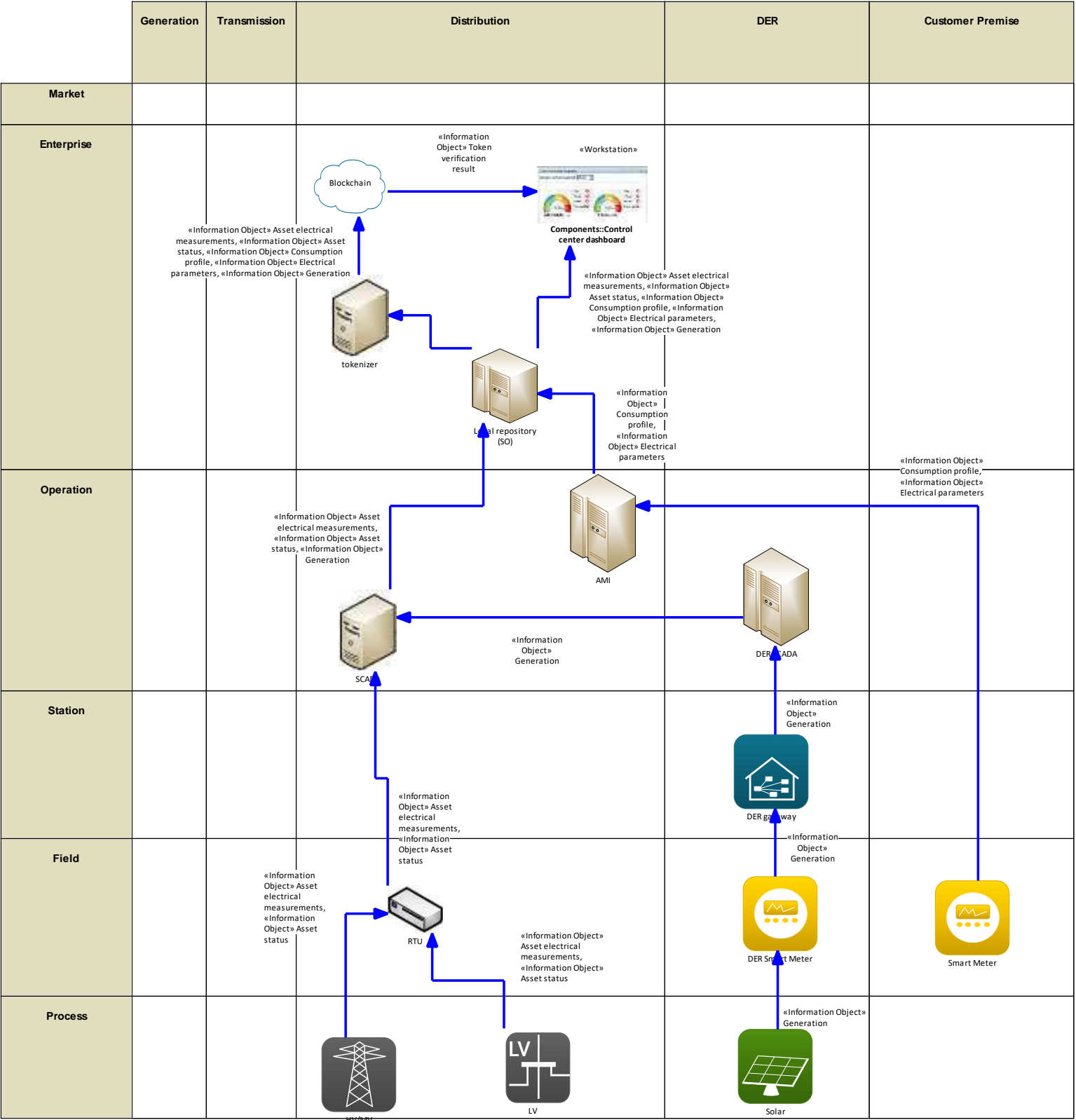


Figure 199 - UC37 Business Layer

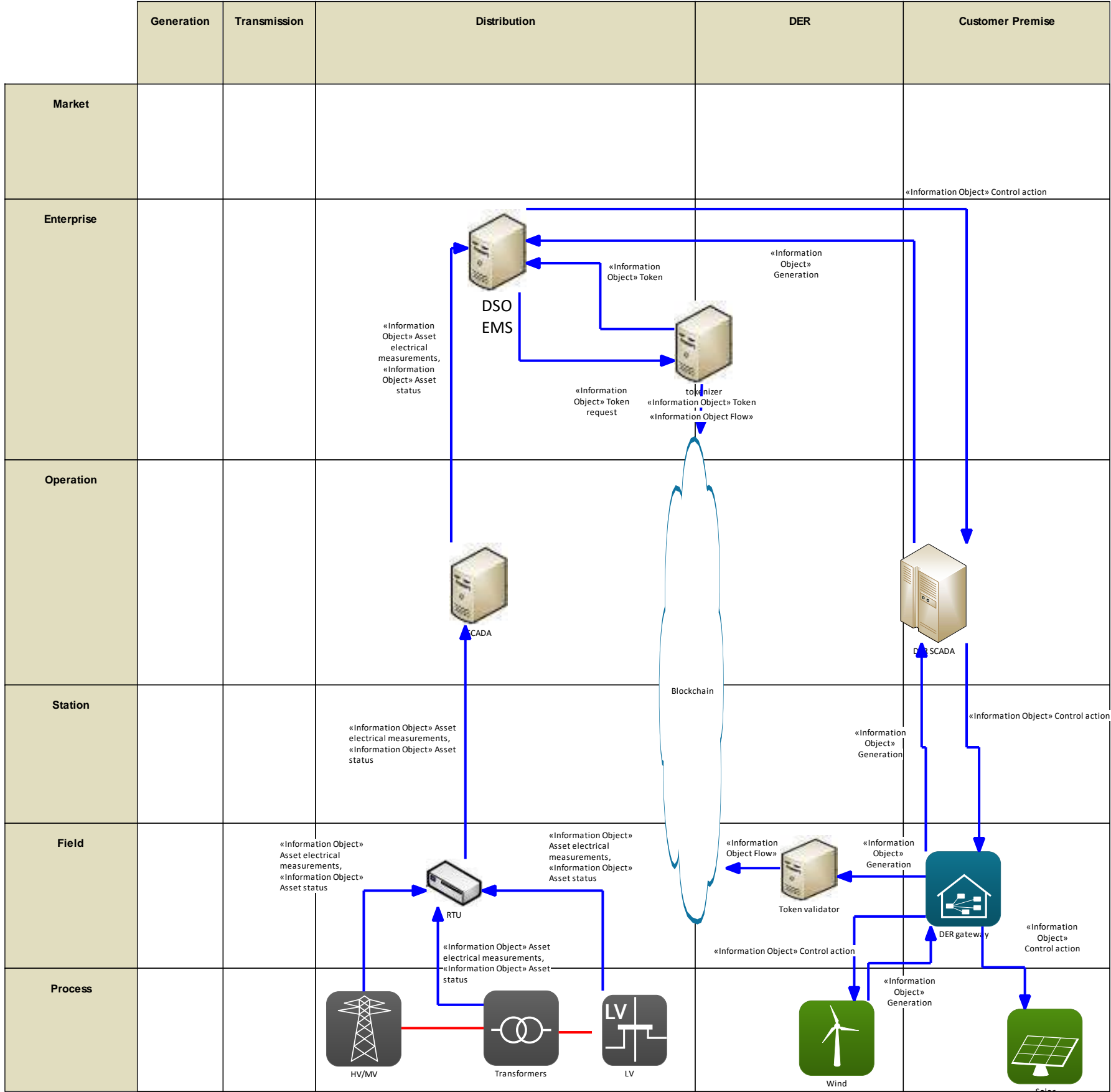


Figure 200 - UC38 Business Layer

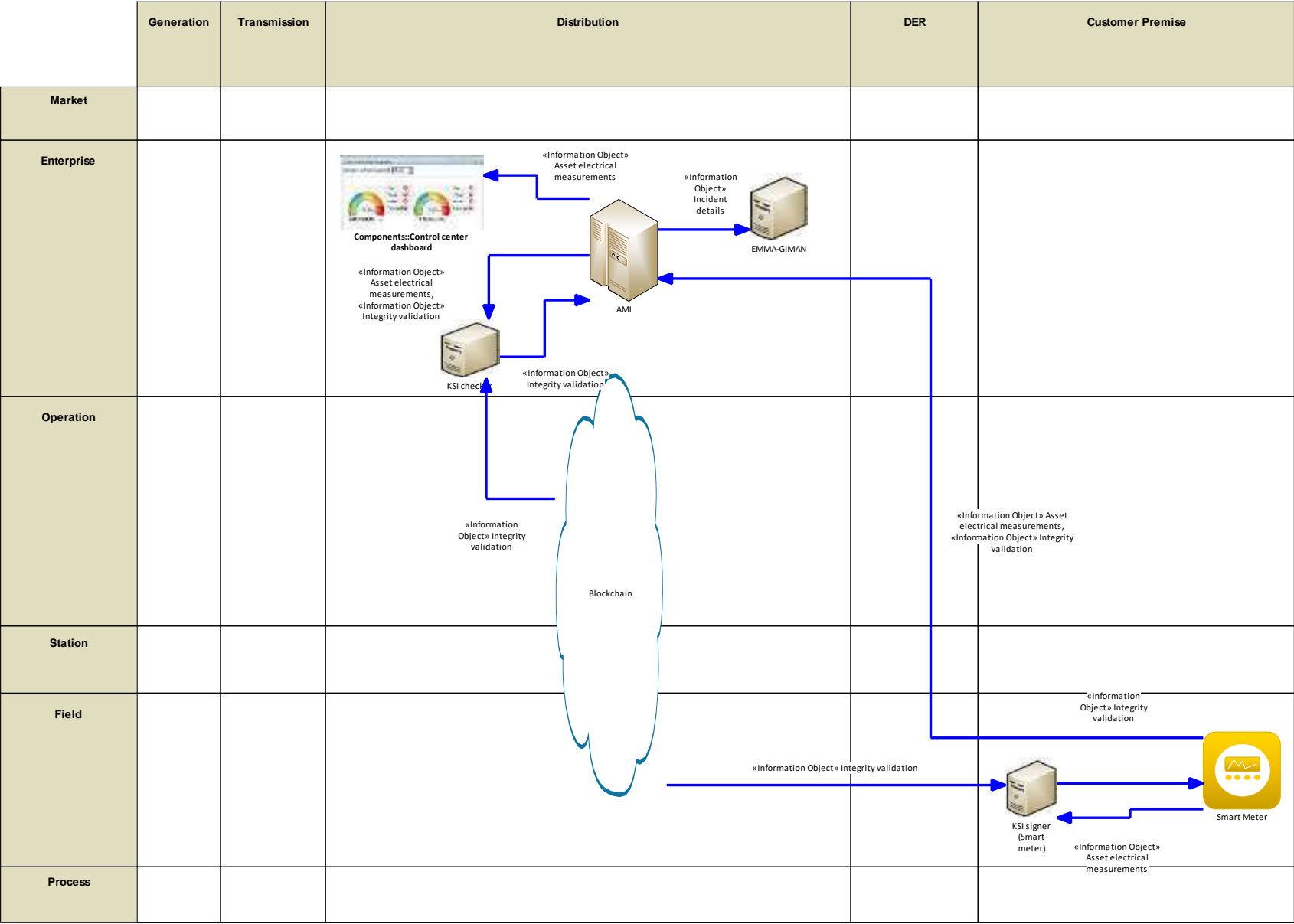


Figure 201 - UC40 Business Layer

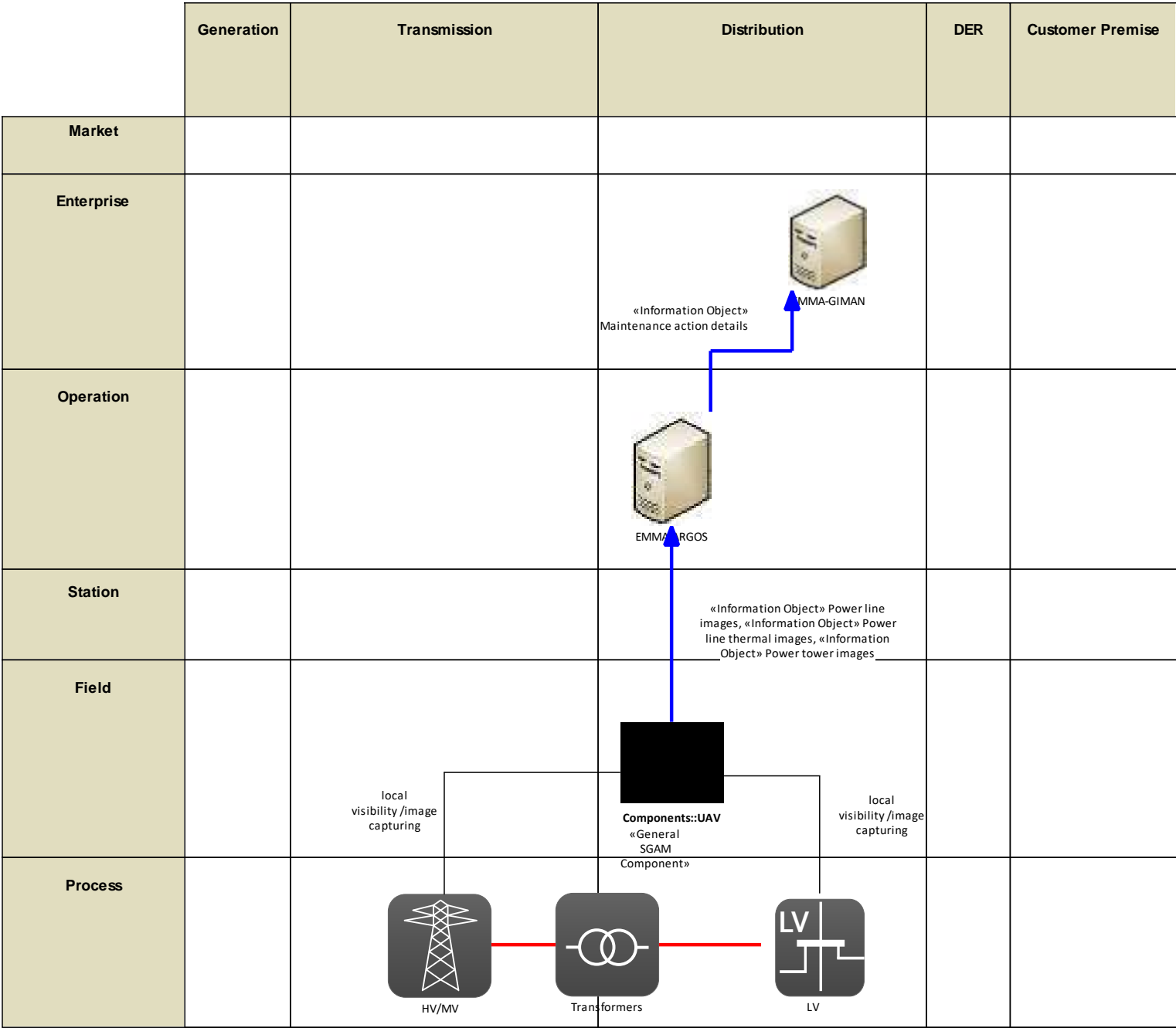


Figure 202 - UC01 Business Layer

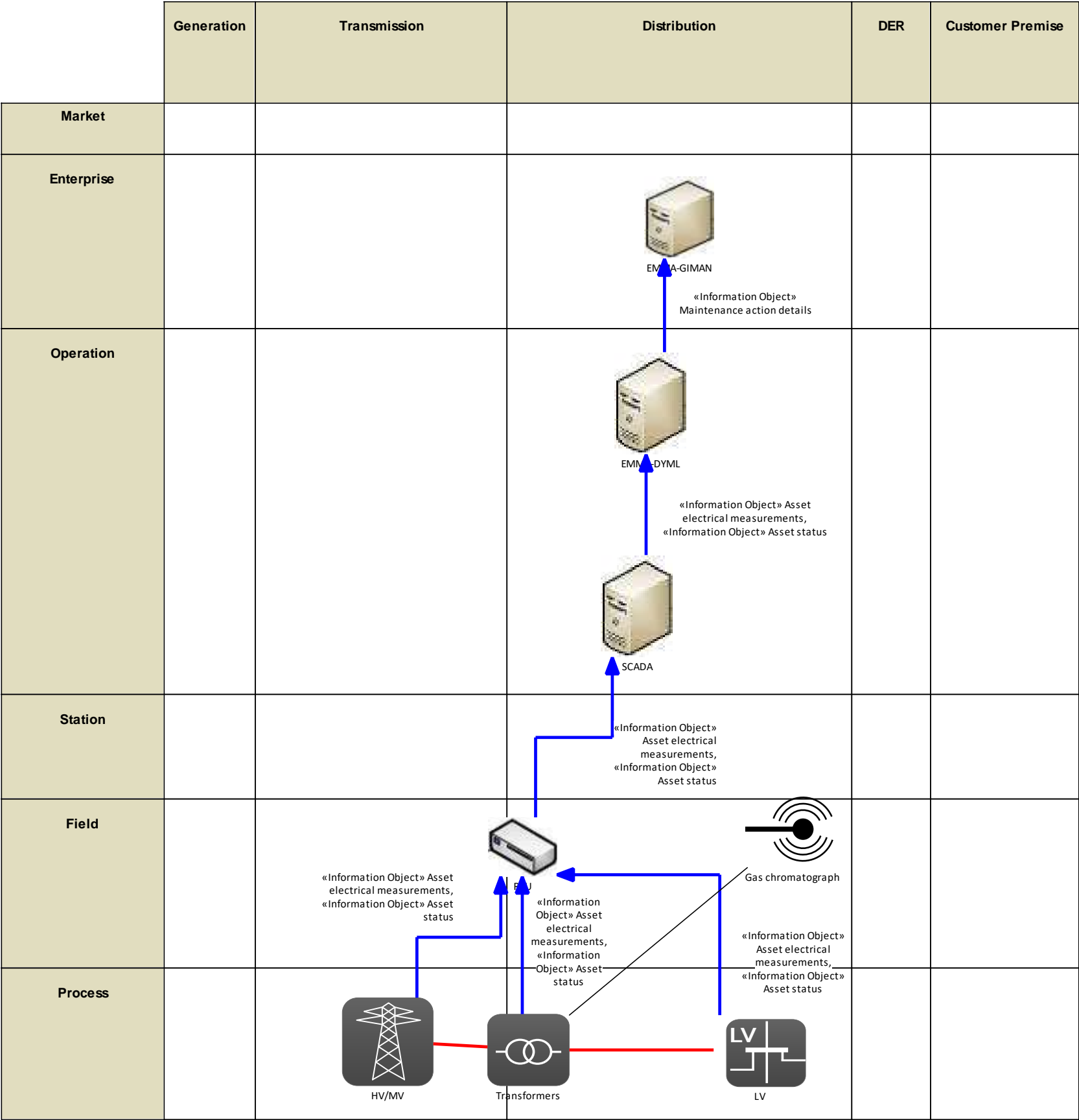


Figure 203 - UC02 Business Layer

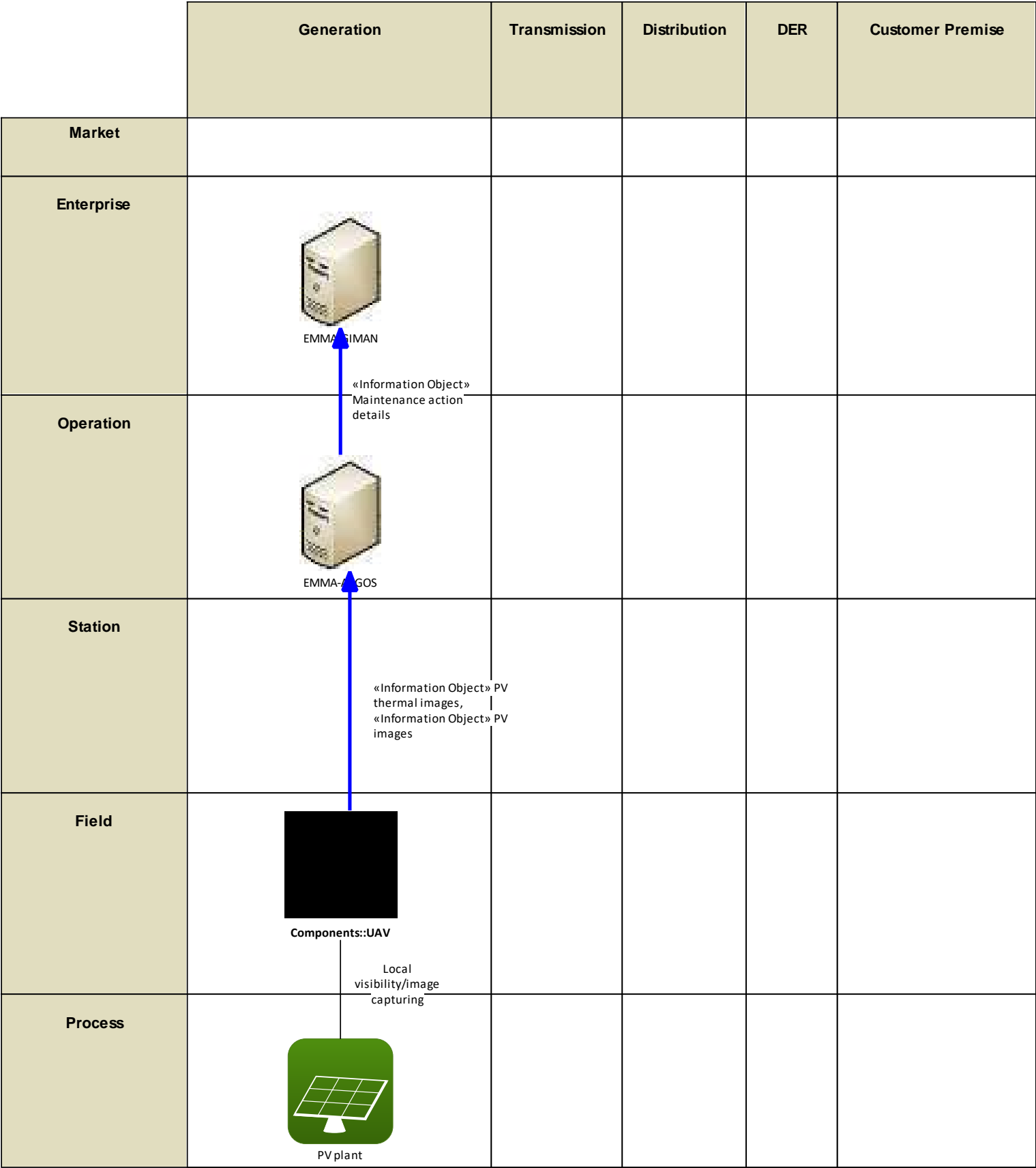


Figure 204 - UC03 Business Layer

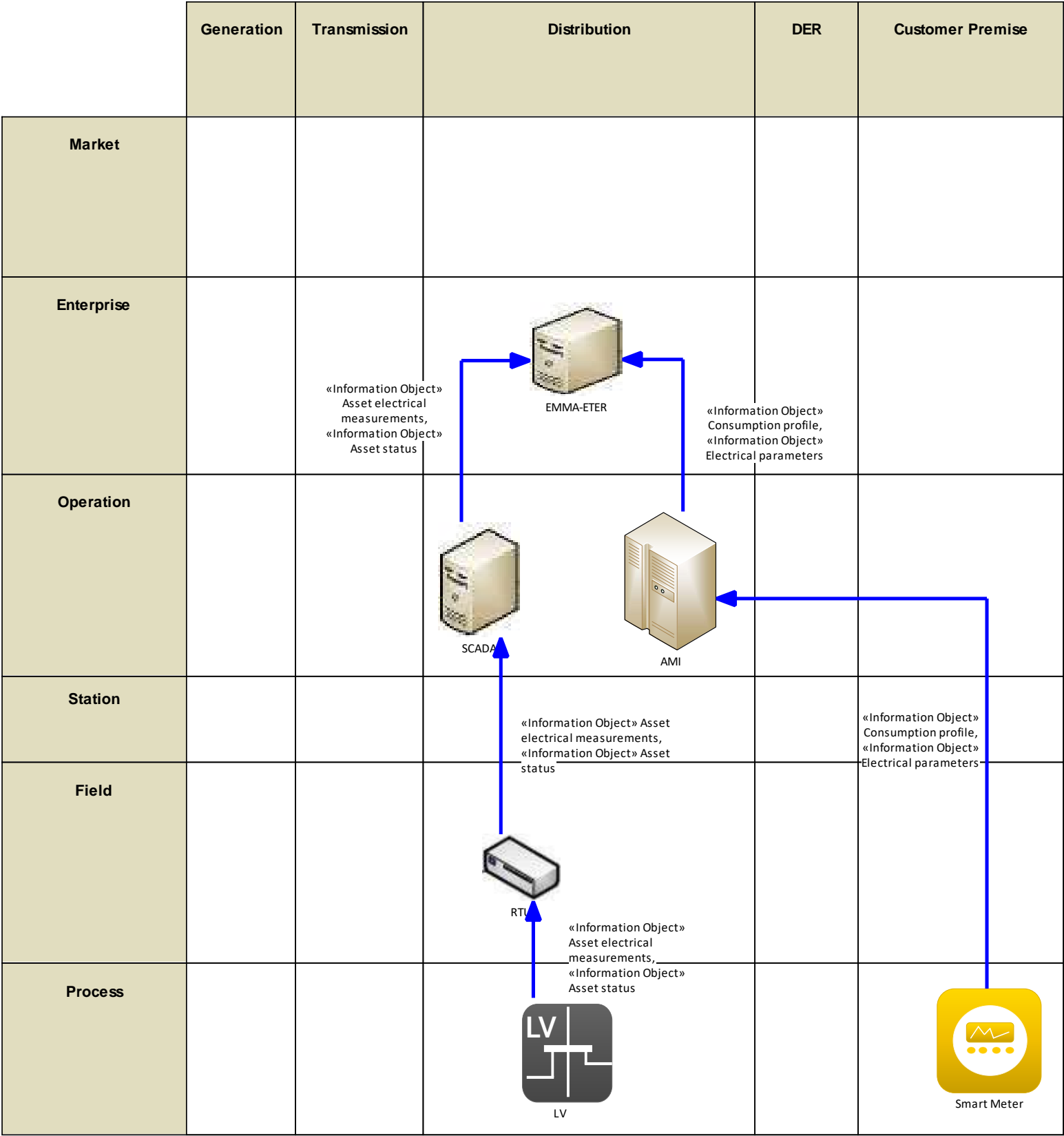


Figure 205 - UC04 Business Layer

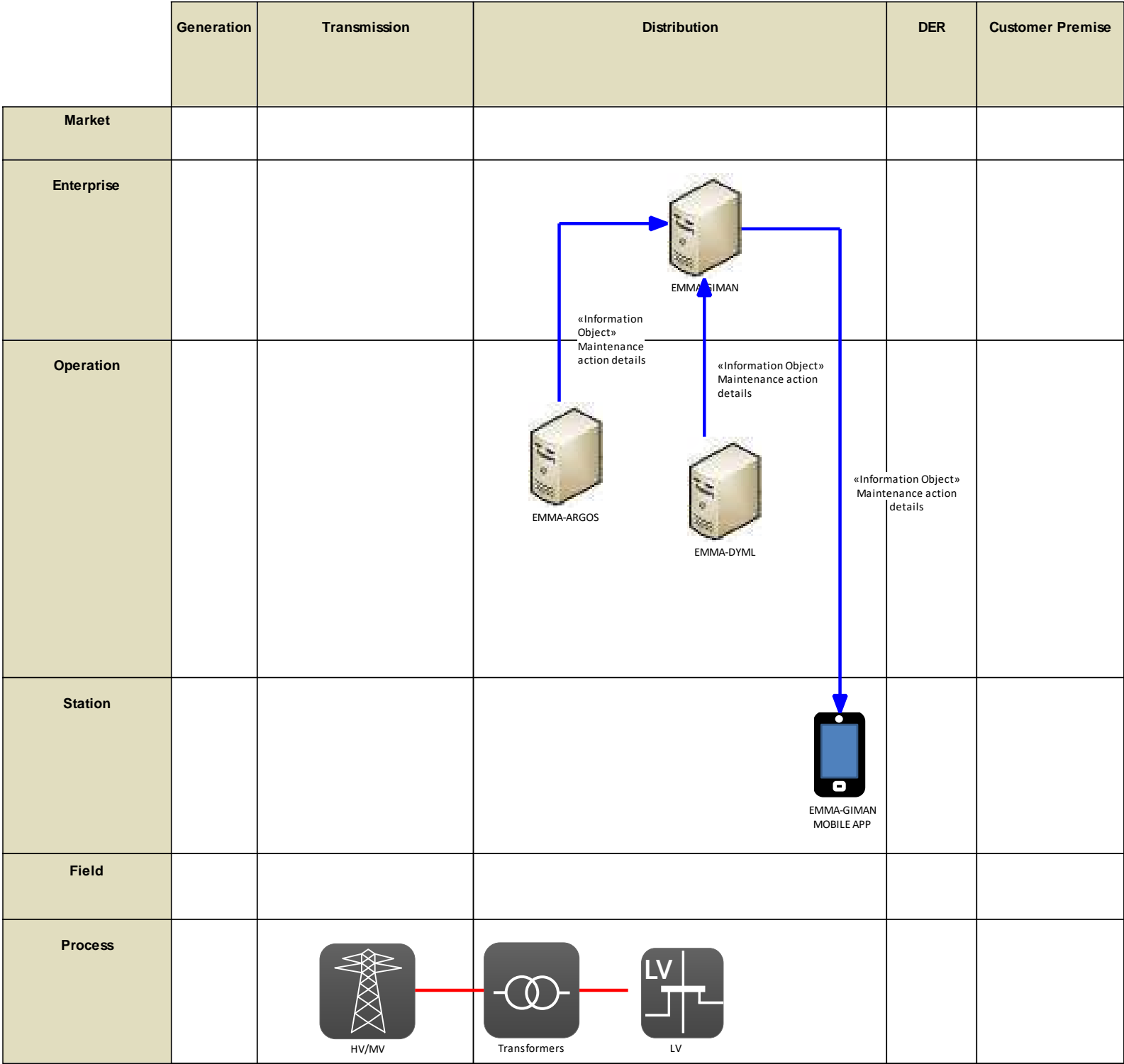


Figure 206 - UC05 Business Layer

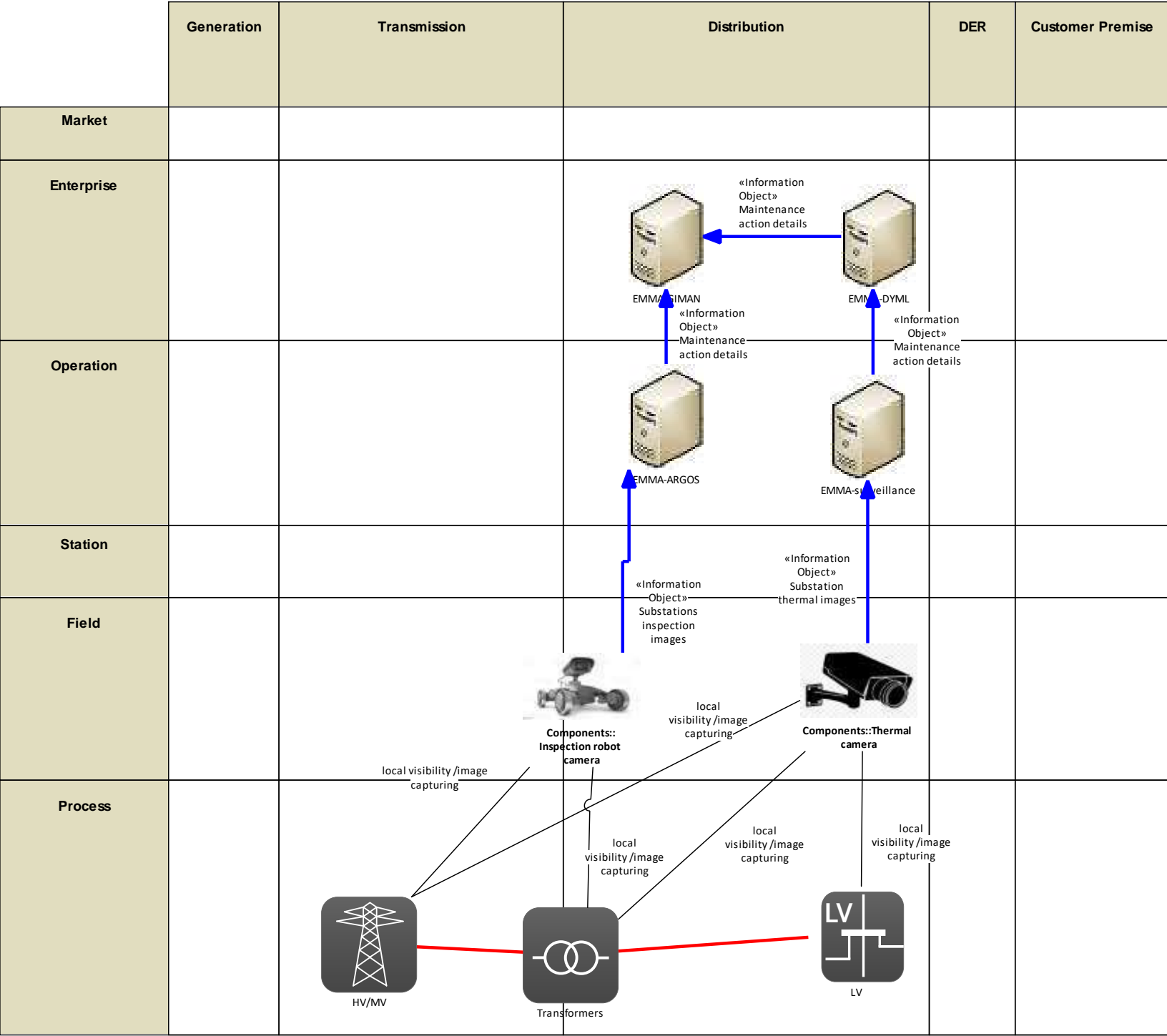


Figure 207 - UC06 Business Layer

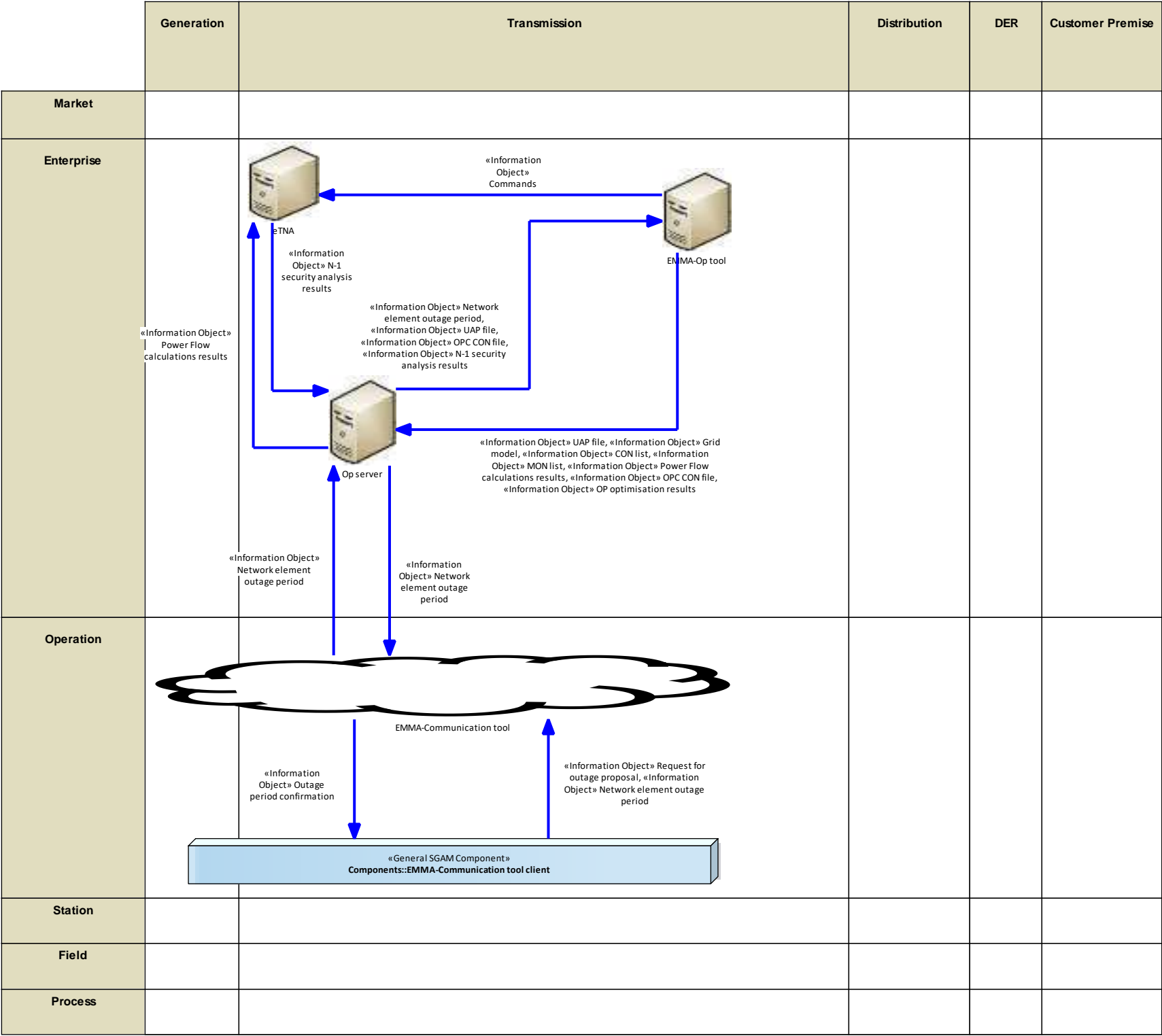


Figure 208 - UC08 Business Layer



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise		<div><p>«Information Object» Calculated emission levels, «Information Object» Comparison of measured and calculated values, «Information Object» Specific parameters related to power quality</p><pre>graph TD; PQS[Power quality server] --> EMA[EMA-PQEL]; GMS[Grid model server] --> EMA; EMA --> PQS</pre><p>Power quality server</p><p>Grid model server</p></div>			
Operation					
Station					
Field					
Process					

Figure 209 - UC09 Business Layer

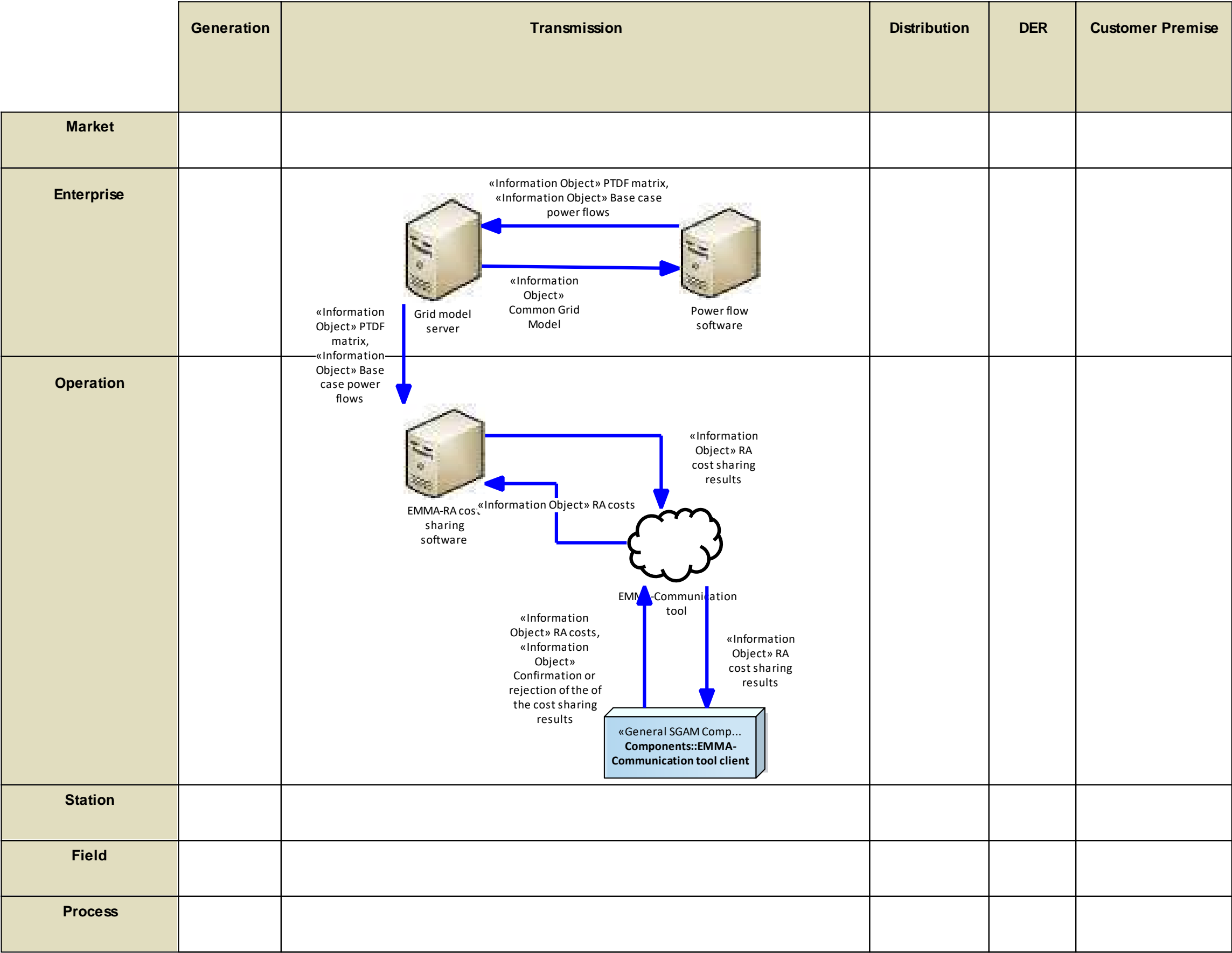


Figure 210 - UC13 Business Layer



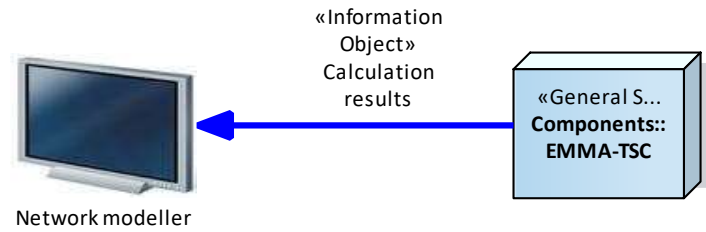
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation		<div><p>«Information Object» Calculation results</p><p>Network modeller</p><p>«General S... Components:: EMMA-TSC»</p></div>			
Station					
Field					
Process					

Figure 211 - UC14 Business Layer

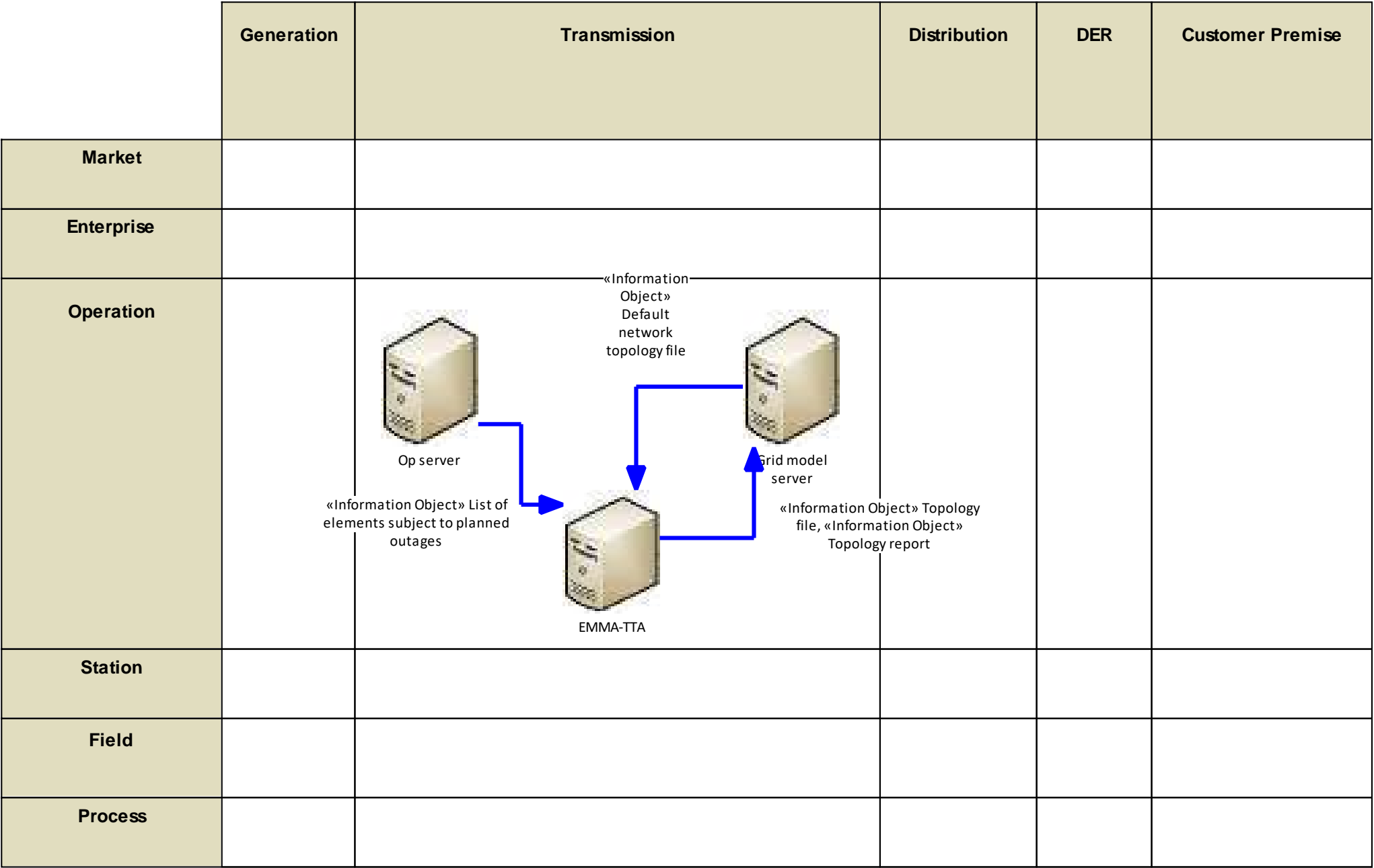


Figure 212 - UC17 Business Layer

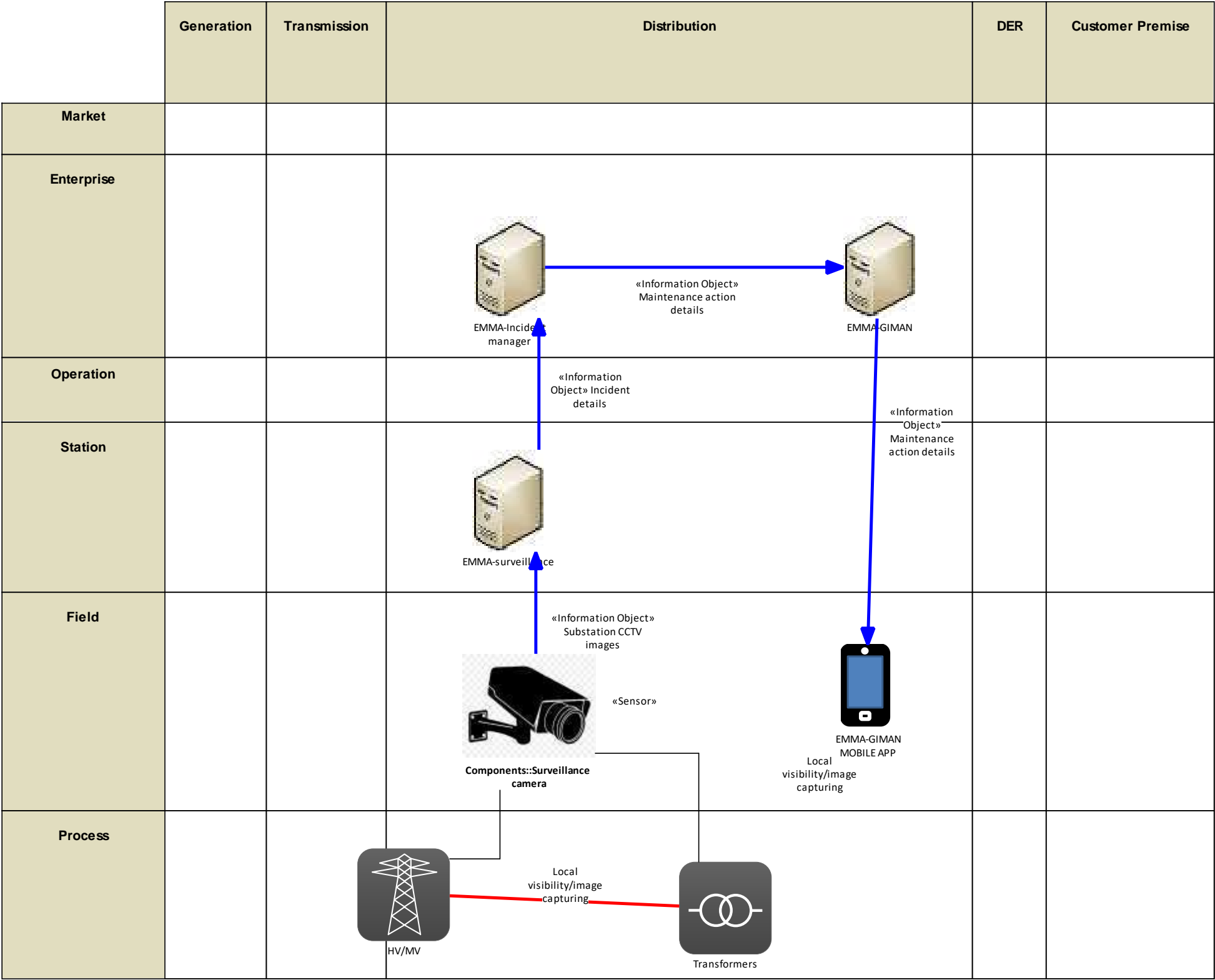


Figure 213 - UC20 Business Layer

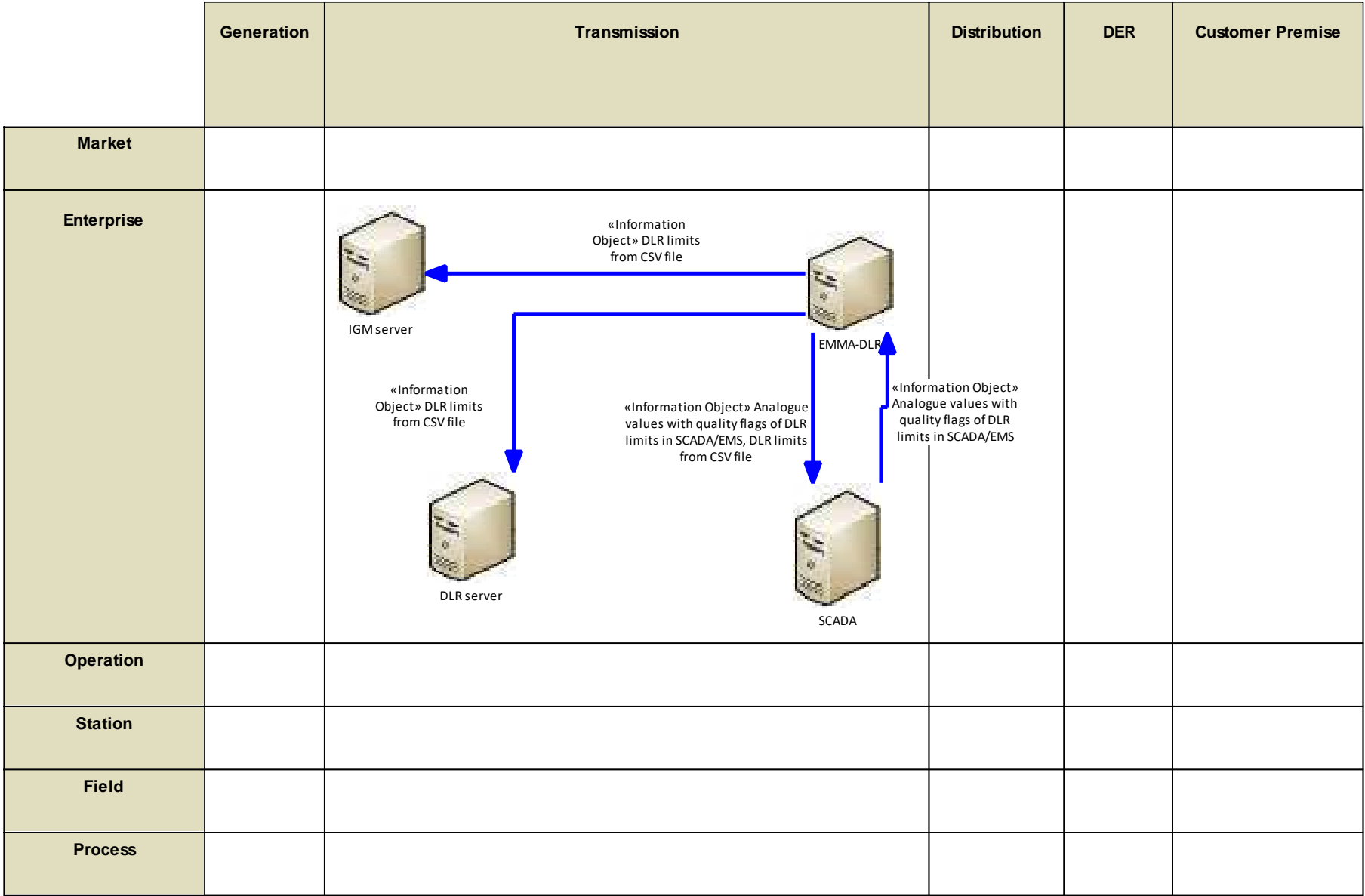


Figure 214 - UC31 Business Layer



13.2.2 Canonical Data Model

13.2.2.1 WP3-C3PO

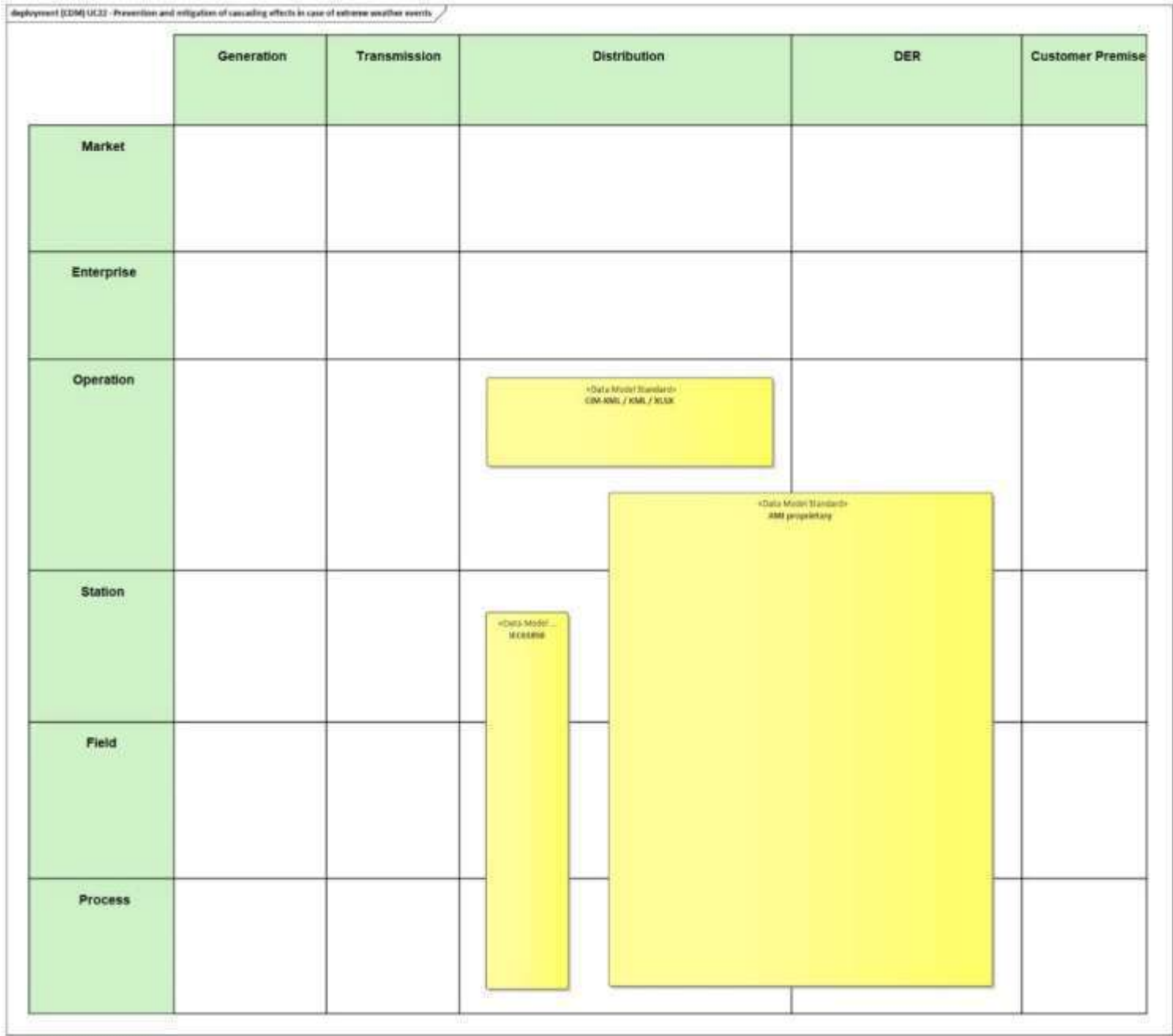


Figure 215 - UC22 Canonical Data Model

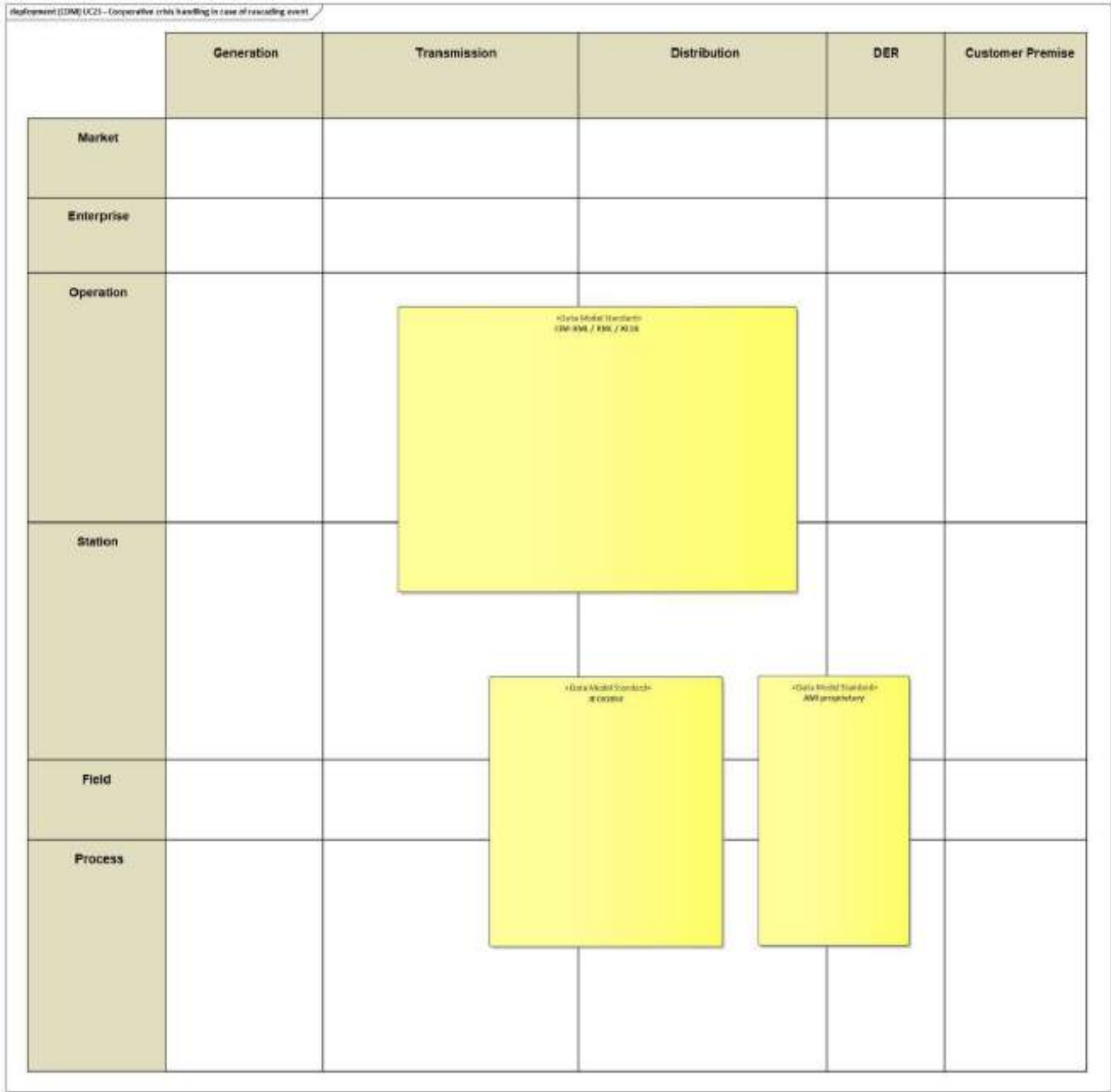


Figure 216 - UC23 Canonical Data Model



deployment [CDM] UC24 - Cyber Security Risk Assessment on EPES infrastructure					
Canonical Data Model	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 217 - UC24 Canonical Data Model

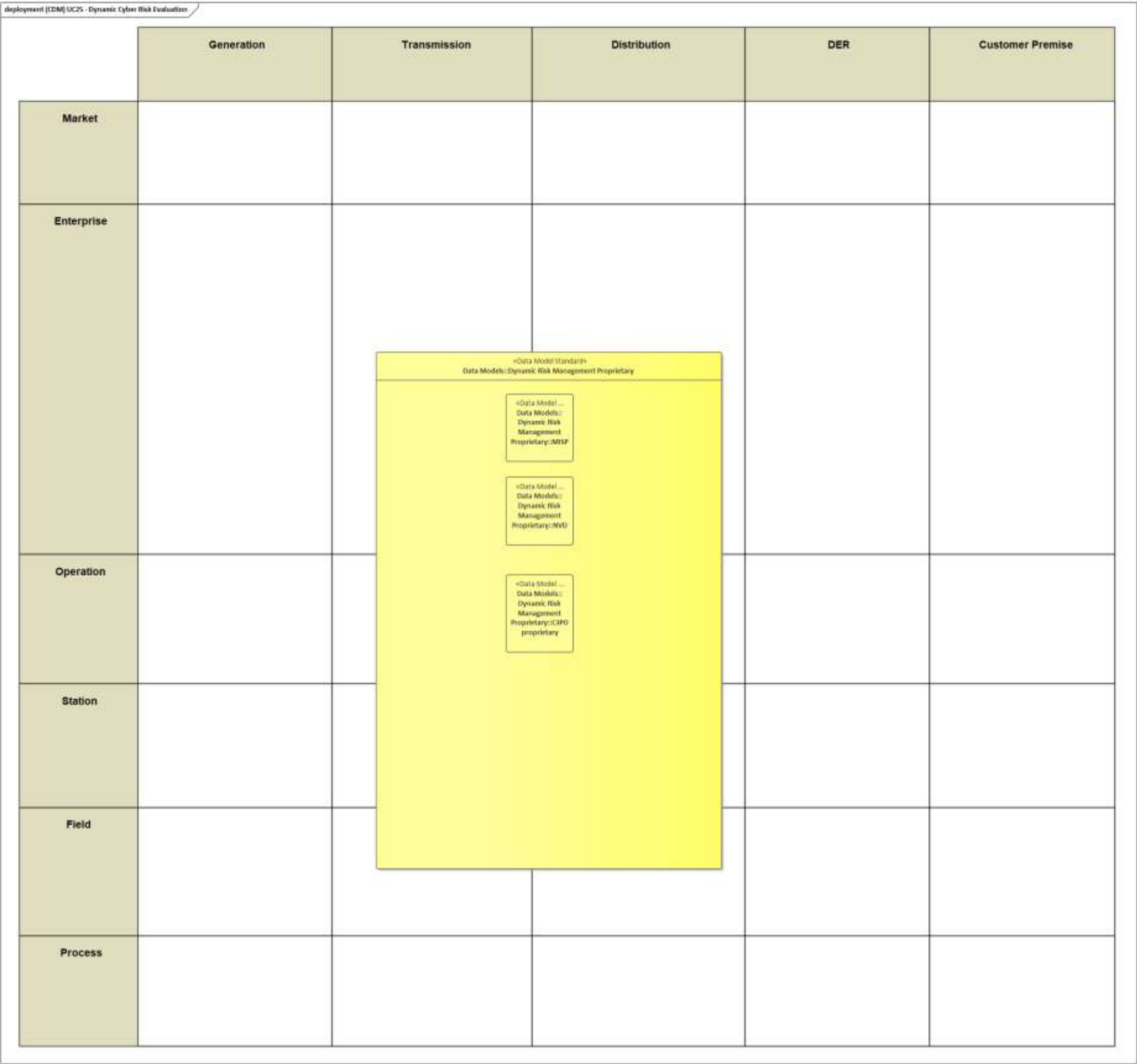


Figure 218 - UC25 Canonical Data Model

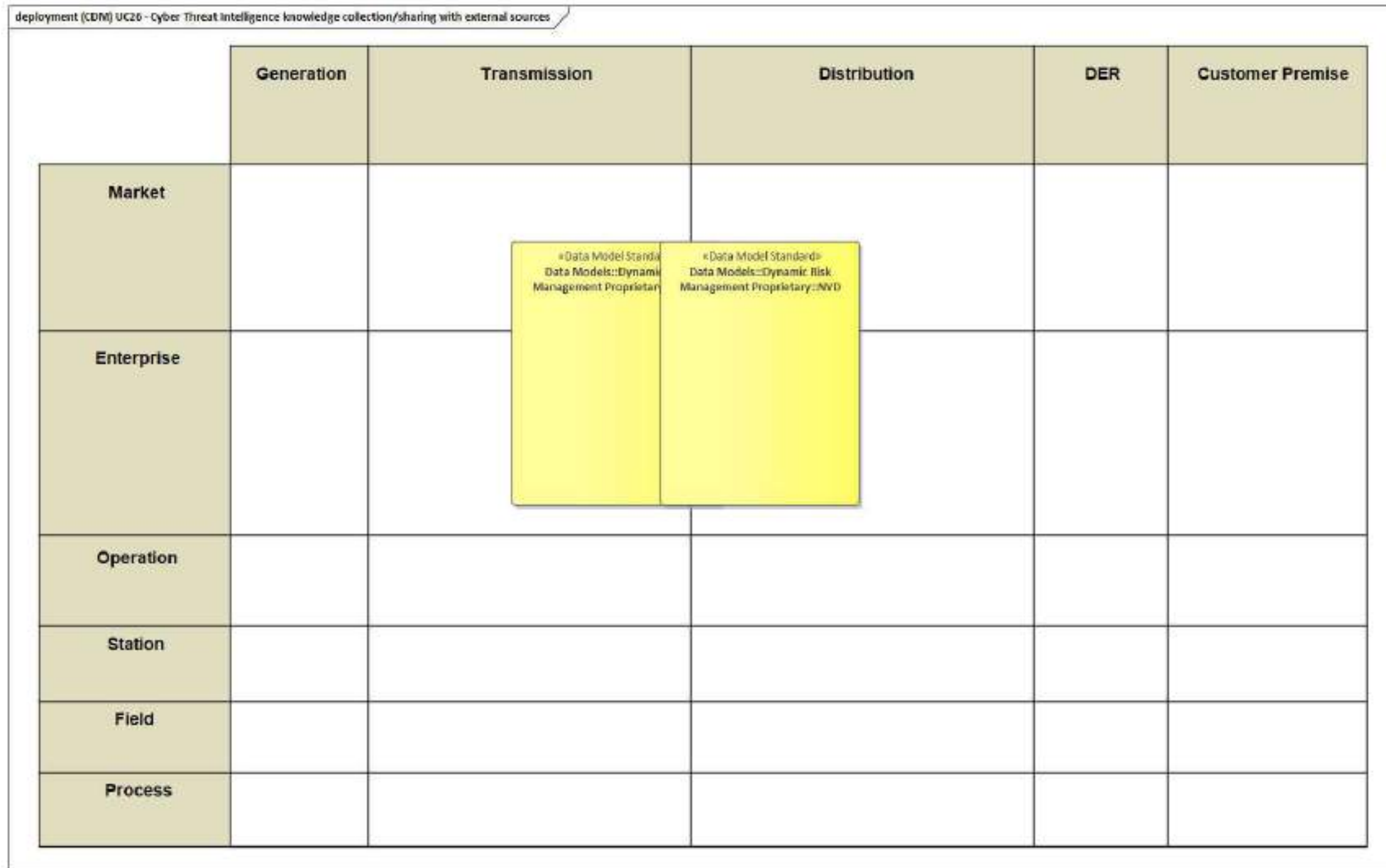


Figure 219 - UC26 Canonical Data Model

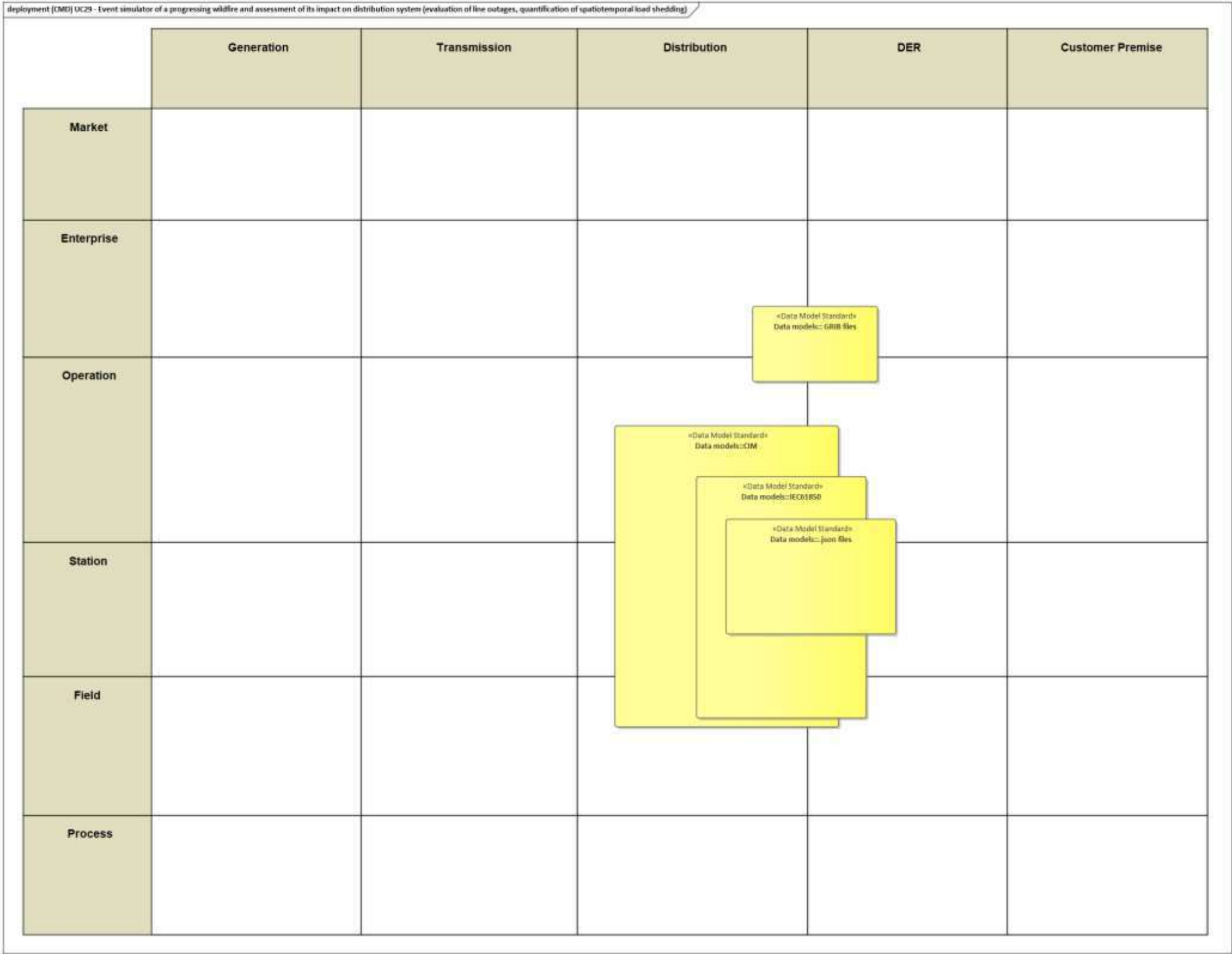


Figure 220 – UC29 Canonical Data Model

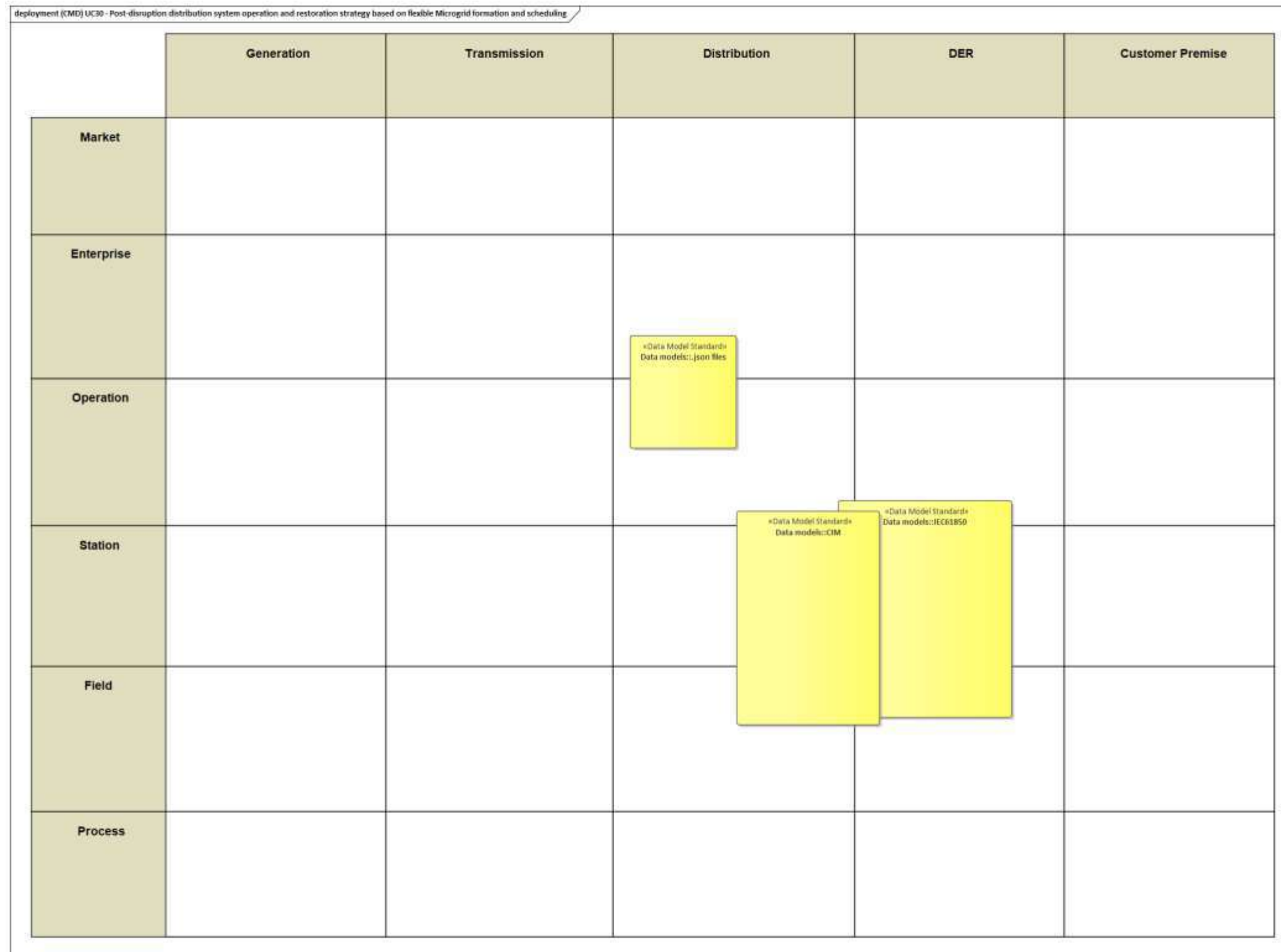


Figure 221 - UC30 Canonical Data Model



Canonical Data Model	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 222 - UC32 Canonical Data Model



Canonical Data Model	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise		«Data Model Standard» Canonical Data Model:: OPDE Risk Register Data Model			
Operation					
Station					
Field					
Process					

Figure 223 - UC39 Canonical Data Model



13.2.2.2 WP4-IRIS

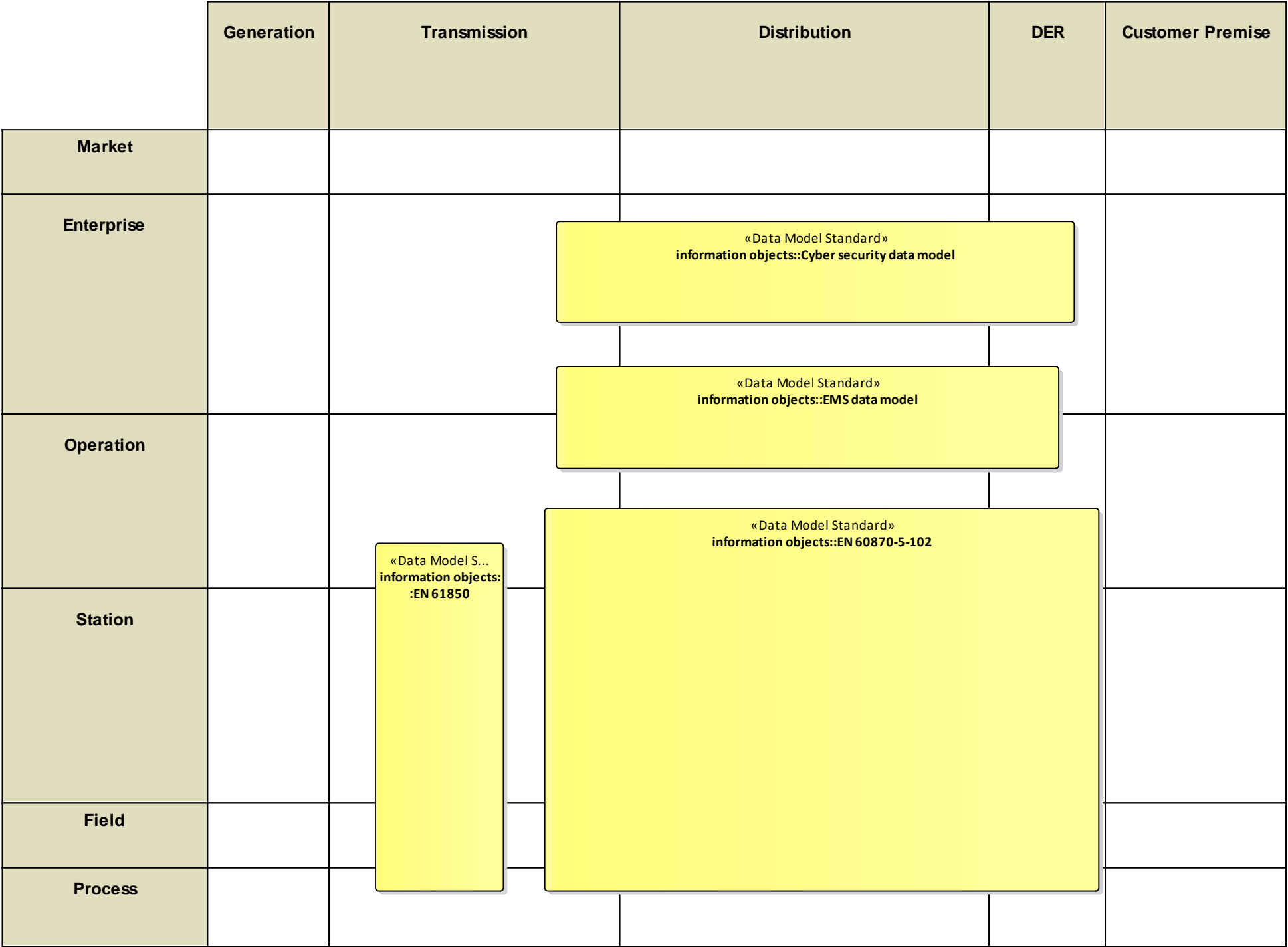


Figure 224 - UC07 Canonical Data Model

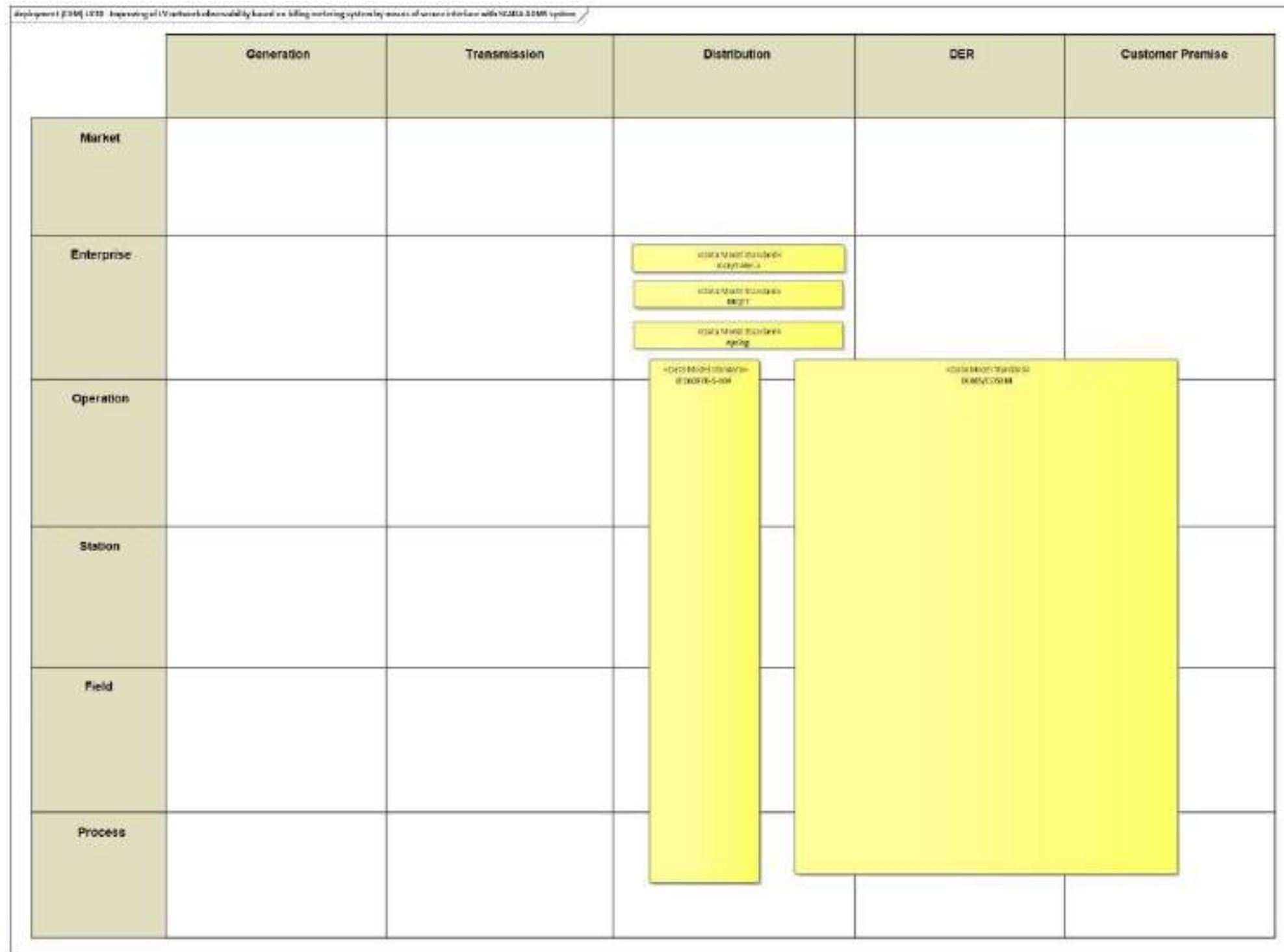


Figure 225 - UC10 Canonical Data Model

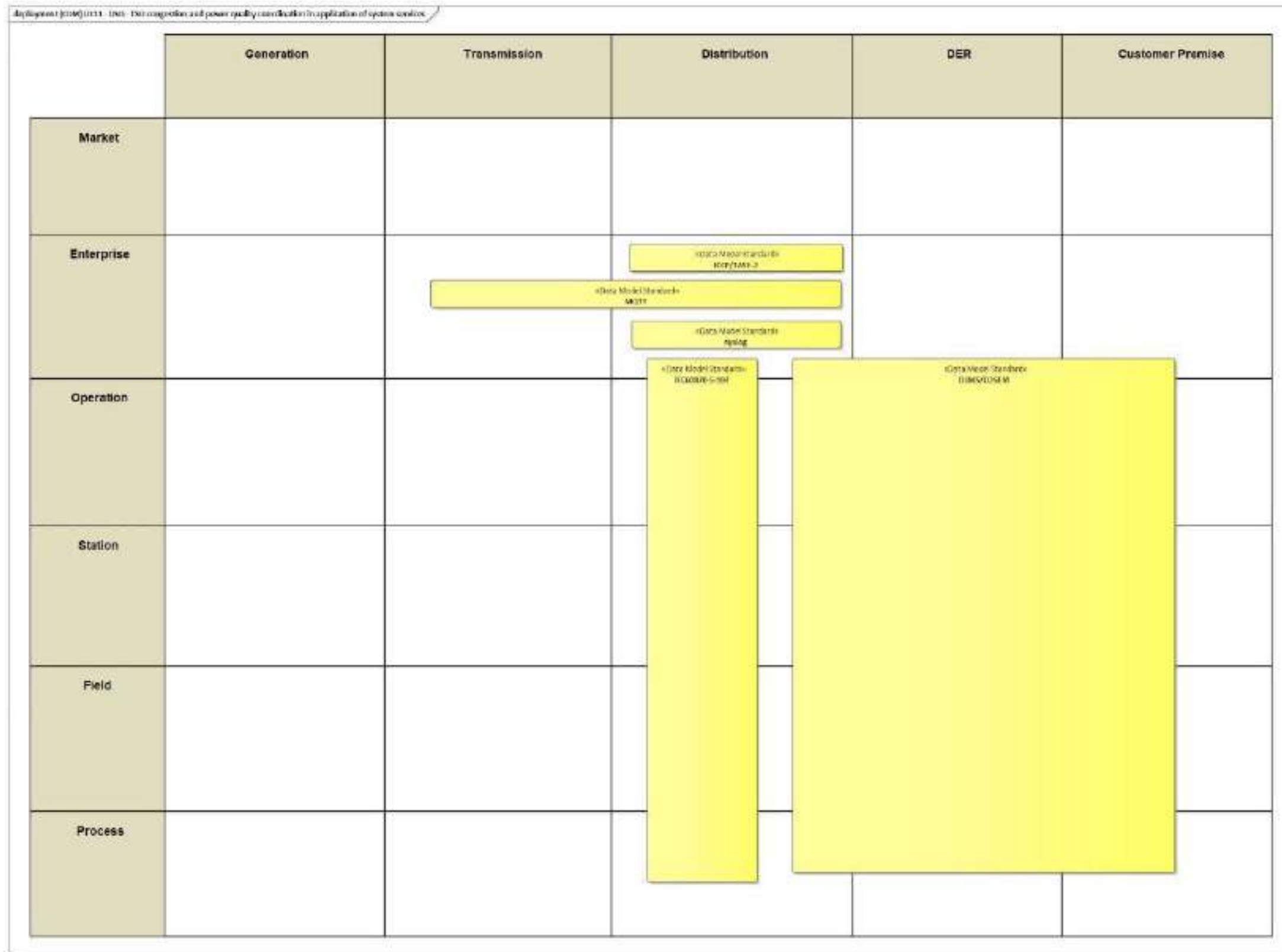


Figure 226 - UC11 Canonical Data Model



deployment (CDM) UC12 - Emergency & Restoration - Over-frequency protection module					
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation		<div>«Data Model Standard» Data Models::IPC</div>			
Station					
Field					
Process					

Figure 227 - UC12 Canonical Data Model

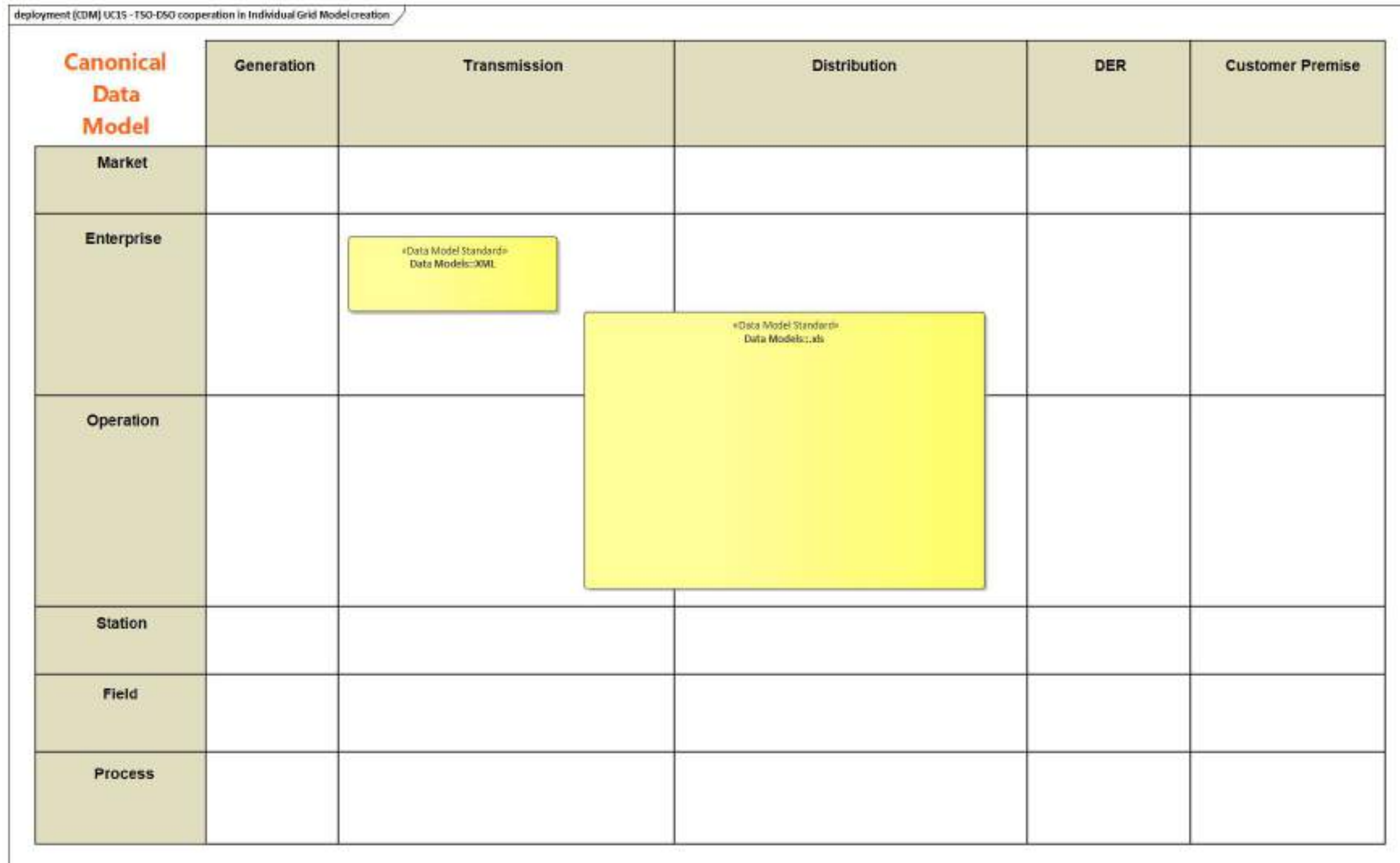


Figure 228 - UC15 Canonical Data Model



deployment (CMD) UC16 - Phasor angles monitoring and prevention of instability					
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

«Data Model ST...
Data models::IEC
60870-5-104

Figure 229 - UC16 Canonical Data Model



deployment [CMD] UC18 - Optimization of PMU installation points					
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation		<div>«Data Model Standard» Data models::Manual entry</div> <div>«Data Model Standard» Data models::xls</div> <div>«Data Model Standard» Data models::SFTP</div>			
Station					
Field					
Process					

Figure 230 - UC18 Canonical Data Model

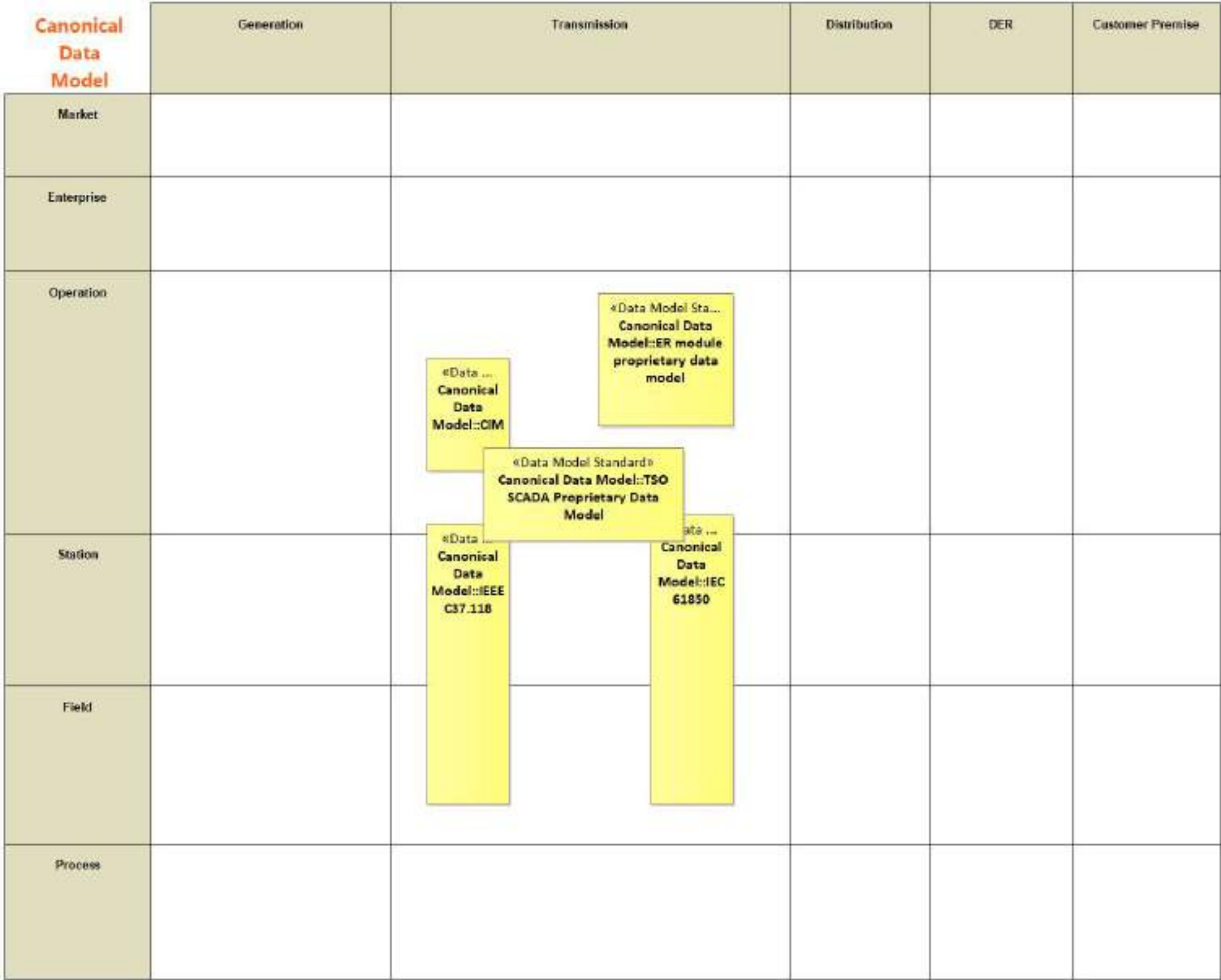


Figure 231 - UC19 Canonical Data Model

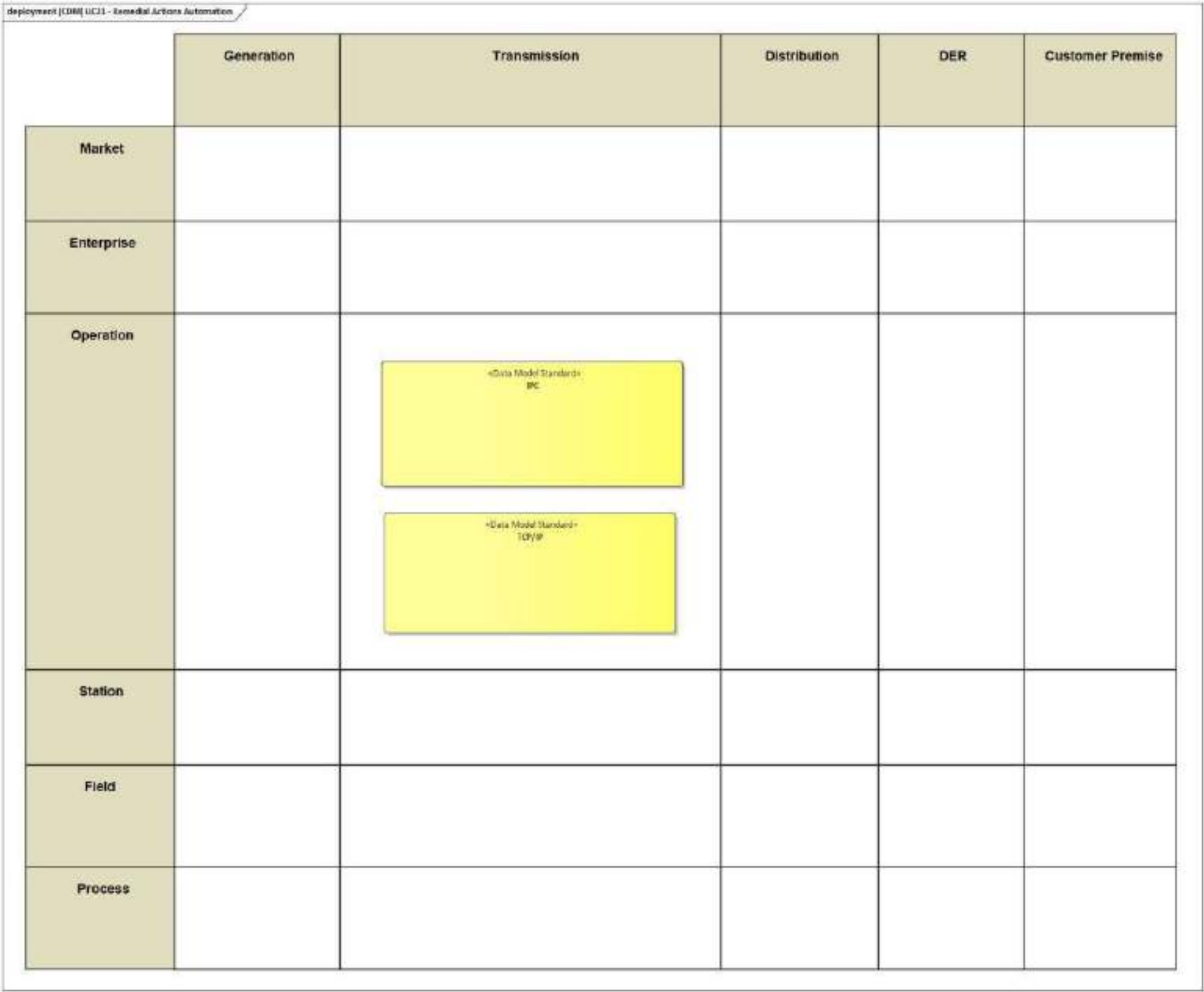


Figure 232 - UC21 Canonical Data Model

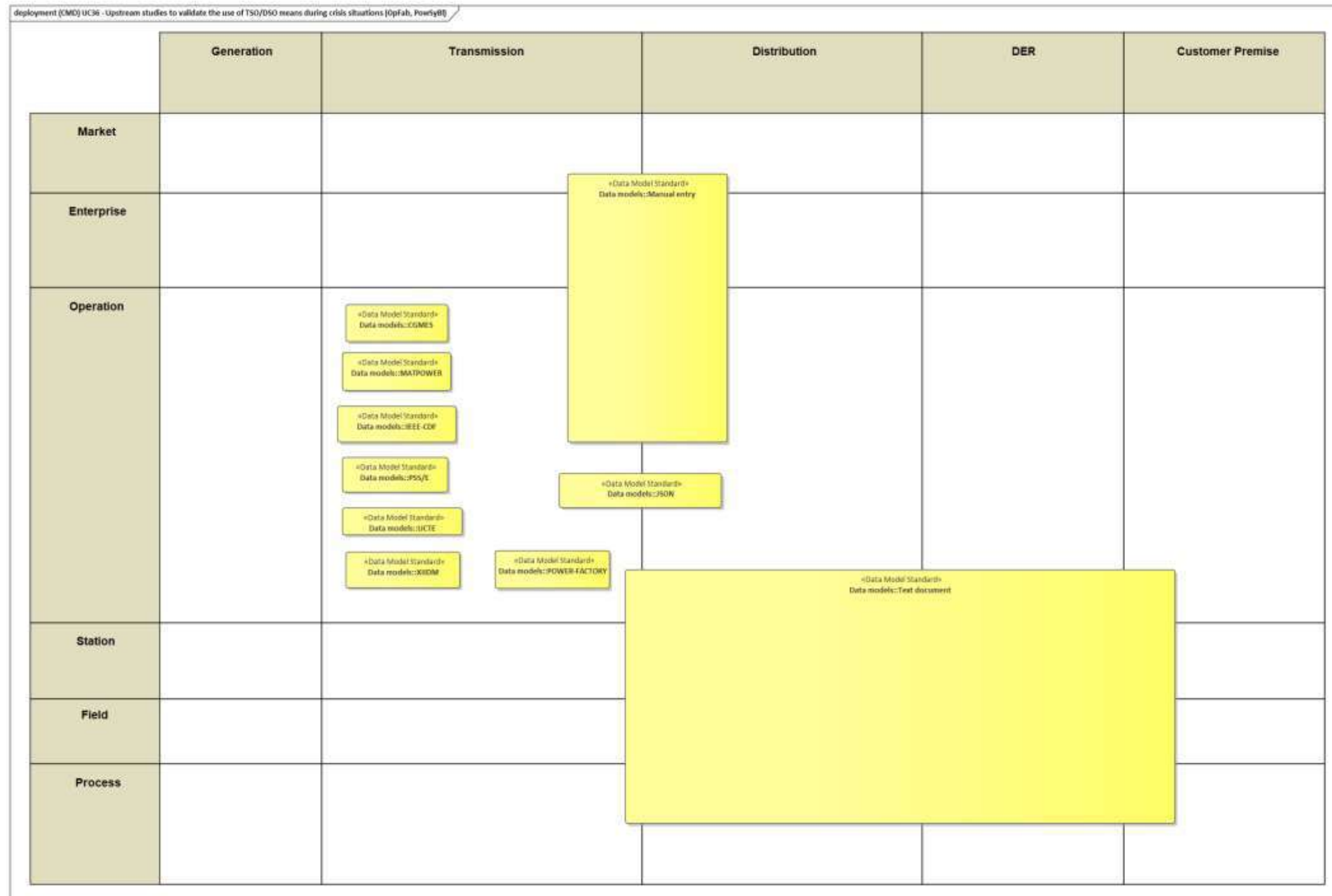


Figure 233 – UC35 Canonical Data Model



13.2.2.3 WP5-PRECOG

Canonical Data Model	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 234 - UC27 Canonical Data Model



Canonical Data Model	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 235 - UC28 Canonical Data Model

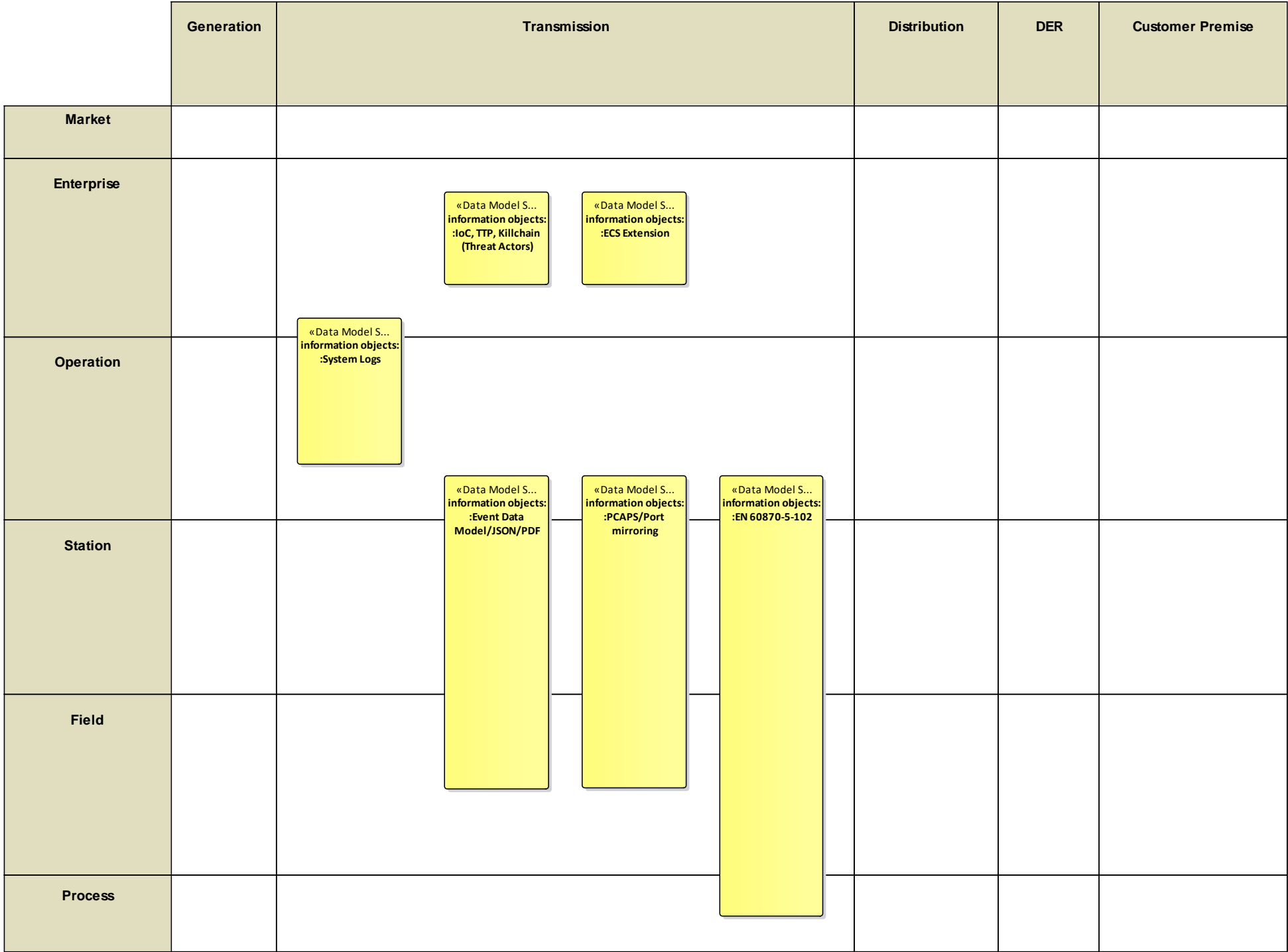


Figure 236 – UC33 Canonical Data Model

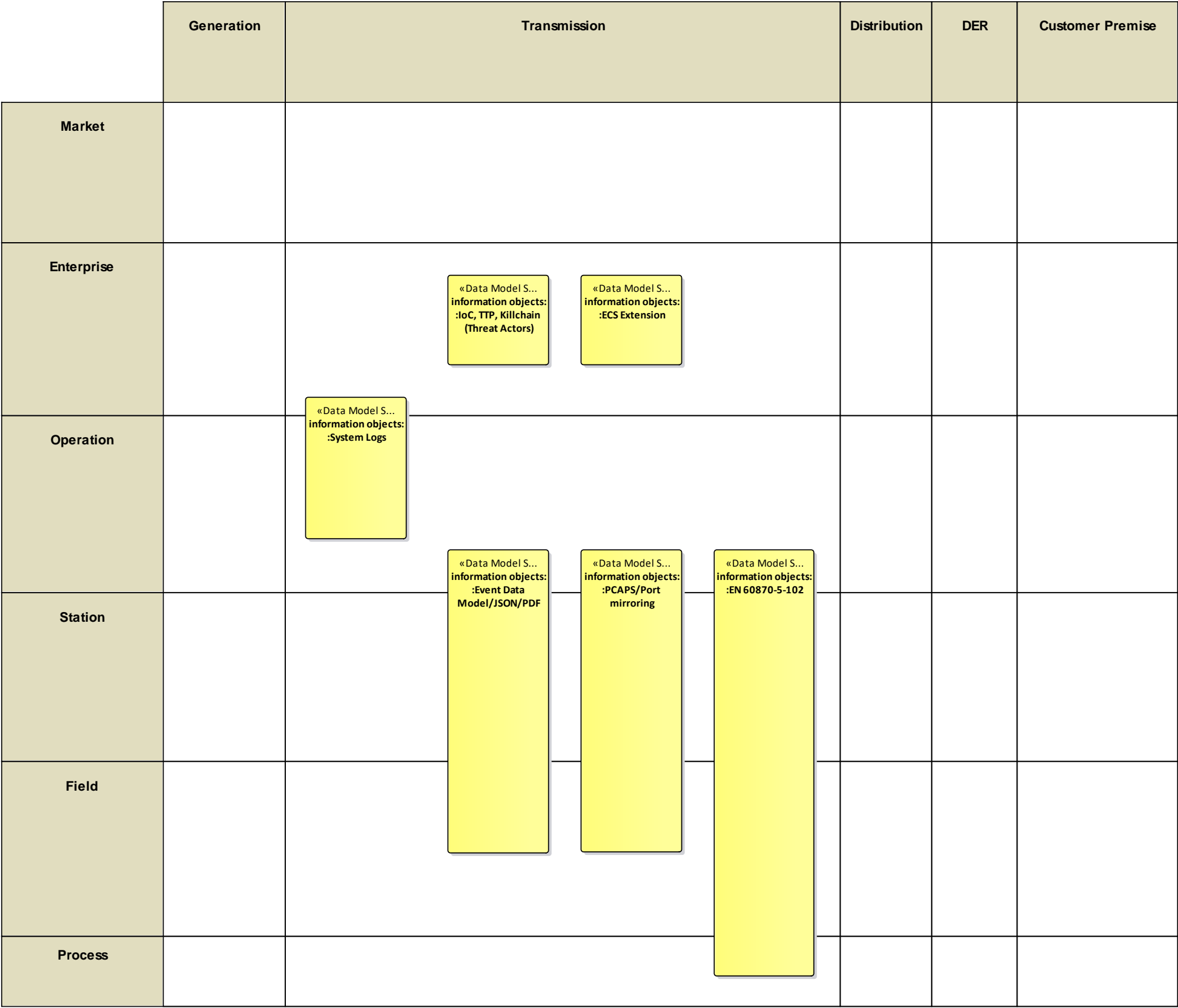


Figure 237 - UC34 Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise		<div>«Data Model S... information objects: :CIM/CGMES</div> <div>«Data Model S... information objects: :KSI datamodel</div>			
Operation					
Station					
Field					
Process					

Figure 238 - UC36 Canonical Data Model

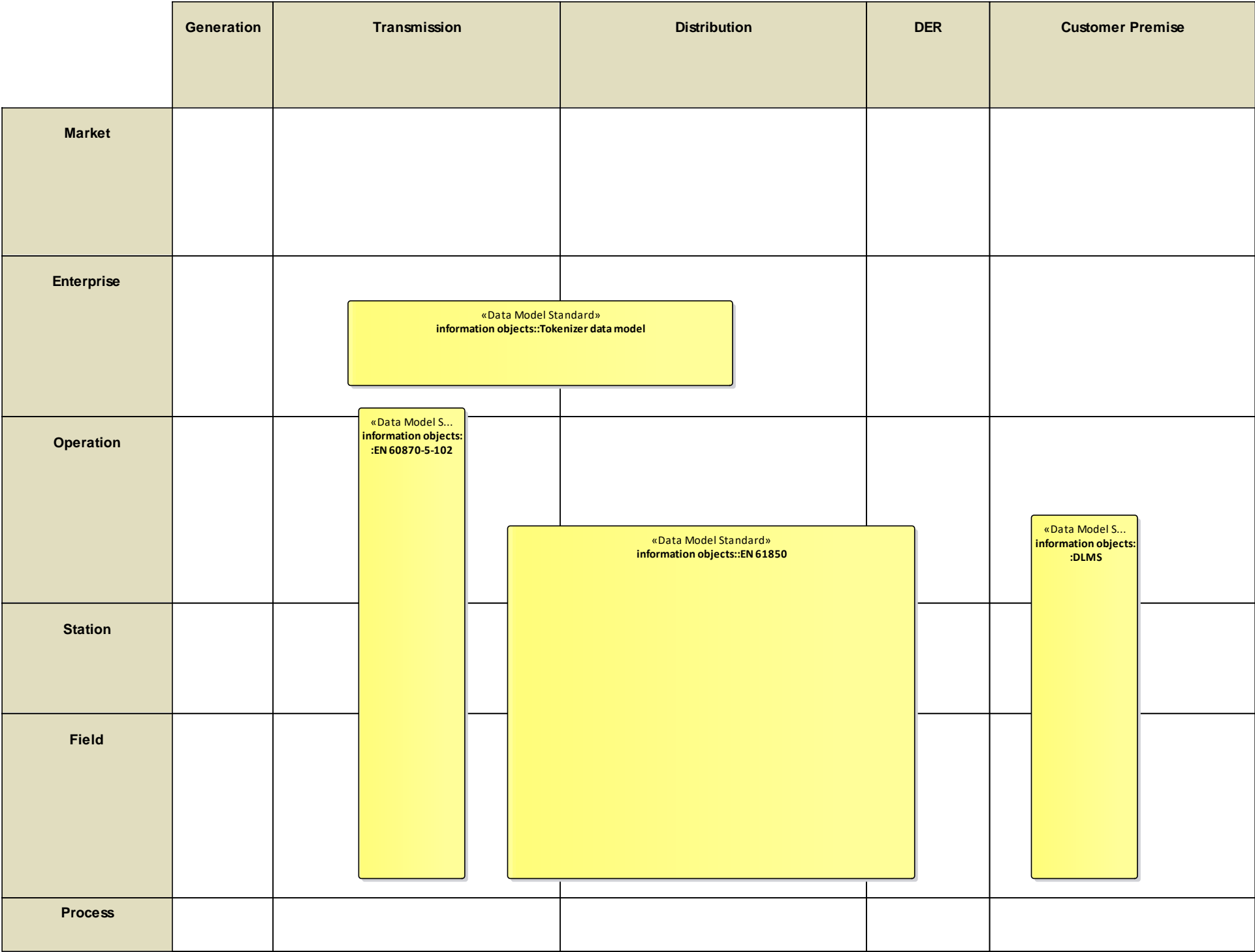


Figure 239 - UC37 Canonical Data Model

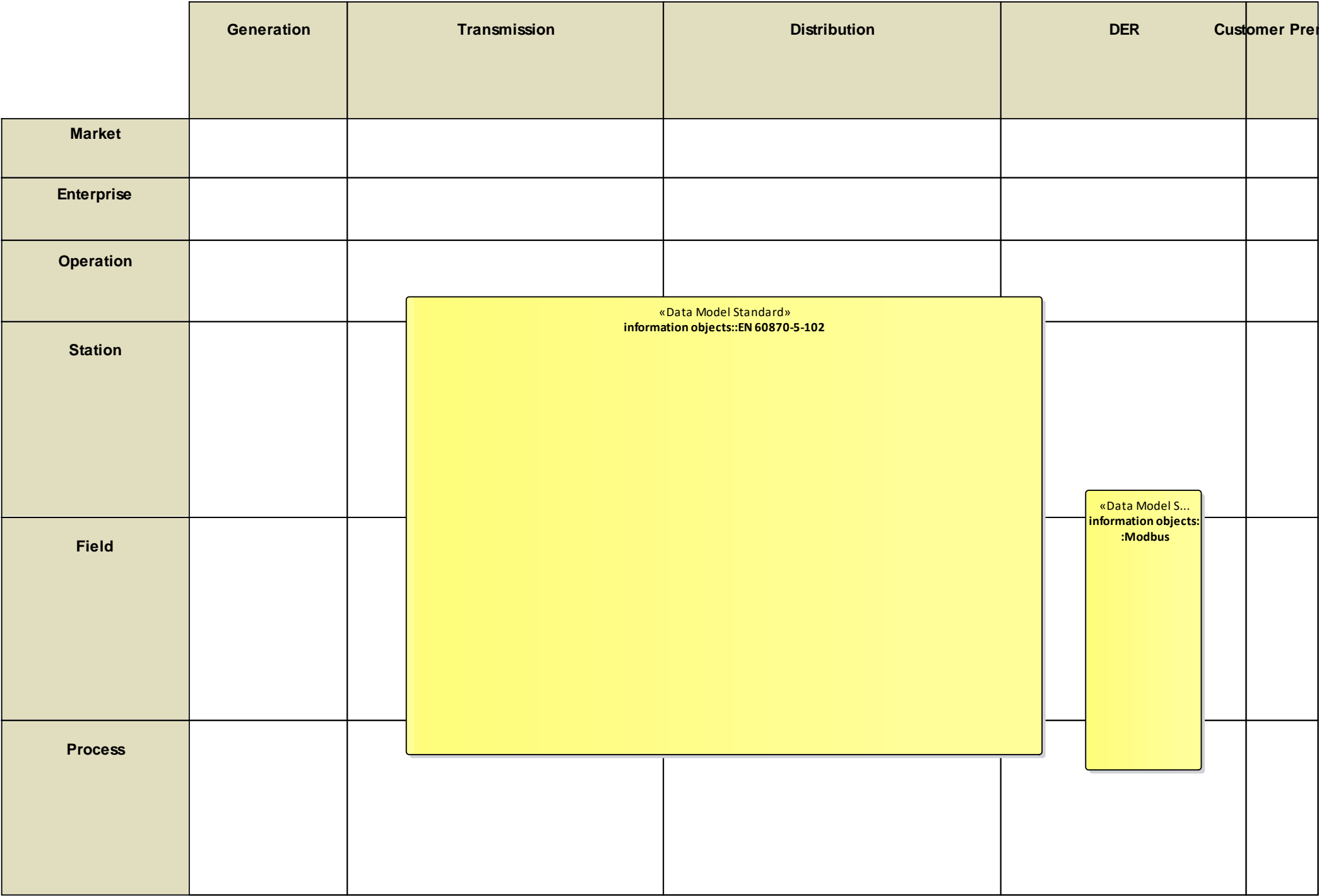


Figure 240 - UC38 Canonical Data Model

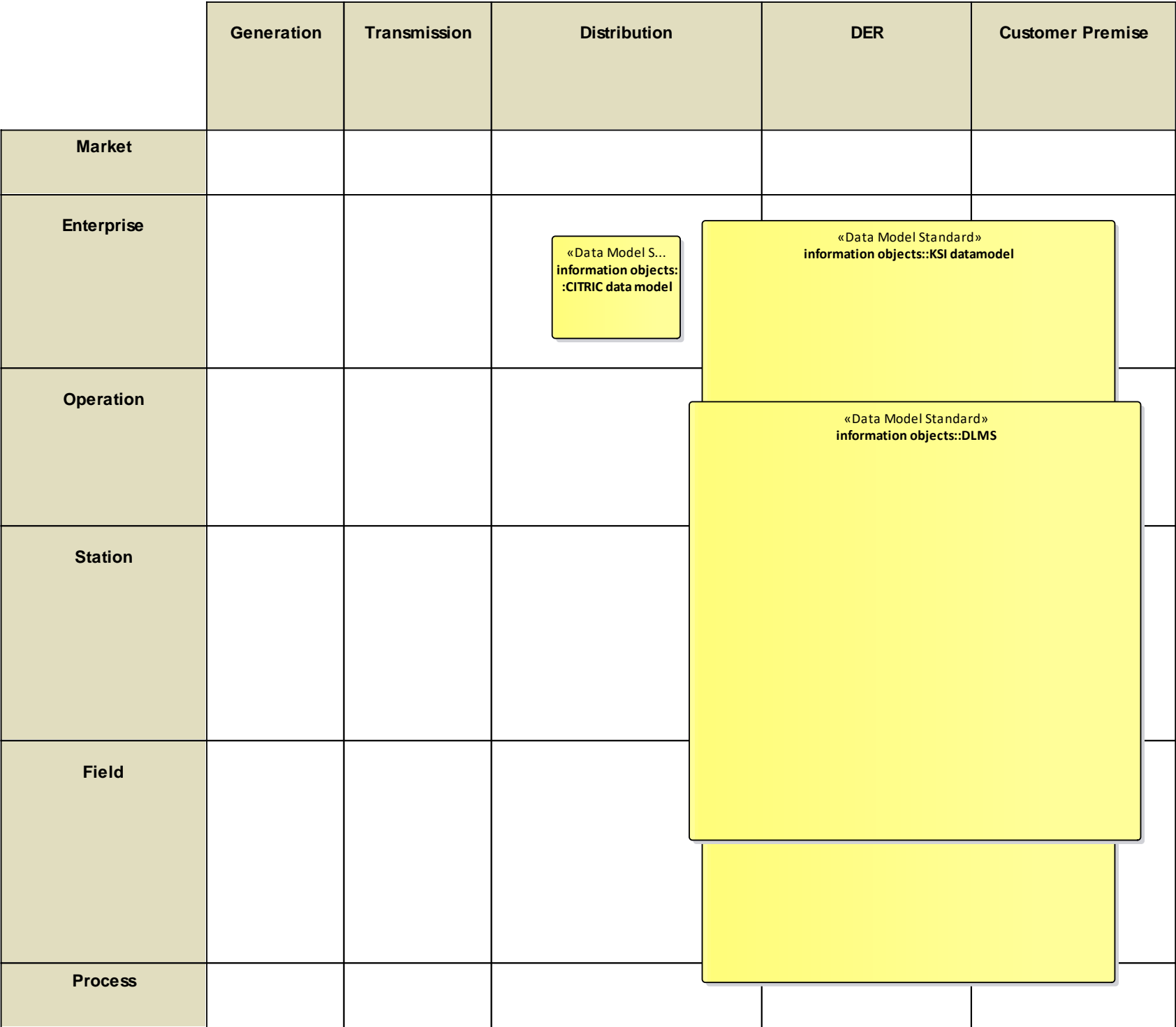


Figure 241 - UC40 Canonical Data Model



13.2.2.4 WP6-EMMA

	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

«Data Model Sta...
information objects::
CITRIC data model

«Data Mode...
information
objects::JPEG/FLIR

Figure 242 - UC01 Canonical Data Model

L

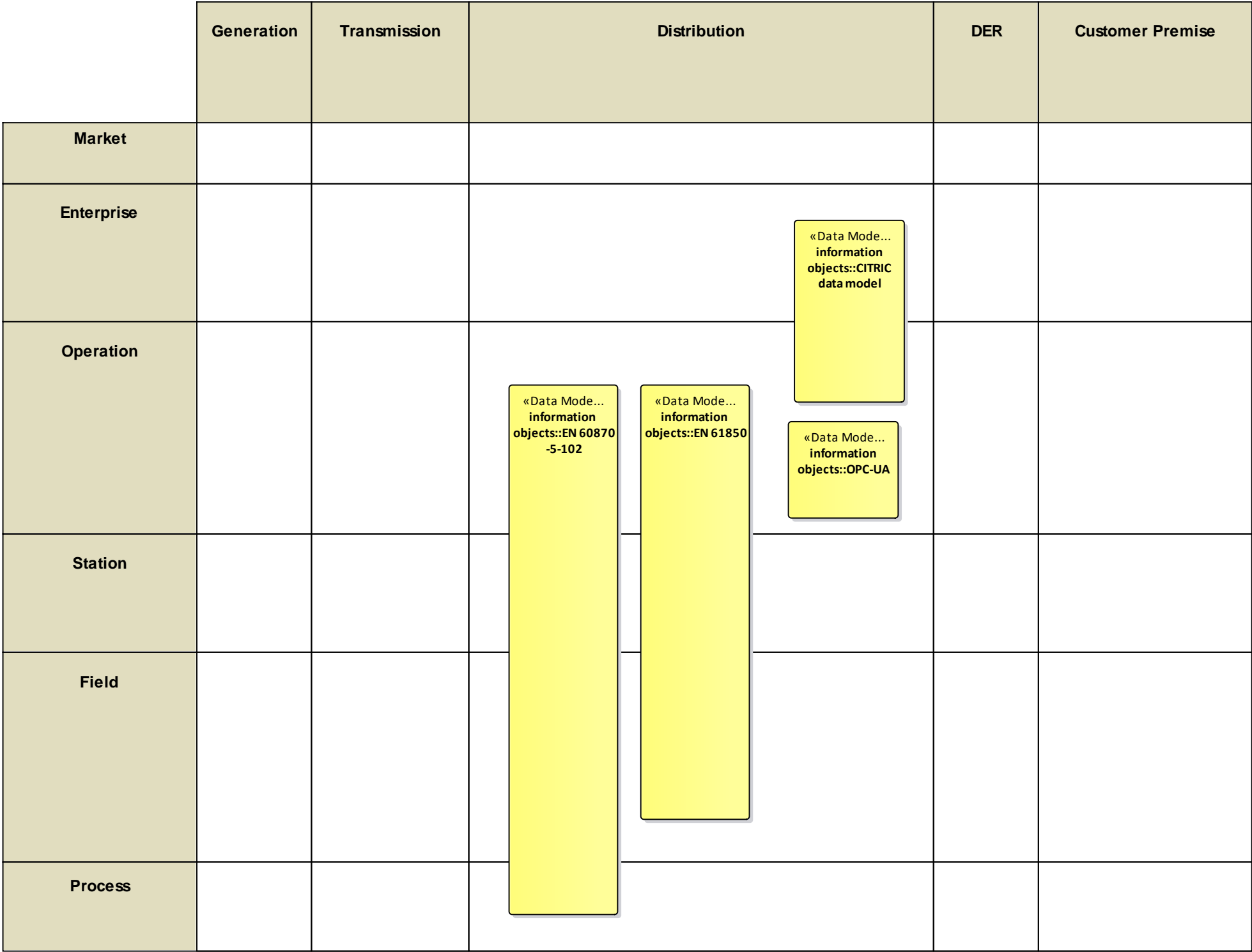


Figure 243 - UC02 Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise	<div>«Data Model S... information objects: :CITRIC data model</div>				
Operation					
Station	<div>«Data Model S... information objects: :JPEG/FLIR</div>				
Field					
Process					

Figure 244 - UC03 Canonical Data Model

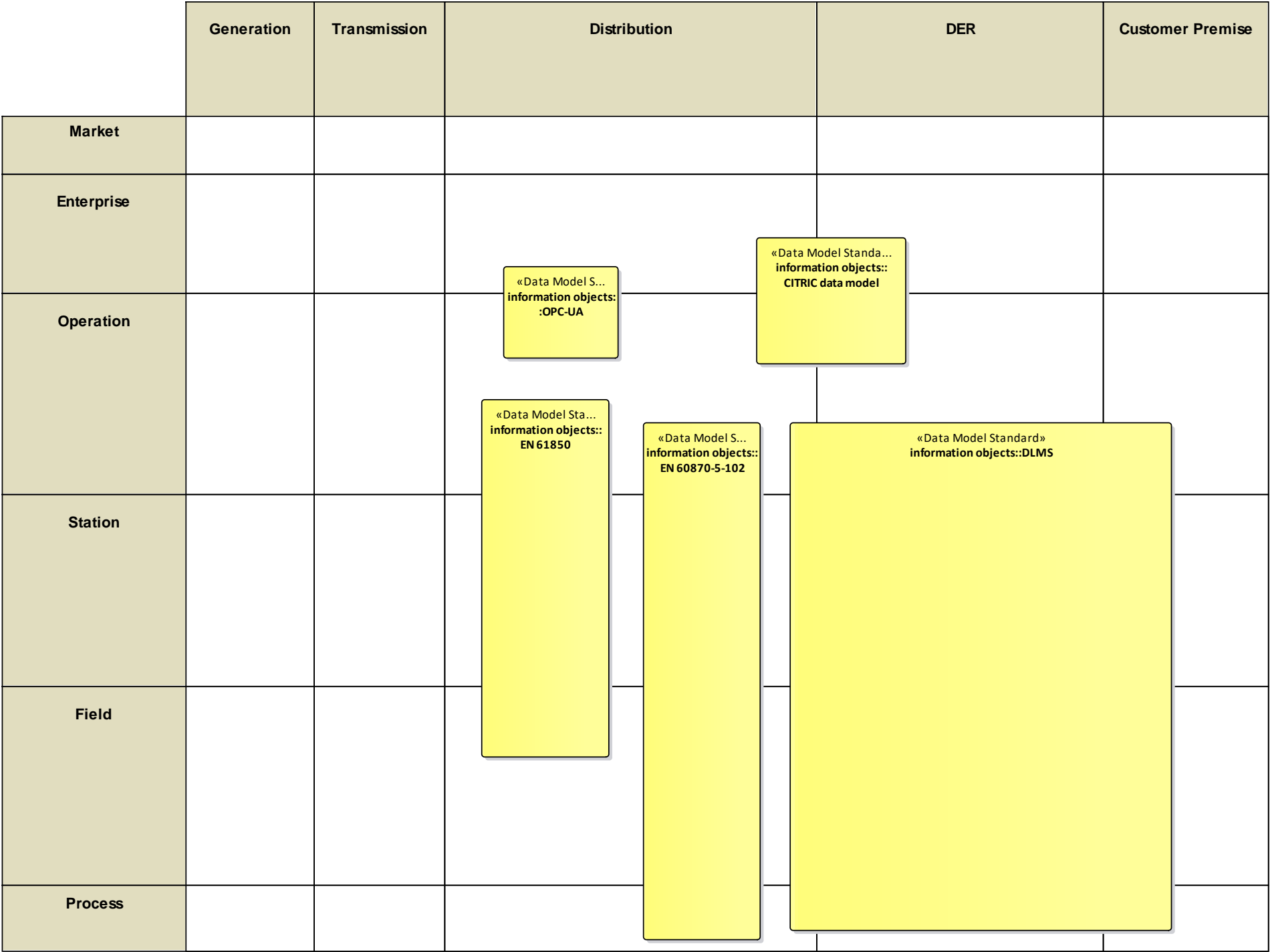


Figure 245 - UC04 Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

«Data Model S...
information objects:
:CITRIC data model

Figure 246 - UC05 Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

«Data Model S...
information objects:
:CITRIC data model

«Data Model S...
information objects:
:JPEG/FLIR

Figure 247 - UC06 Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise		<div>«Data Model S... information objects: :CIM/CGMES</div> <div>«Data Model S... information objects: :eTNA data model</div> <div>«Data Model S... information objects: :Op tool datamodel</div>			
Operation		<div>«Data Model S... information objects: :Communication tool datamodel</div>			
Station					
Field					
Process					

Figure 248 - UC08 Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise		<div>«Data Model S... information objects: :CIM/CGMES</div> <div>«Data Model S... information objects: :PQEL Data model</div>			
Operation					
Station					
Field					
Process					

Figure 249 - UC09 Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise		<div>«Data Model S... information objects: :CIM/CGMES</div>			
Operation		<div>«Data Model S... information objects: :Communication tool datamodel</div>			
Station					
Field					
Process					

Figure 250 – UC13Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation		<div>«Data Model S... information objects: :CIM/CGMES</div>			
Station					
Field					
Process					

Figure 251 - UC14 Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation		<div>«Data Model S... information objects: :Op tool datamodel</div> <div>«Data Model S... information objects: :CIM/CGMES</div>			
Station					
Field					
Process					

Figure 252 - UC17 Canonical Data Model



	Generation	Transmission	Distribution		DER	Customer Premise
Market						
Enterprise						
Operation						
Station						
Field						
Process						

«Data Model S...
information objects:
:CITRIC data model

«Data Model S...
information objects:
:JPEG/FLIR

Figure 253 - UC20 Canonical Data Model



	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise		<div>«Data Model S... information objects: :CIM/CGMES</div> <div>«Data Model S... information objects: :OPC-UA</div>			
Operation					
Station					
Field					
Process					

Figure 254 - UC31 Canonical Data Model

13.2.3 Standard and Information Object Mapping

13.2.3.1 WP3-C3PO

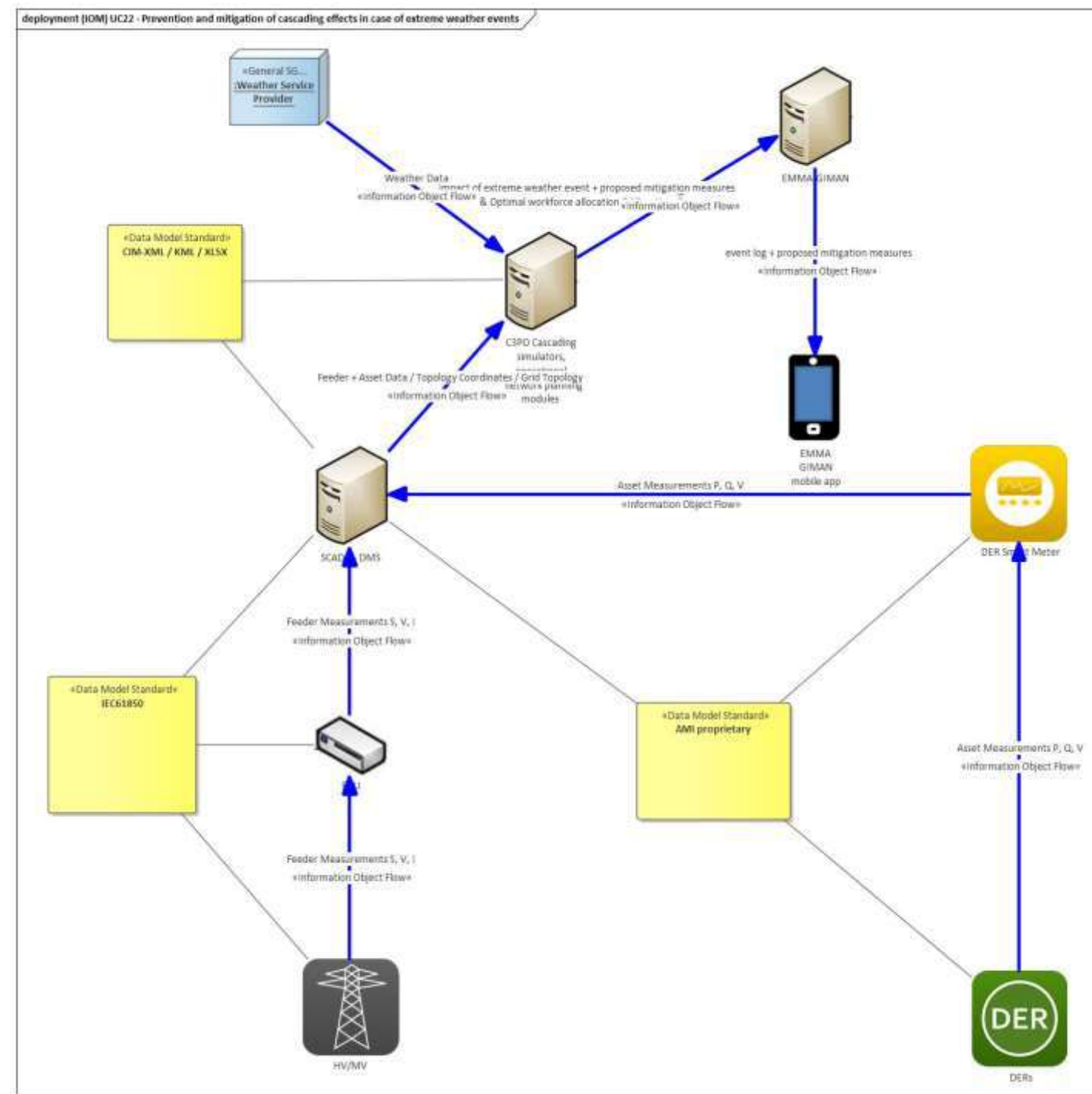


Figure 255 - UC22 Information Object Mapping

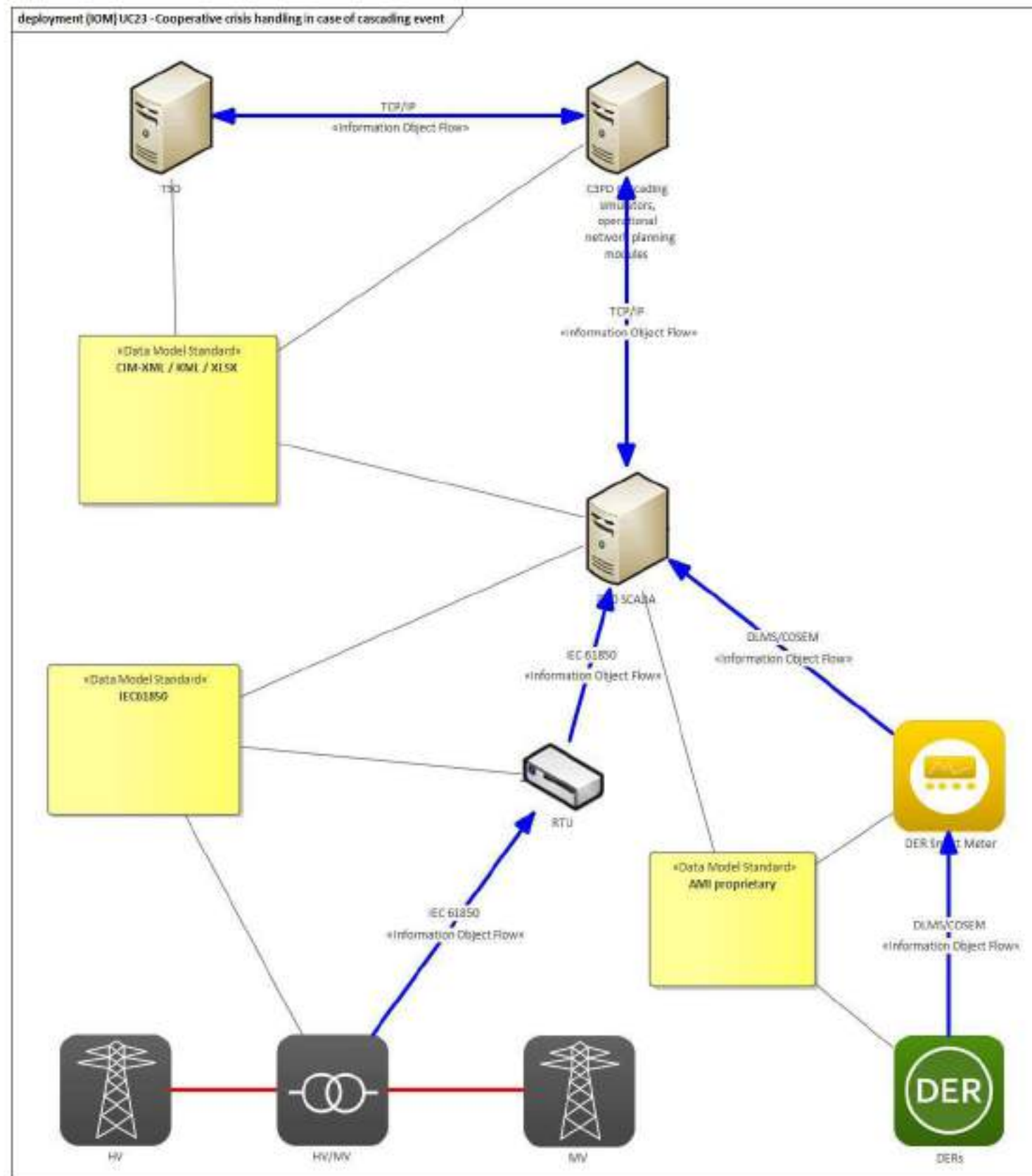


Figure 256 - UC23 Information Object Mapping

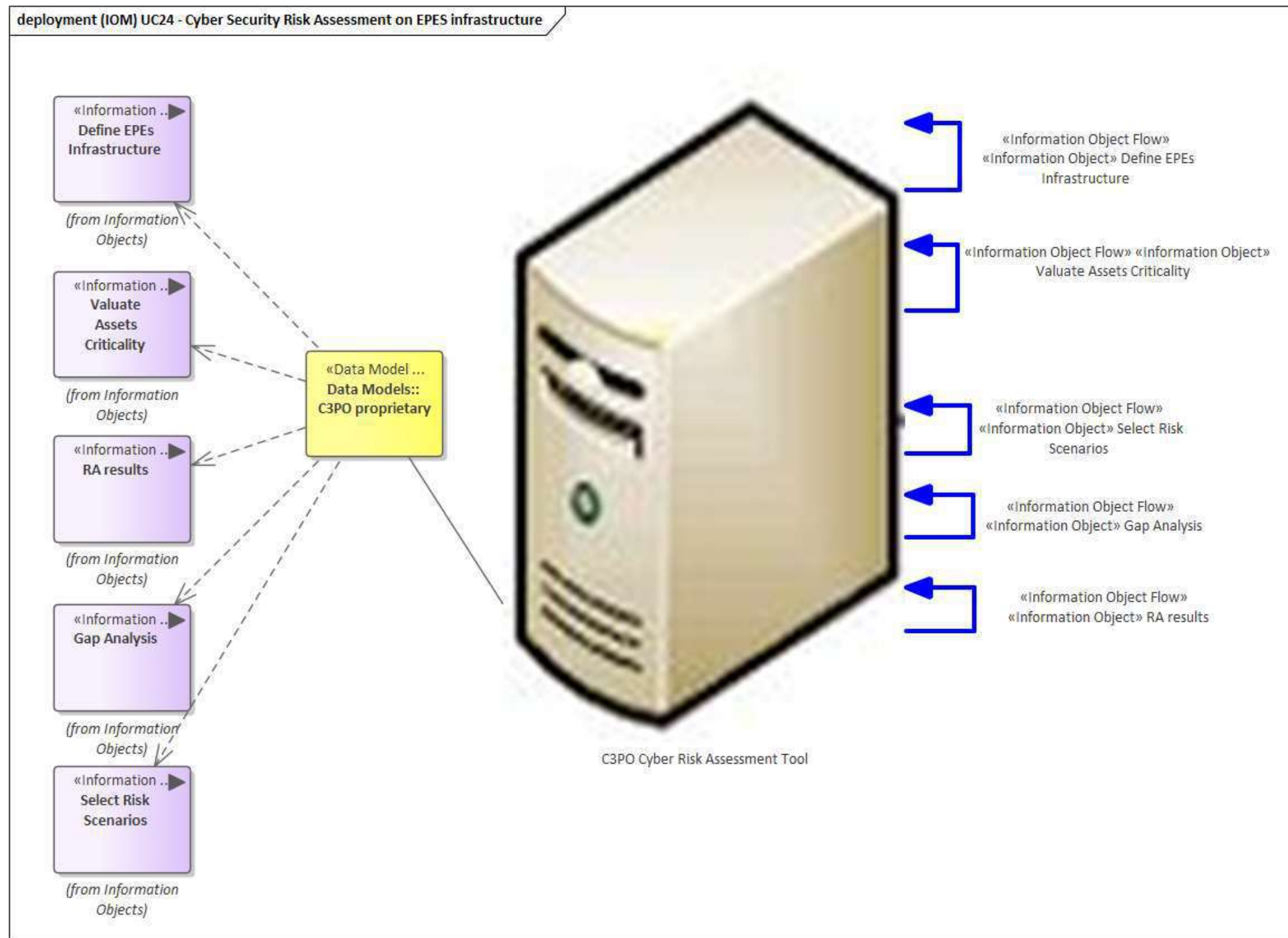


Figure 257 - UC24 Information Object Mapping

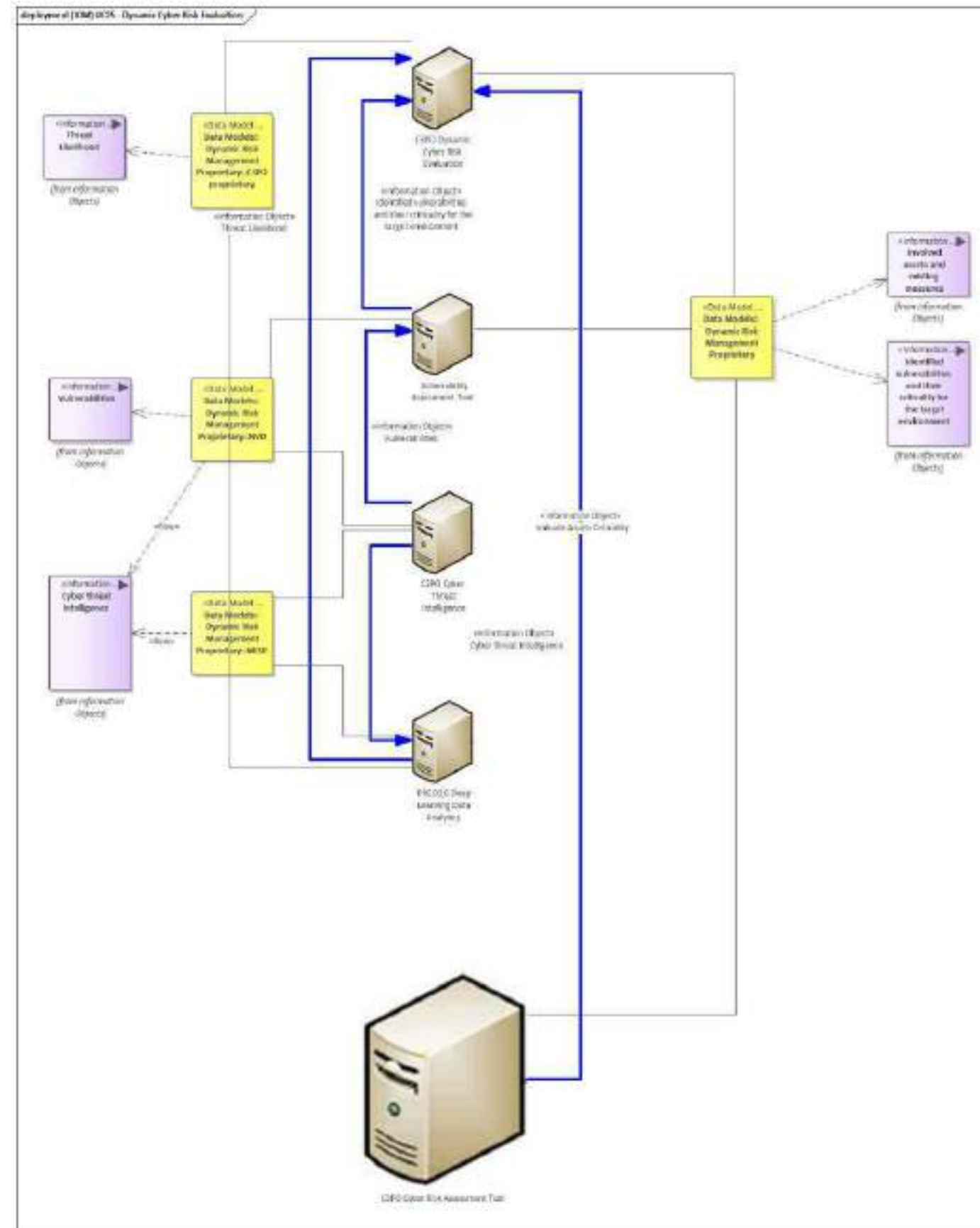


Figure 258 - UC25 Information Object Mapping

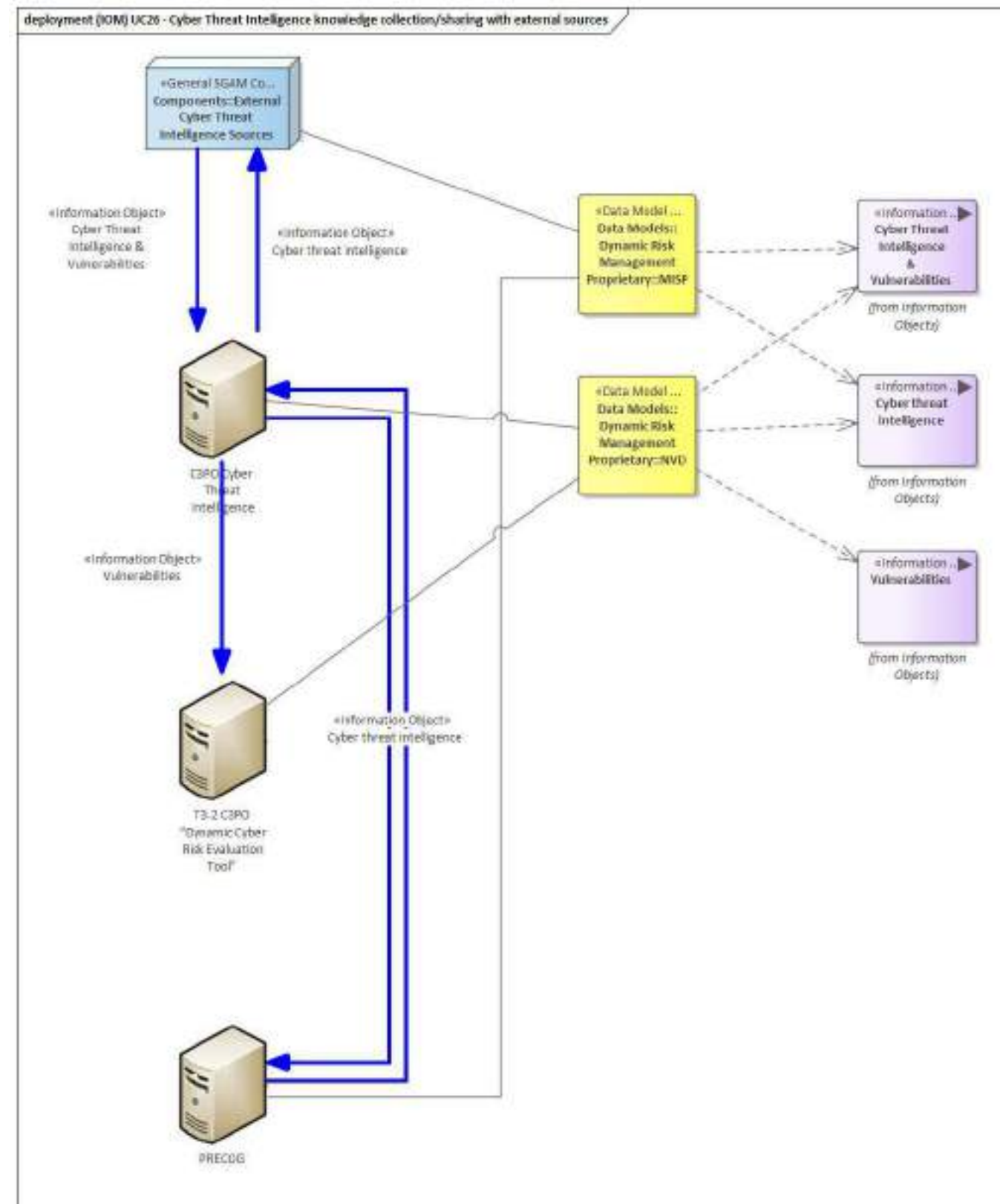
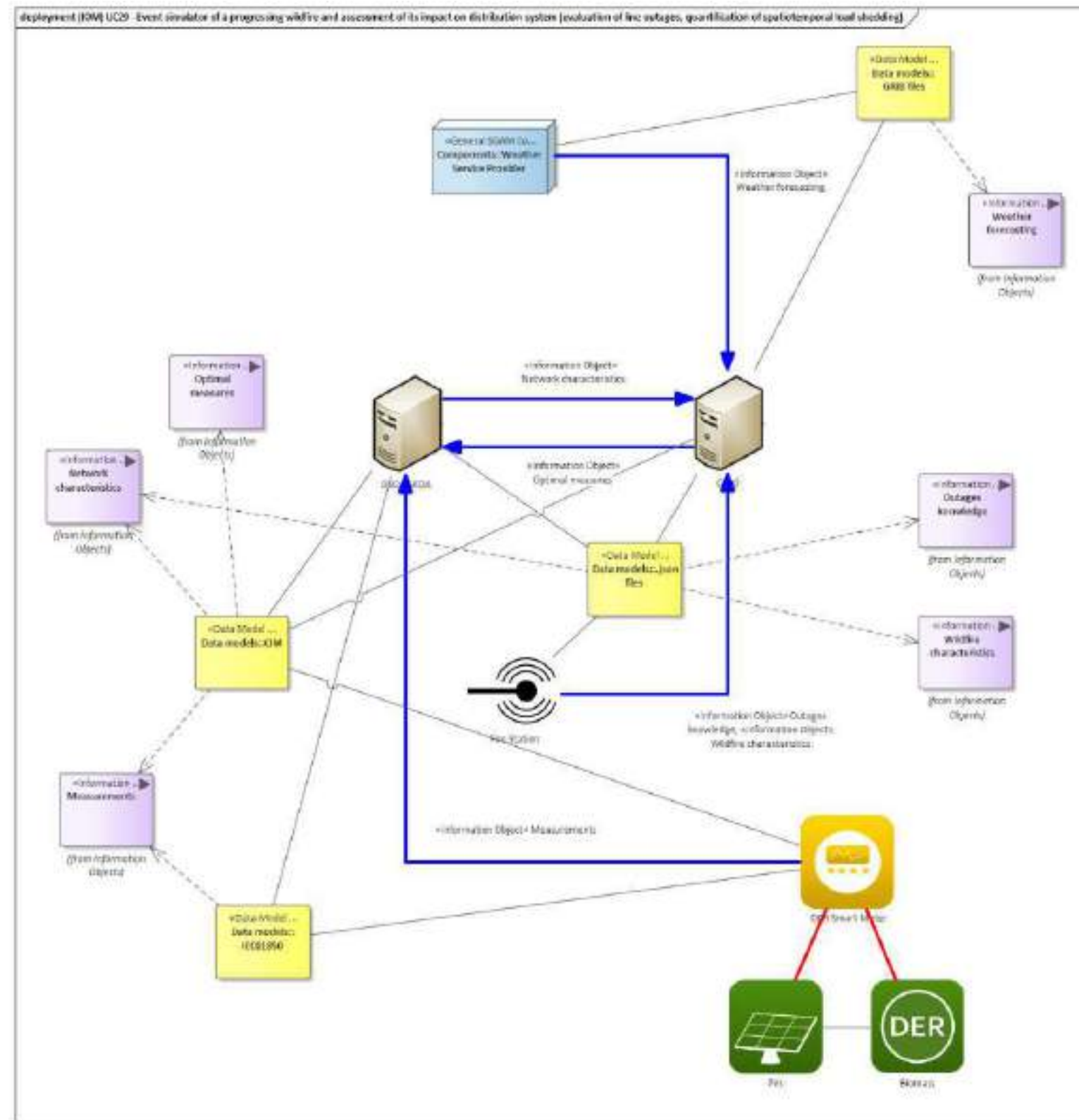


Figure 259 - UC26 Information Object Mapping



921



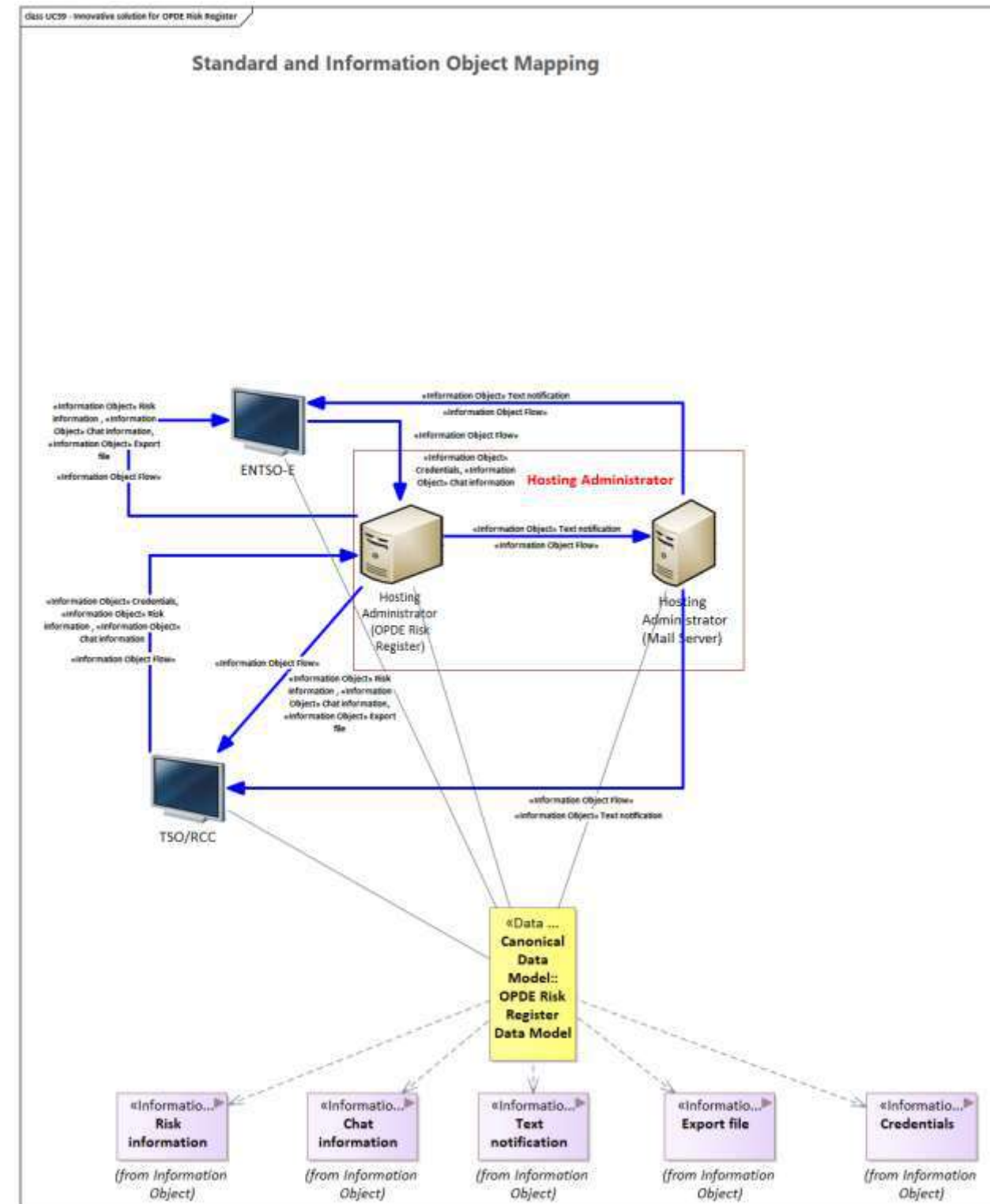


Figure 263 - UC39 Information Object Mapping

13.2.3.2 WP4-IRIS

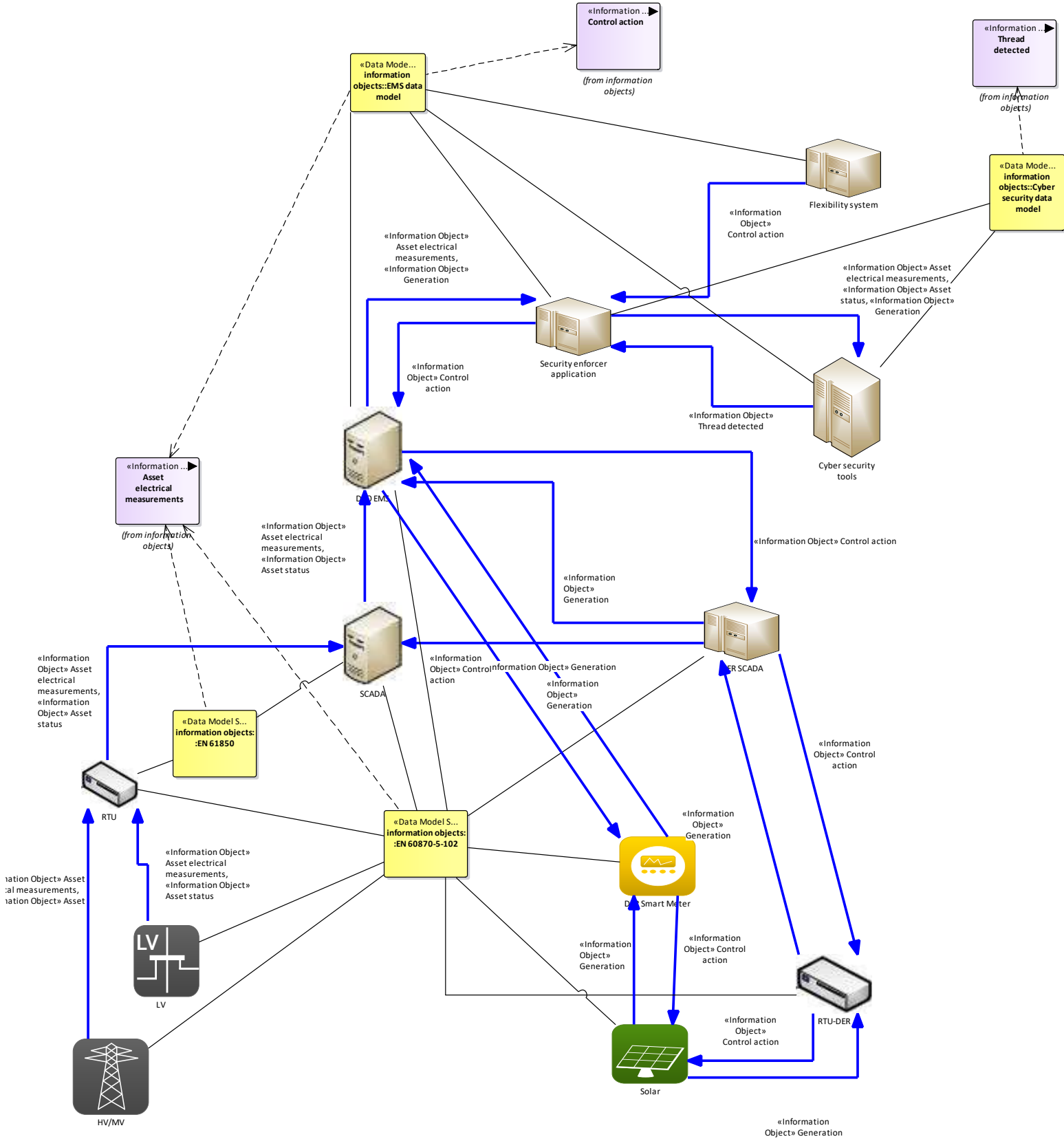


Figure 264 - UC07 Information Object Mapping

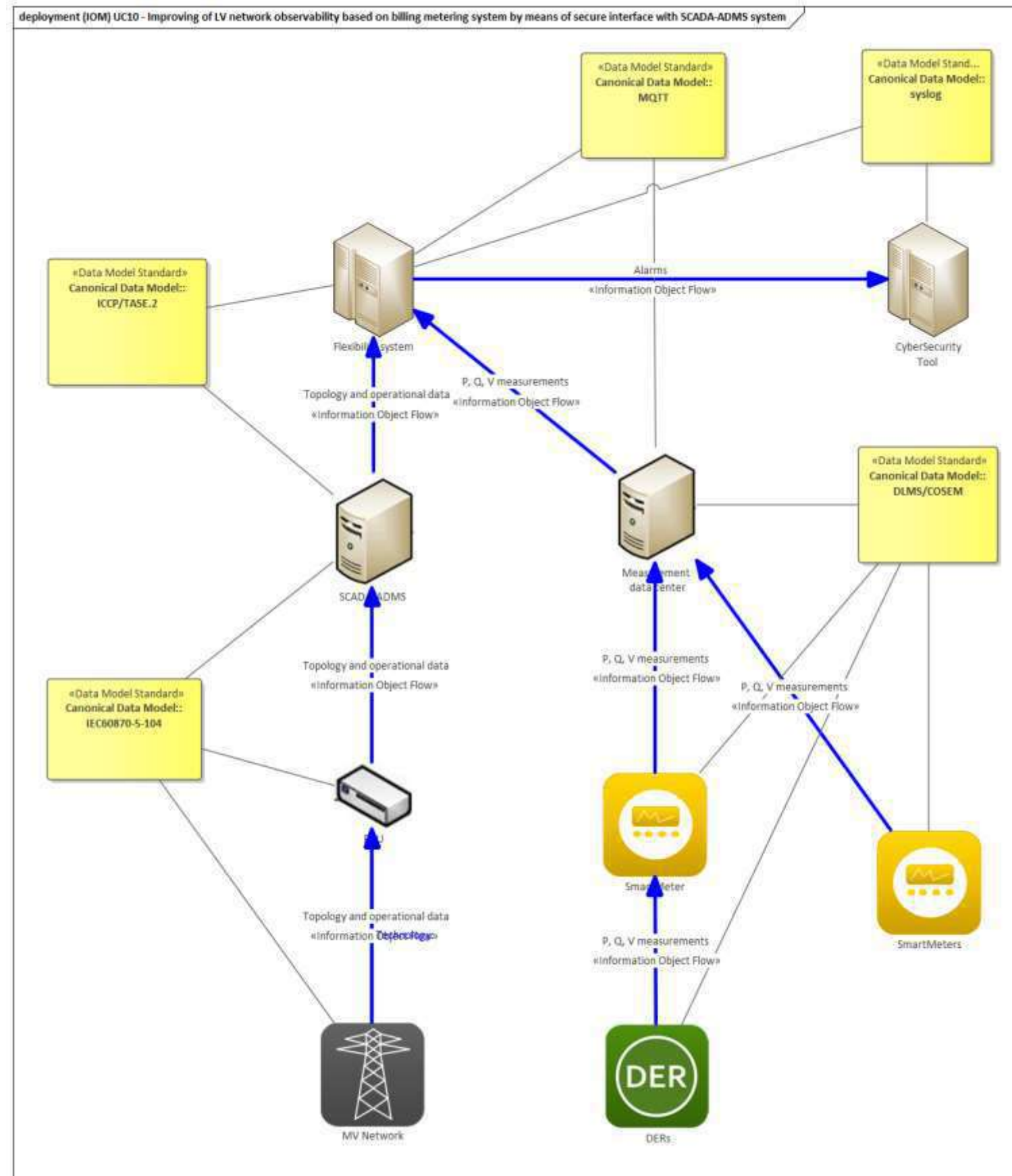


Figure 265 - UC10 Information Object Mapping

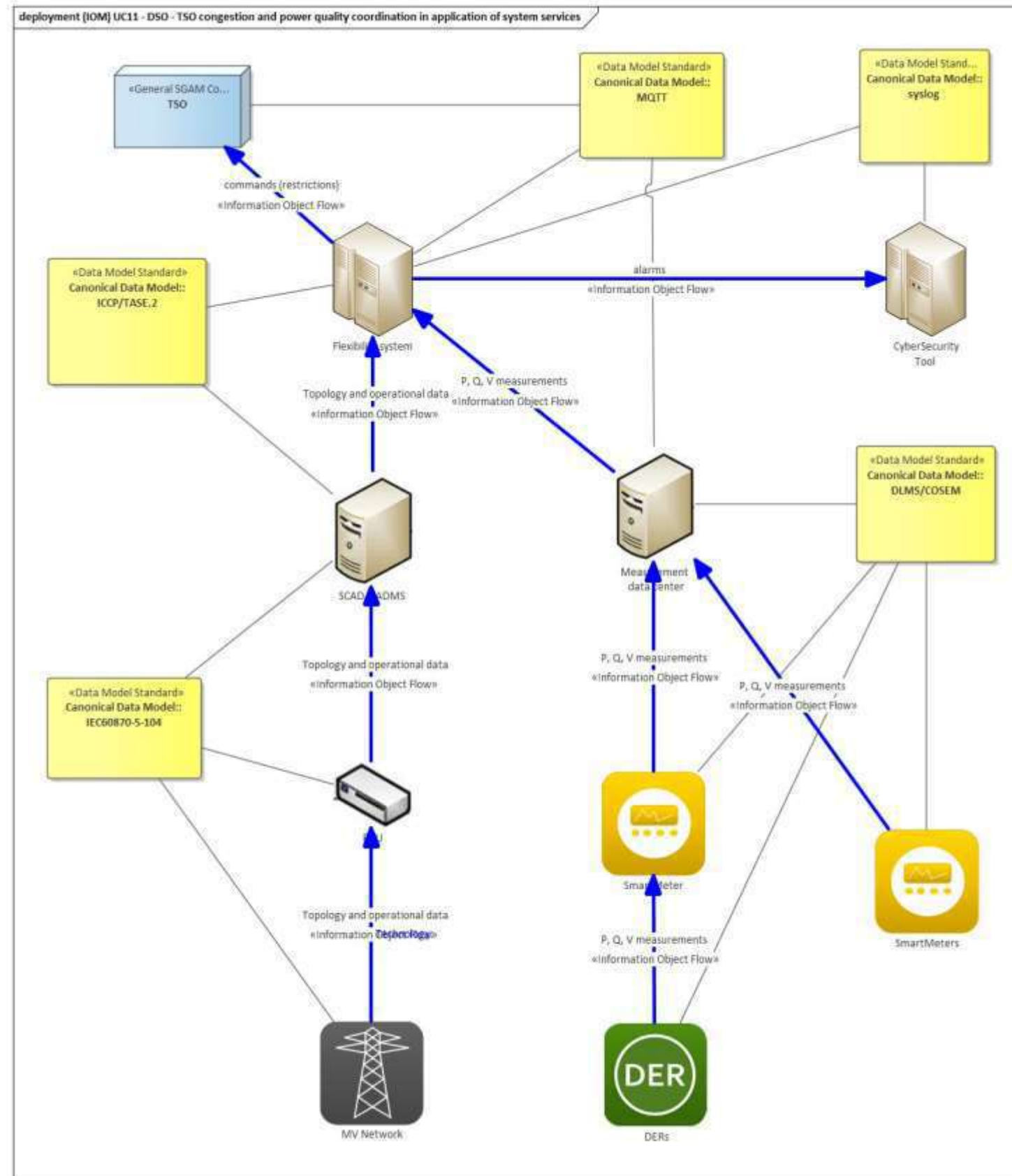


Figure 266 - UC11 Information Object Mapping

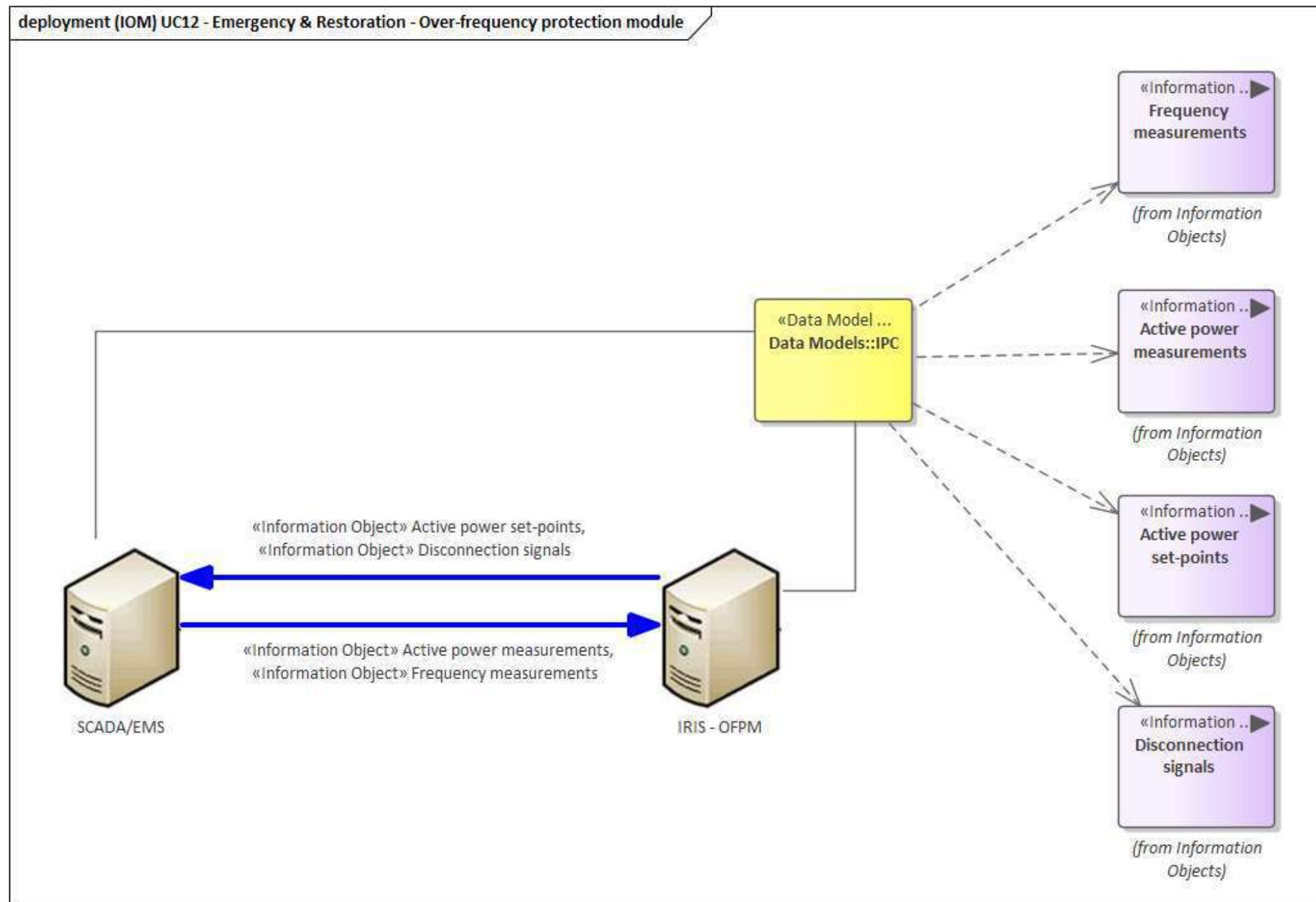


Figure 267 - UC12 Information Object Mapping

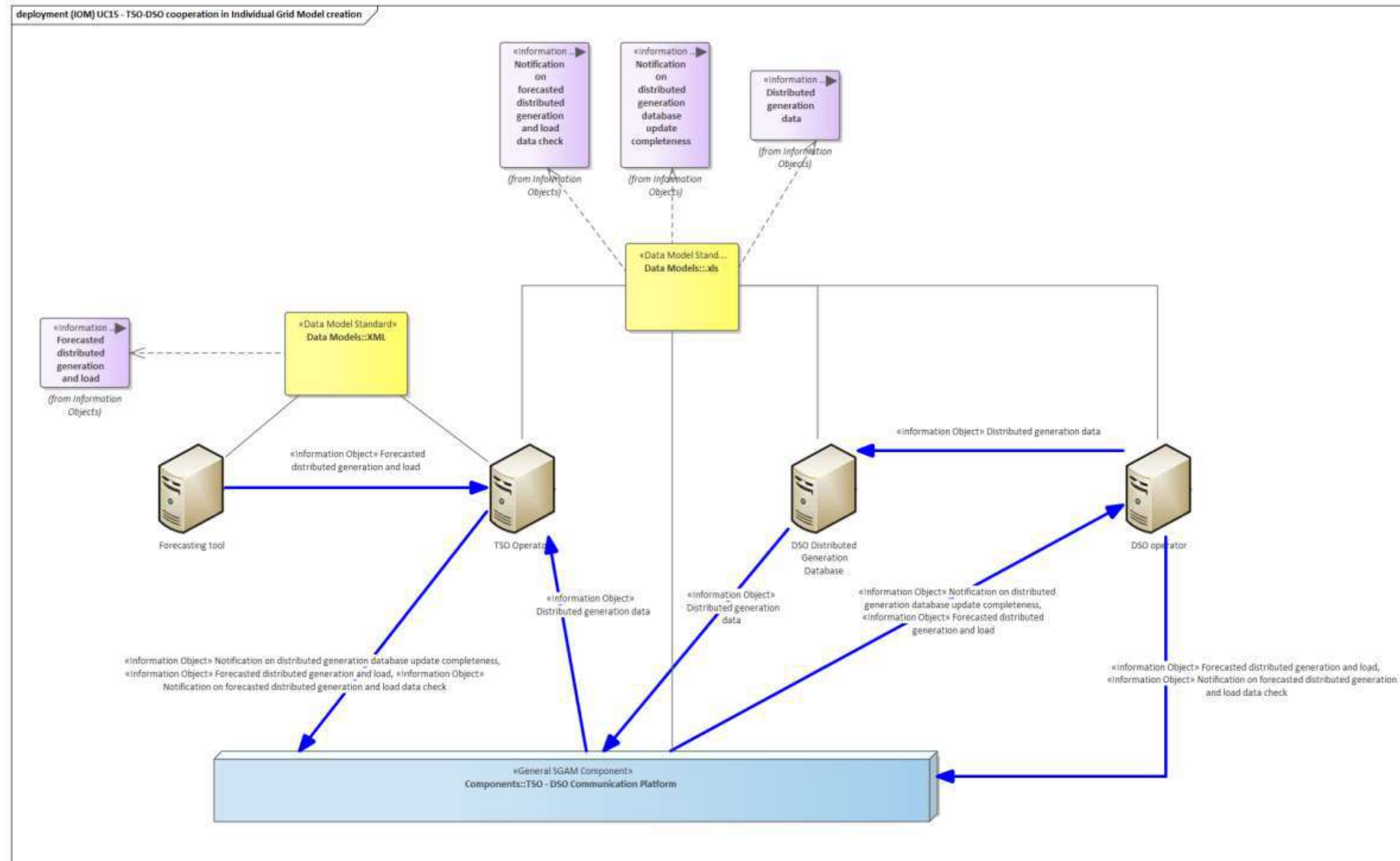


Figure 268 - UC15 Information Object Mapping

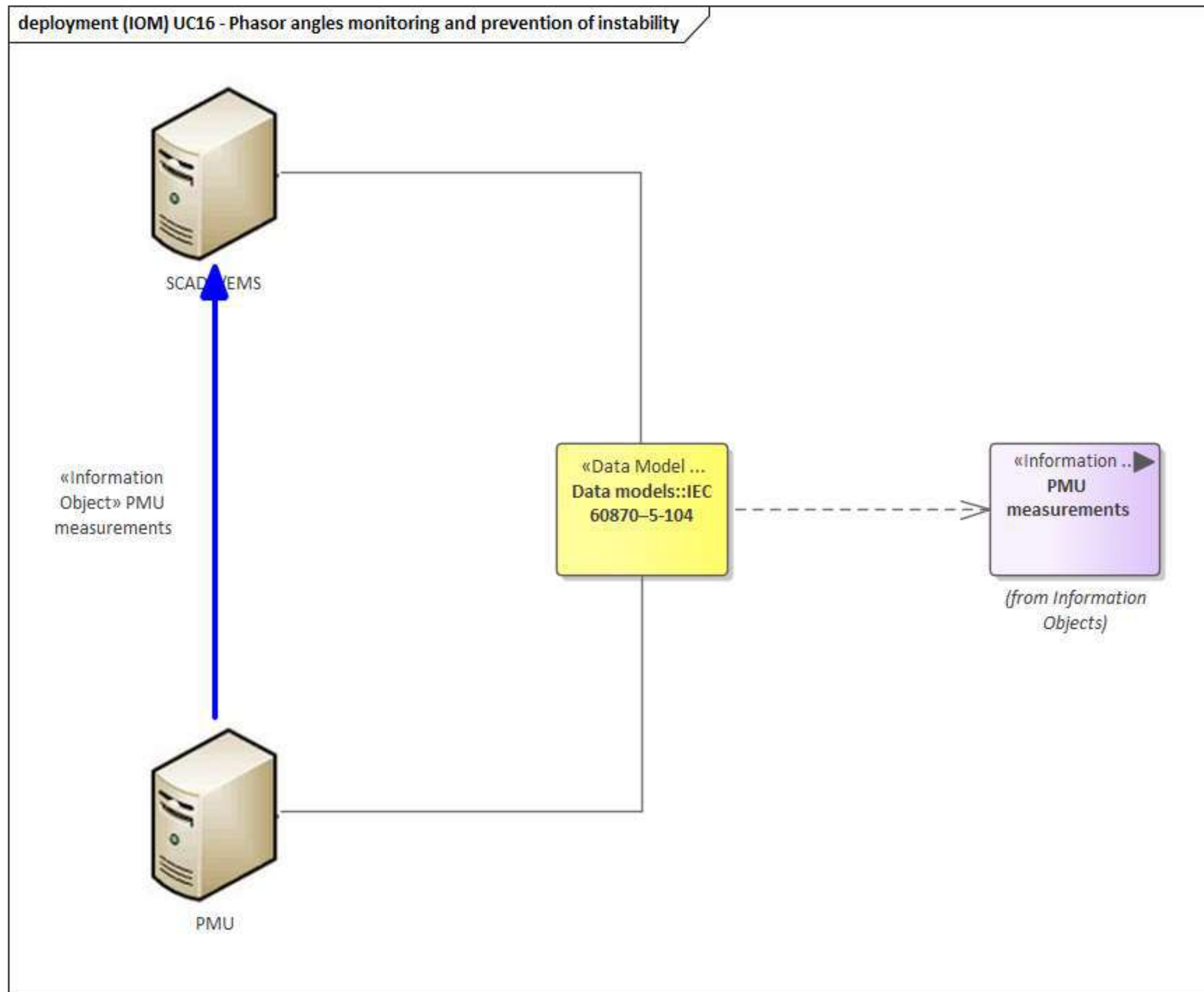


Figure 269 - UC16 Information Object Mapping

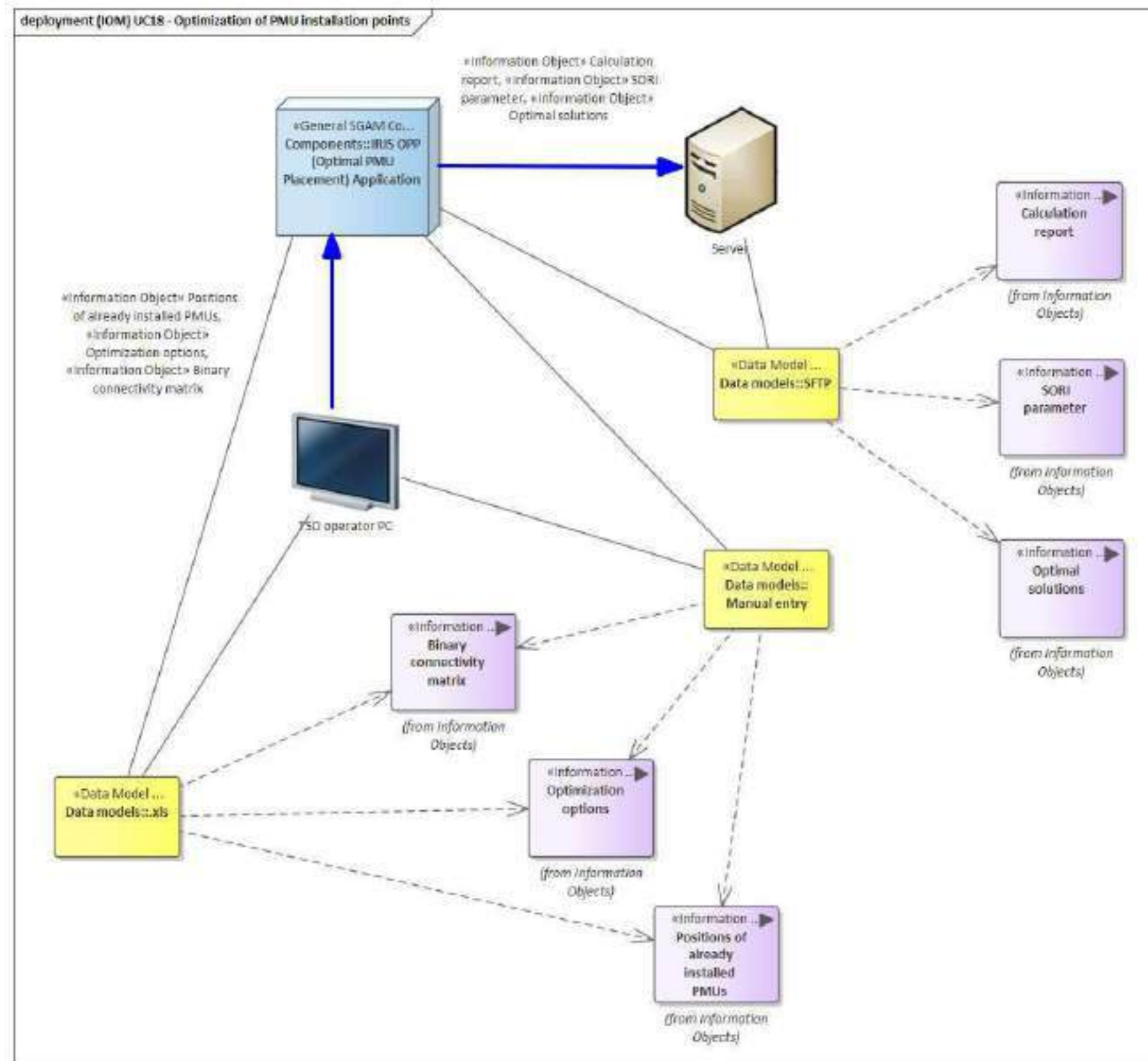


Figure 270 - UC18 Information Object Mapping

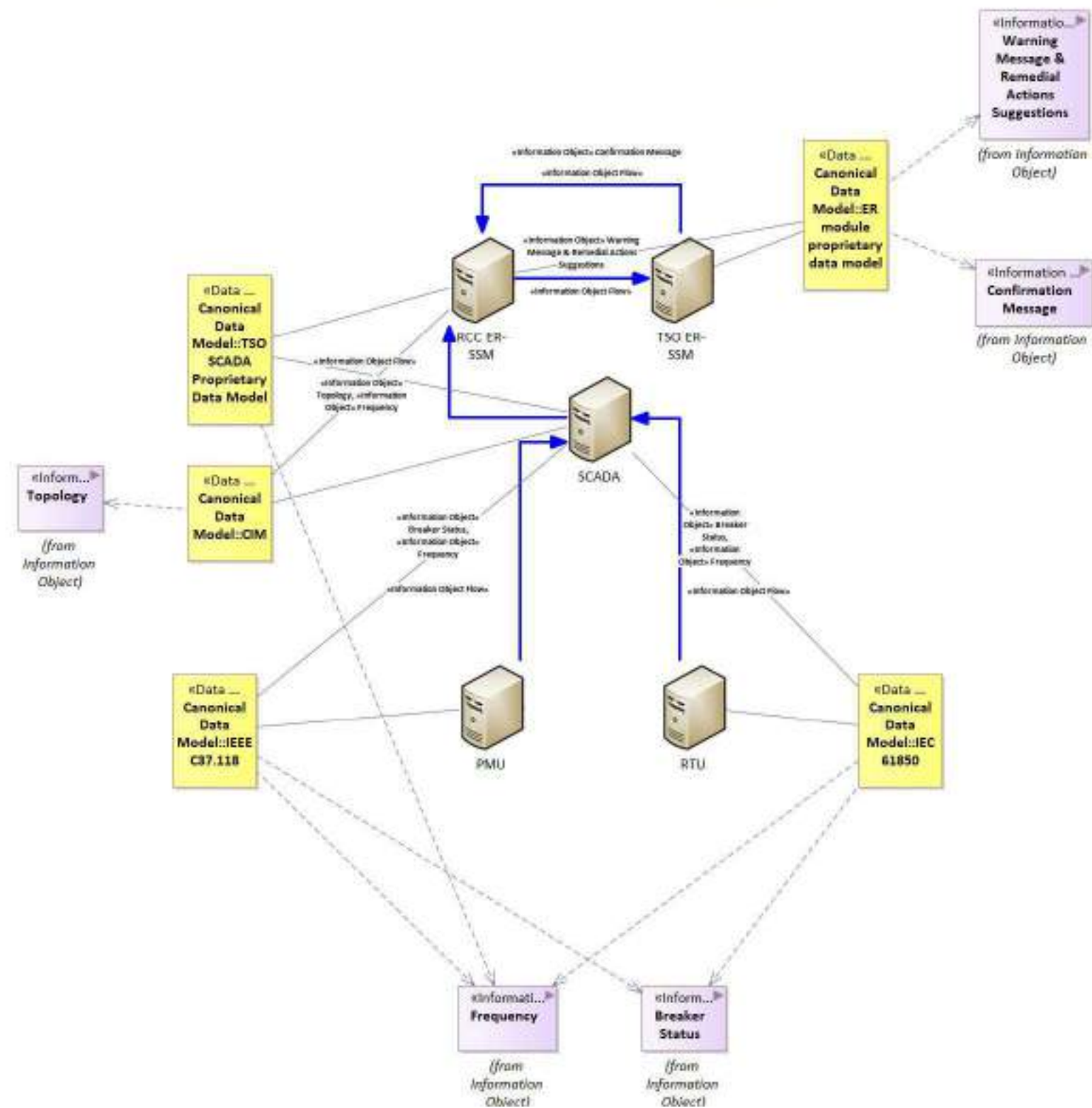


Figure 271 - UC19 Information Object Mapping

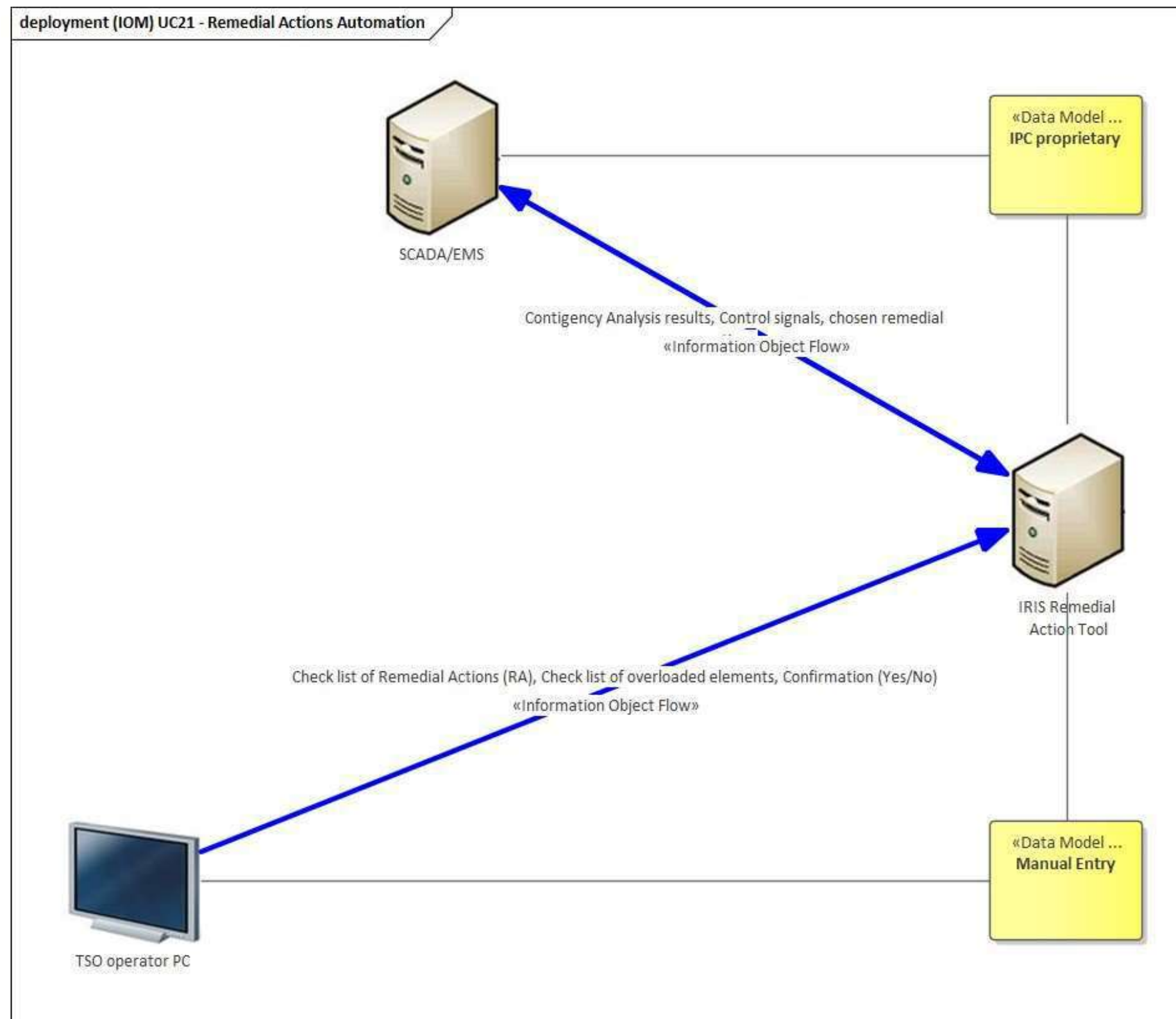
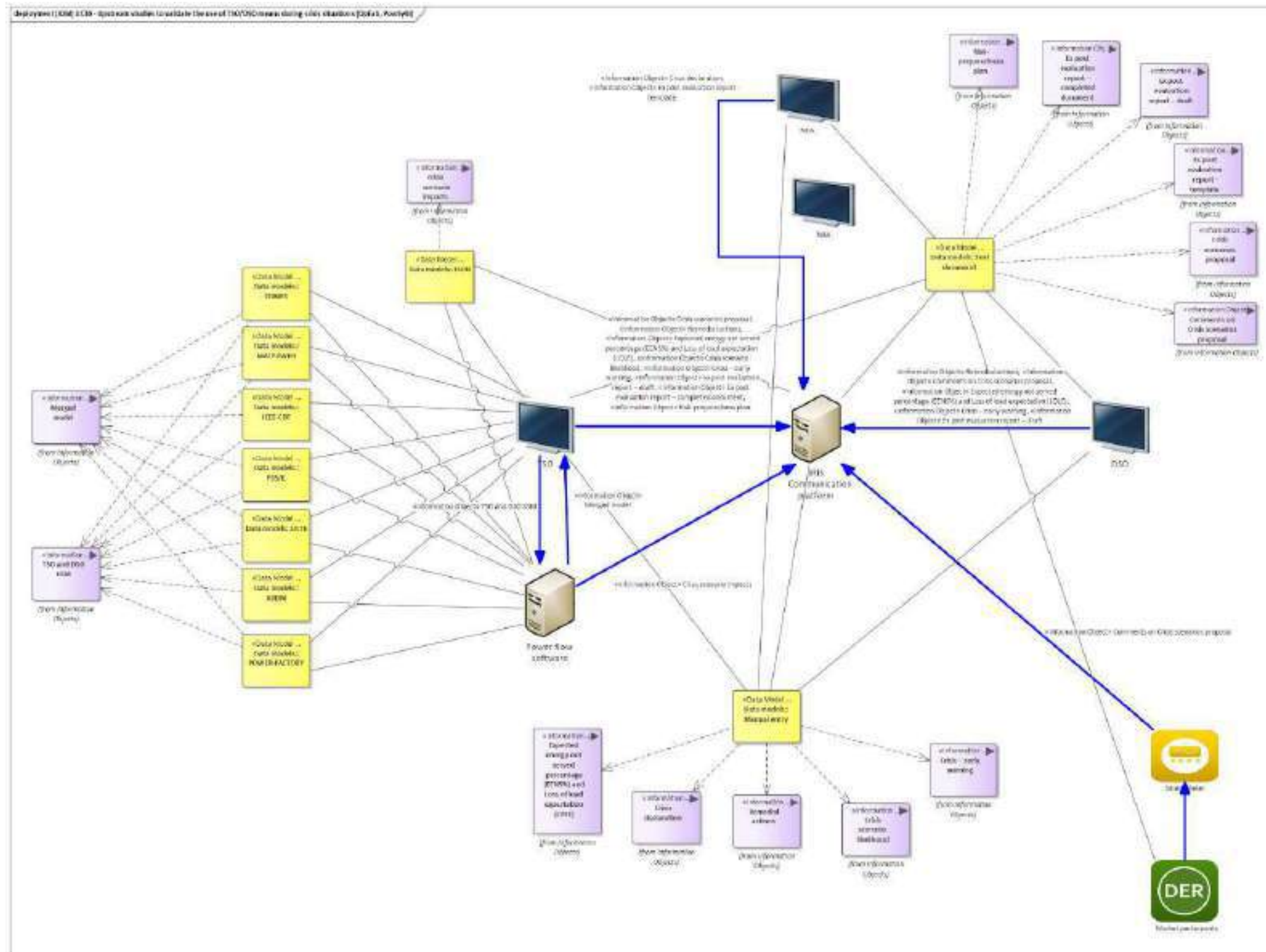


Figure 272 - UC21 Information Object Mapping



13.2.3.3 WP5-PRECOG

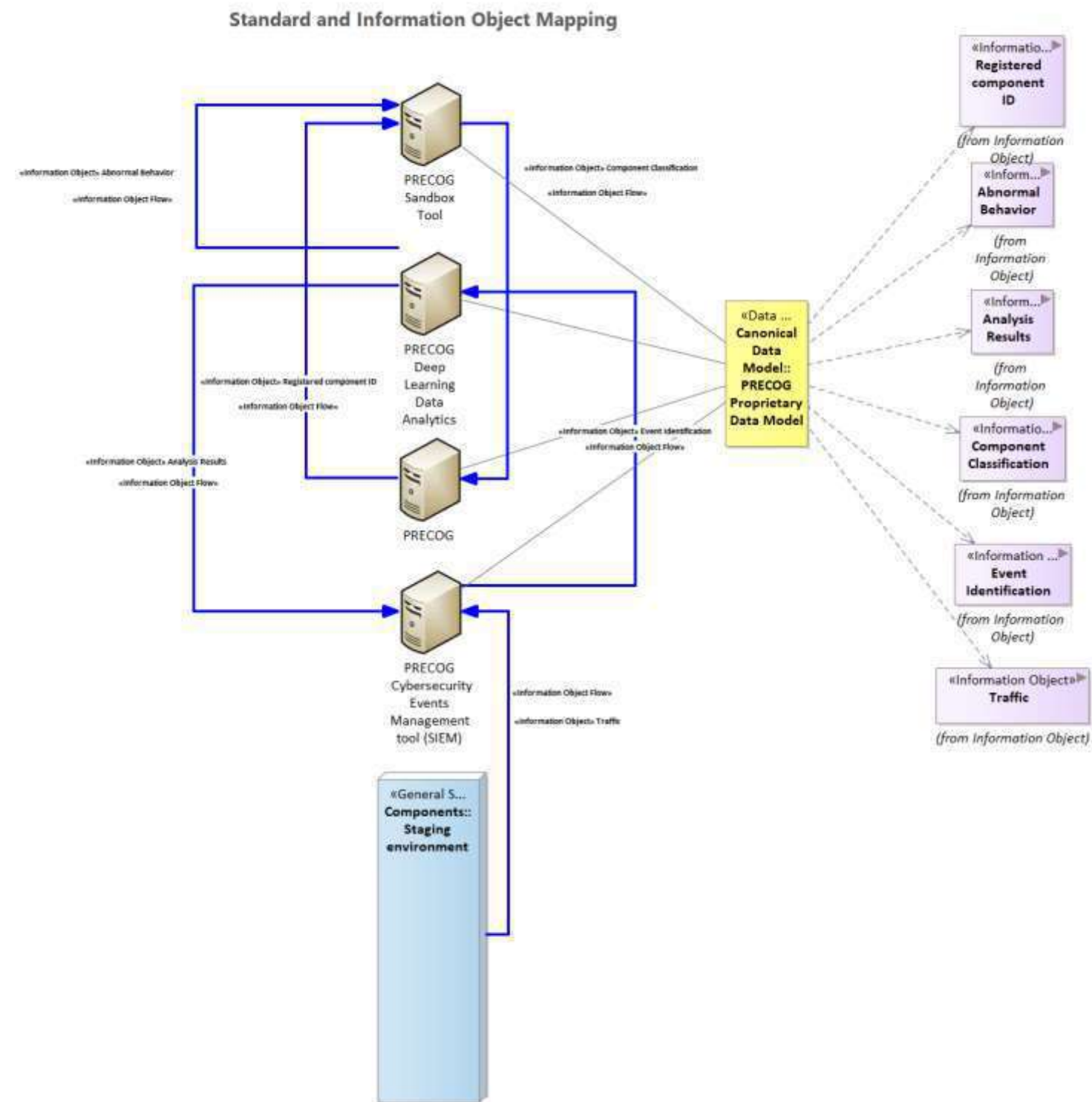


Figure 274 - UC27 Information Object Mapping

Standard and Information Object Mapping

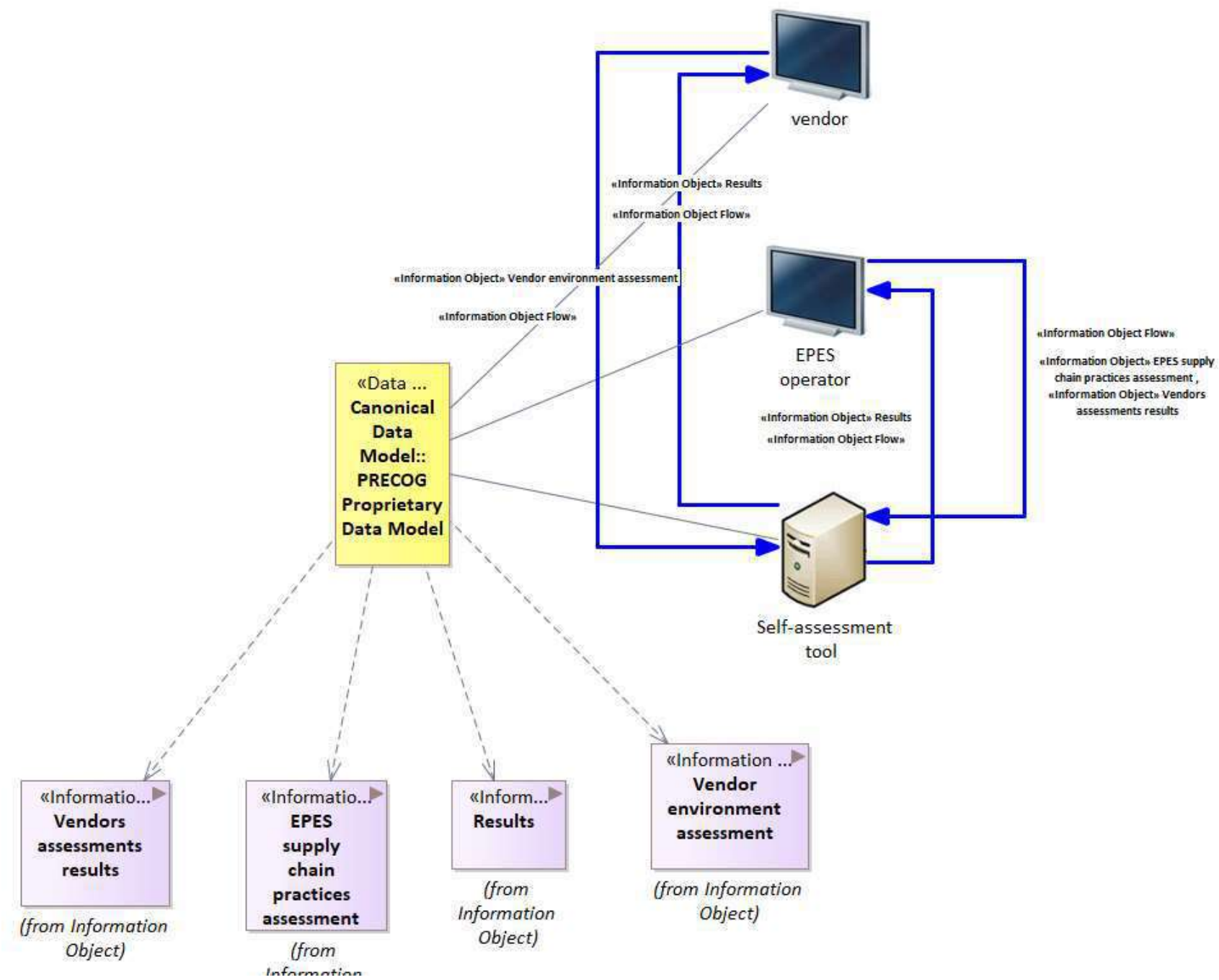


Figure 275 - UC28 Information Object Mapping

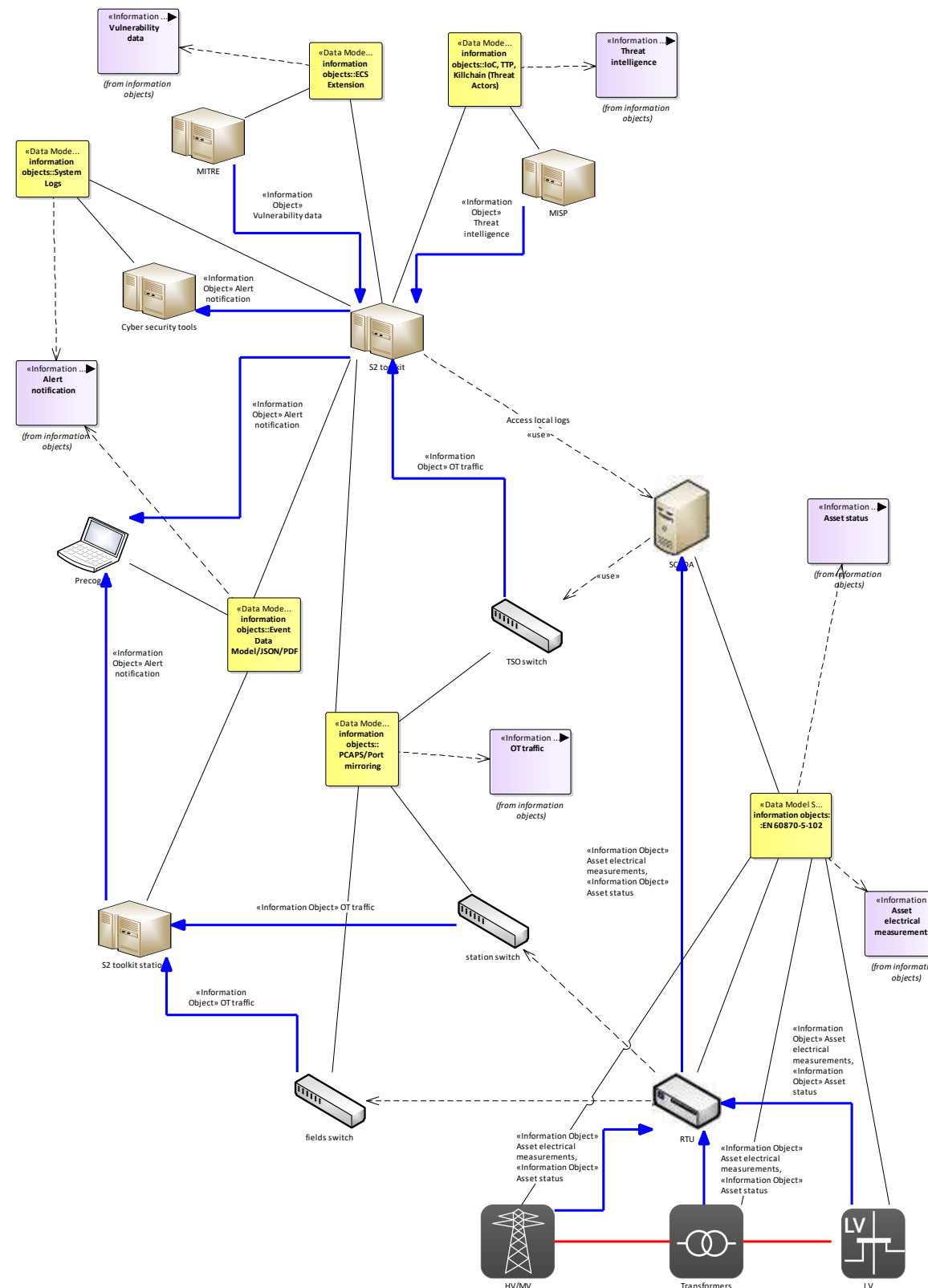


Figure 276 - UC33 Information Object Mapping

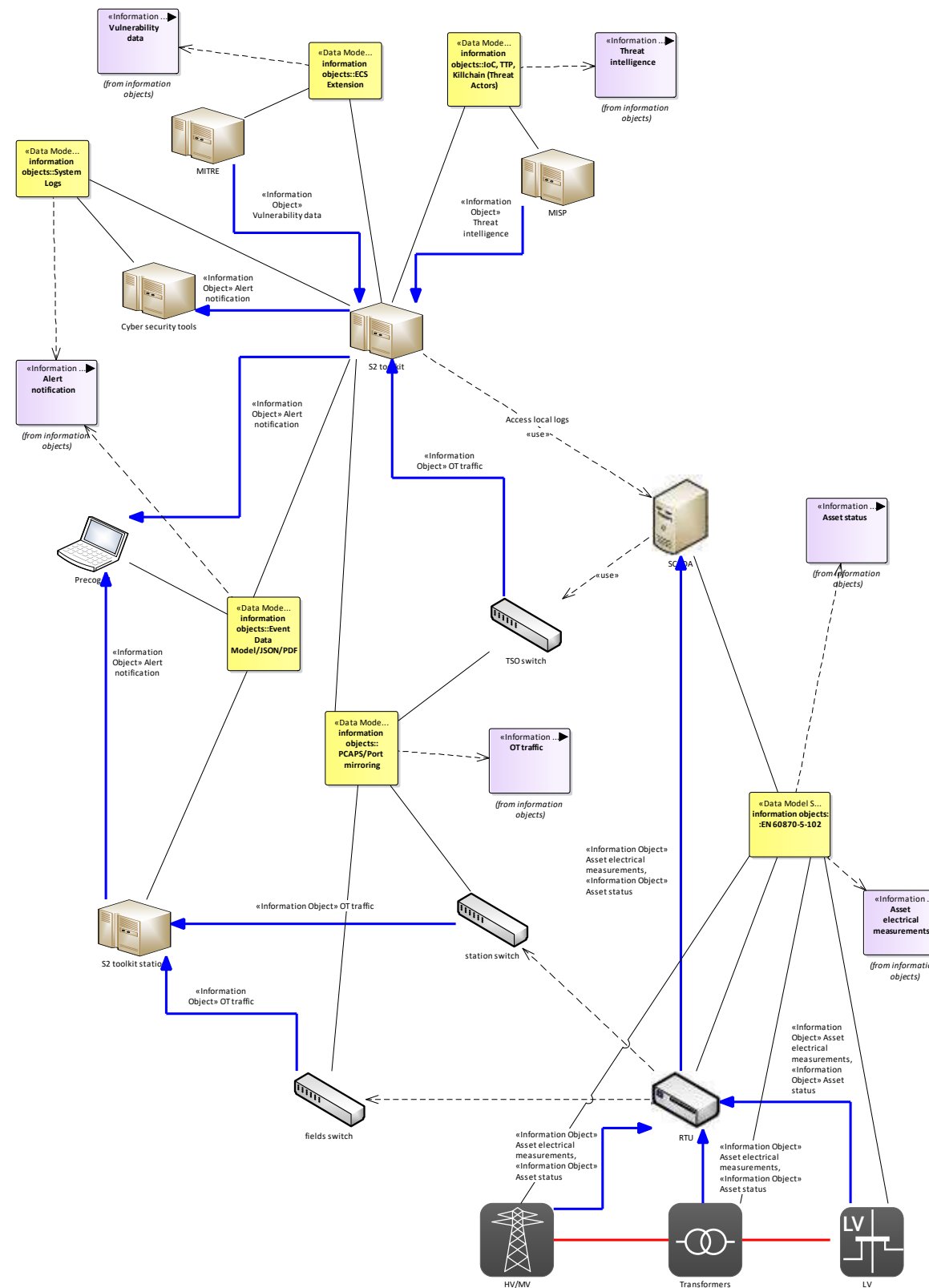


Figure 277 - UC34 Information Object Mapping

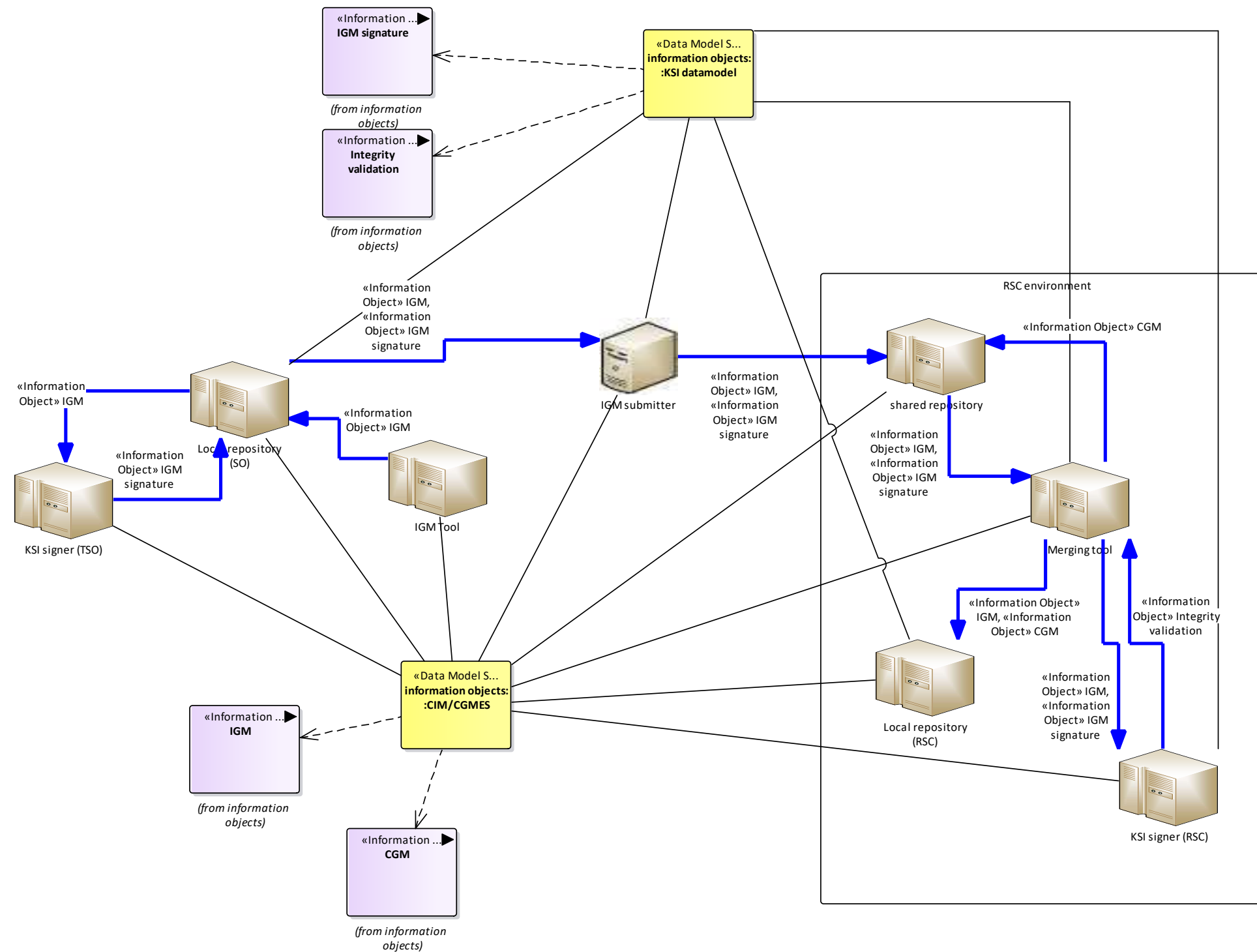


Figure 278 - UC36 Information Object Mapping

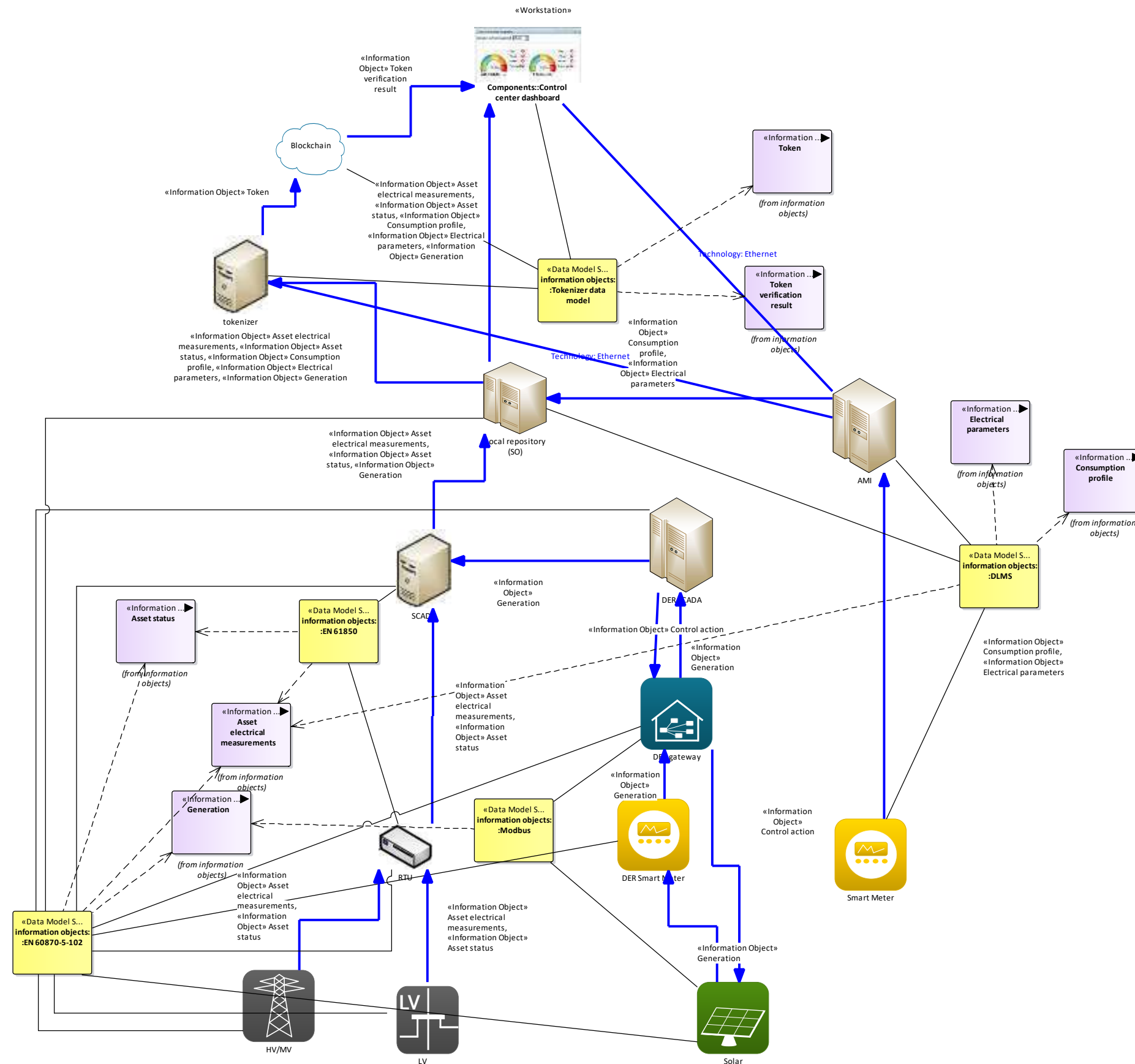
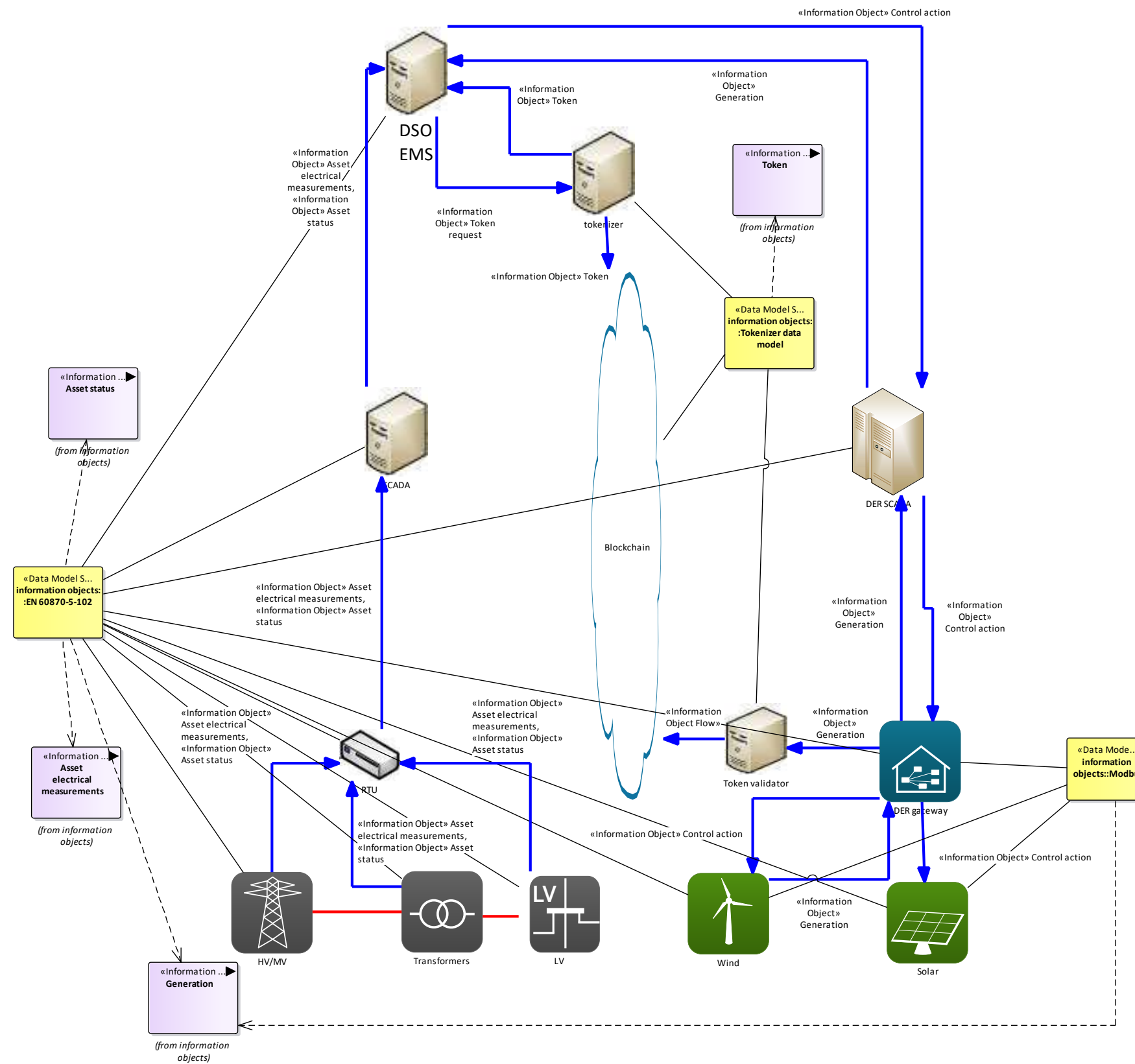


Figure 279 - UC37 Information Object Mapping



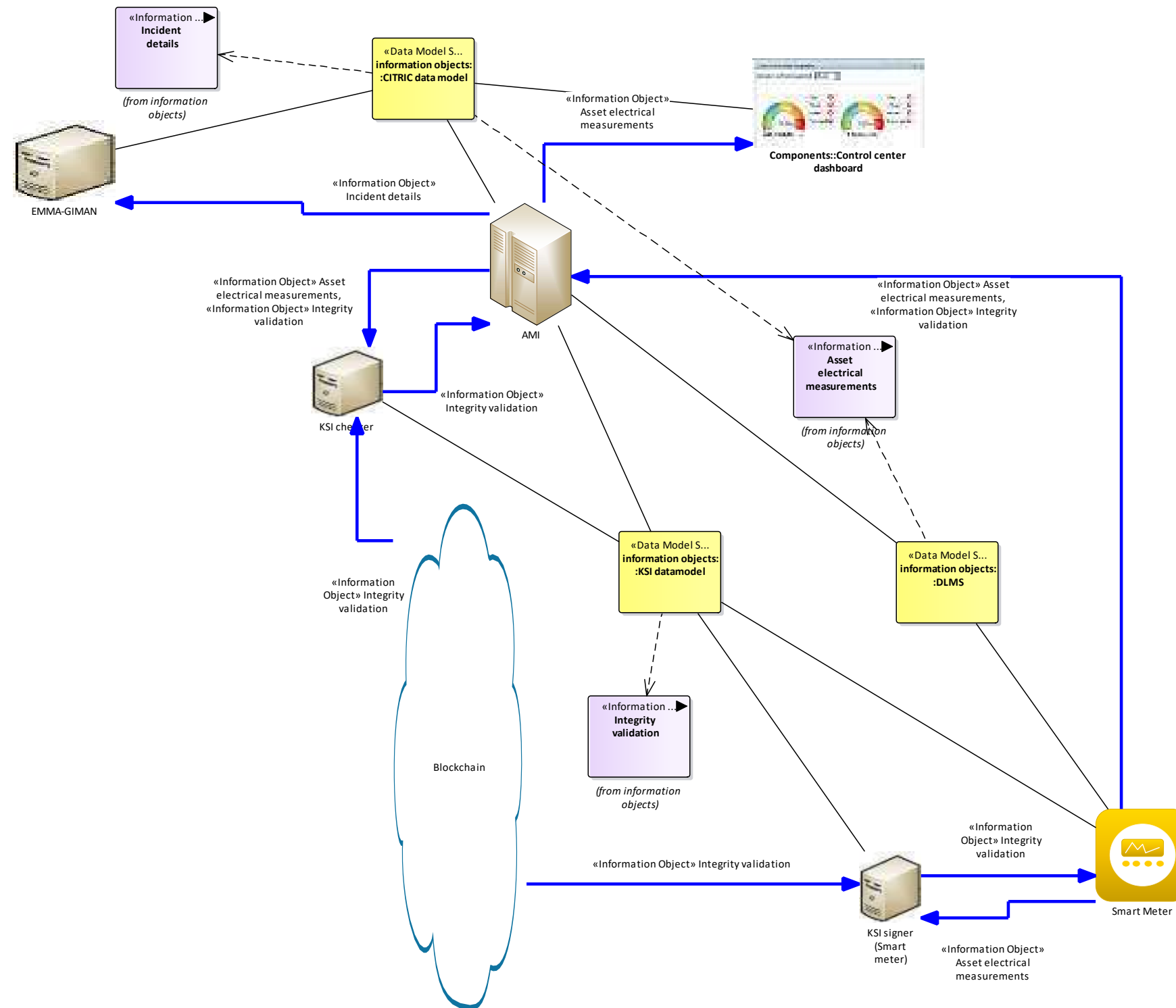


Figure 281 - UC40 Information Object Mapping



13.2.3.4 WP6-EMMA

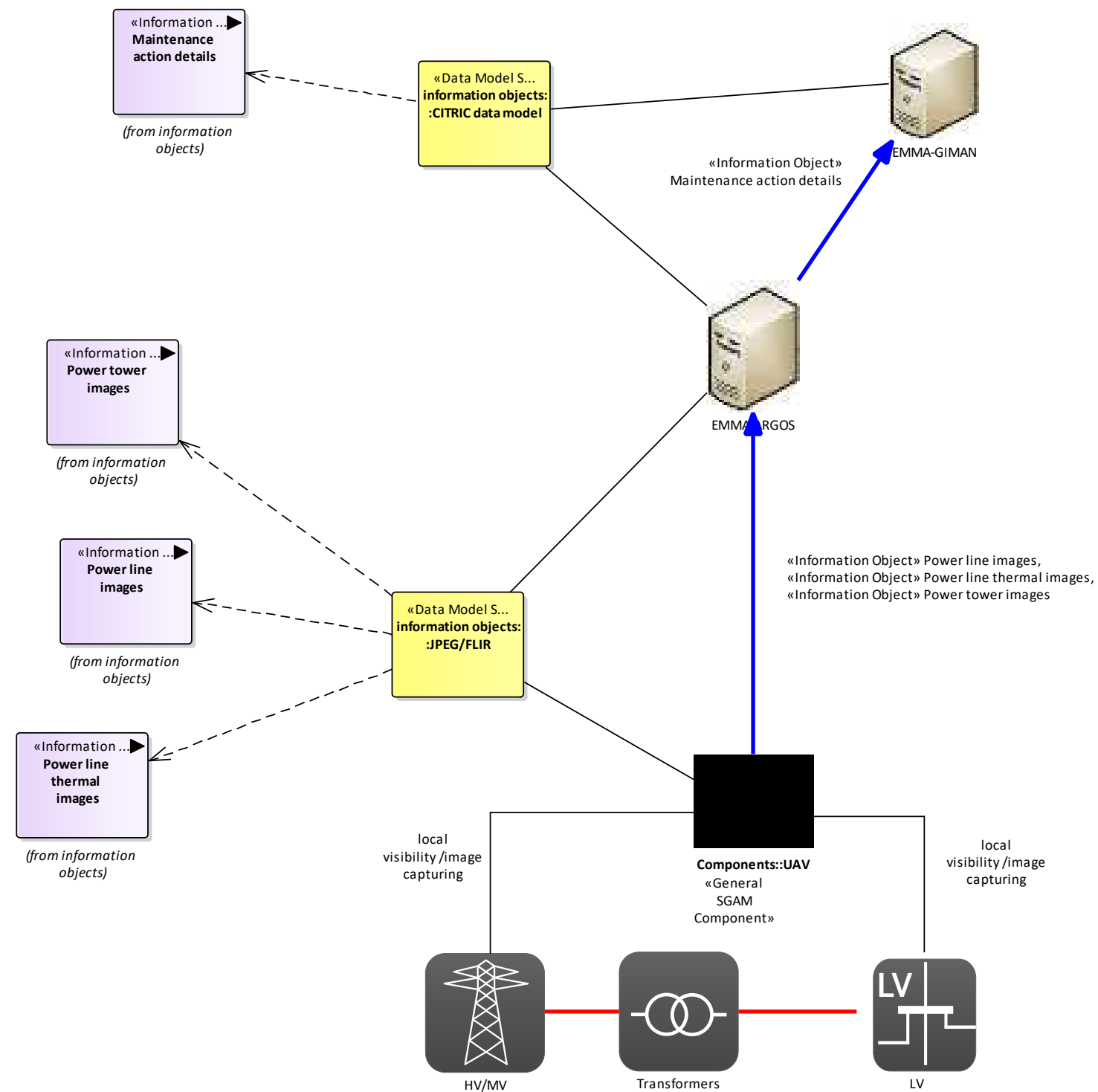


Figure 282 – UC01 Information Object Mapping

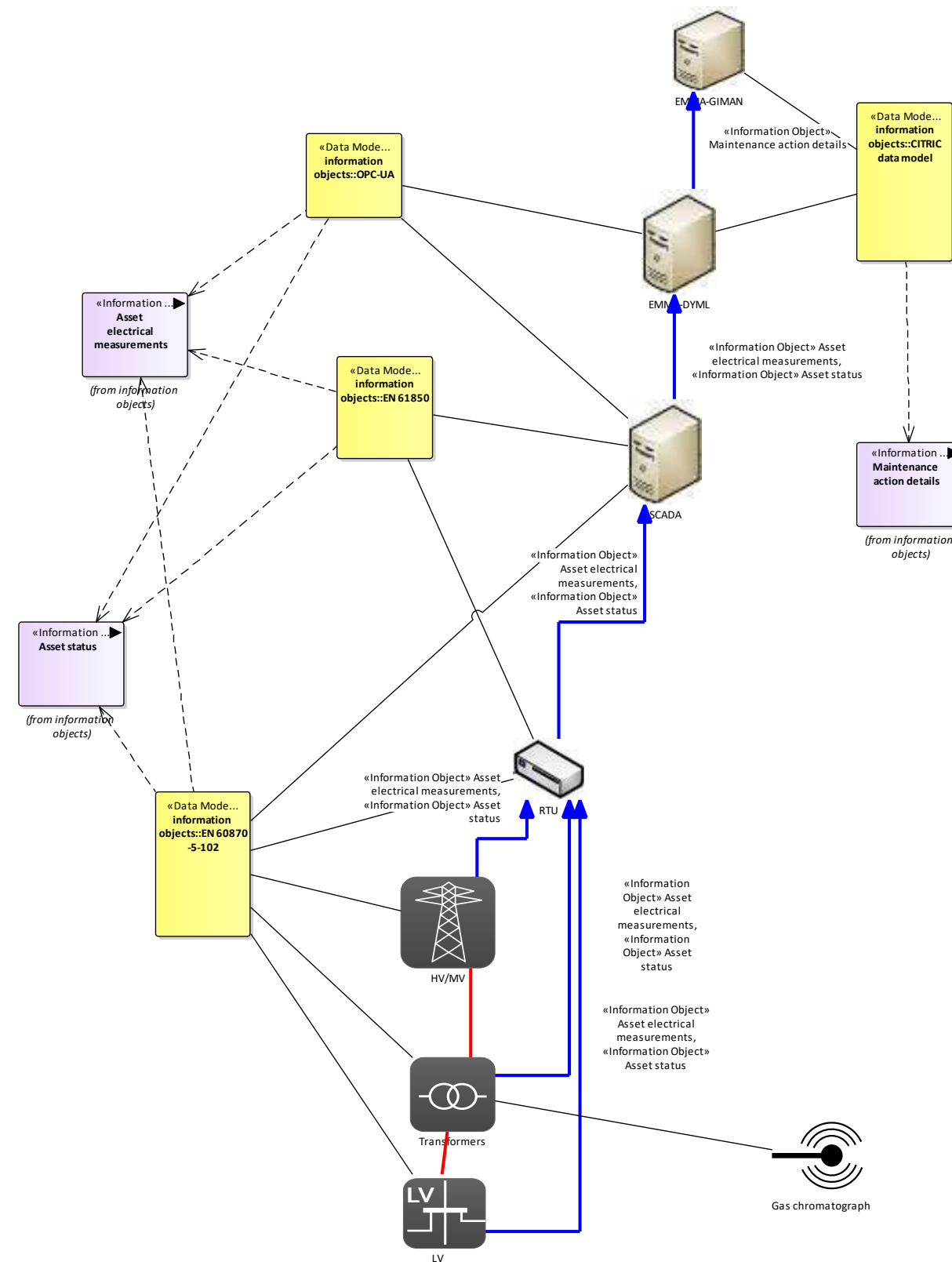


Figure 283 - UC02 Information Object Mapping

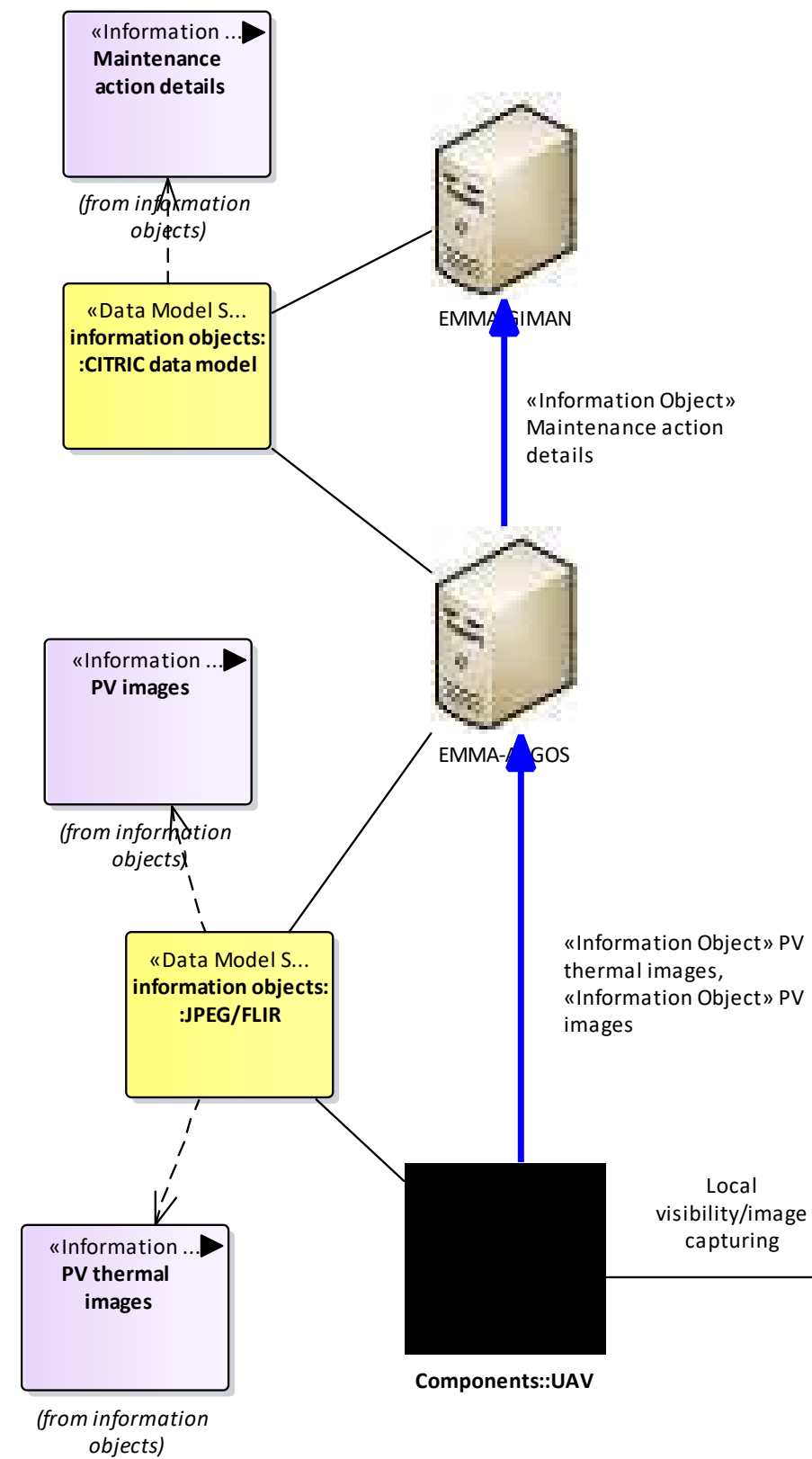


Figure 284 - UC03 Information Object Mapping

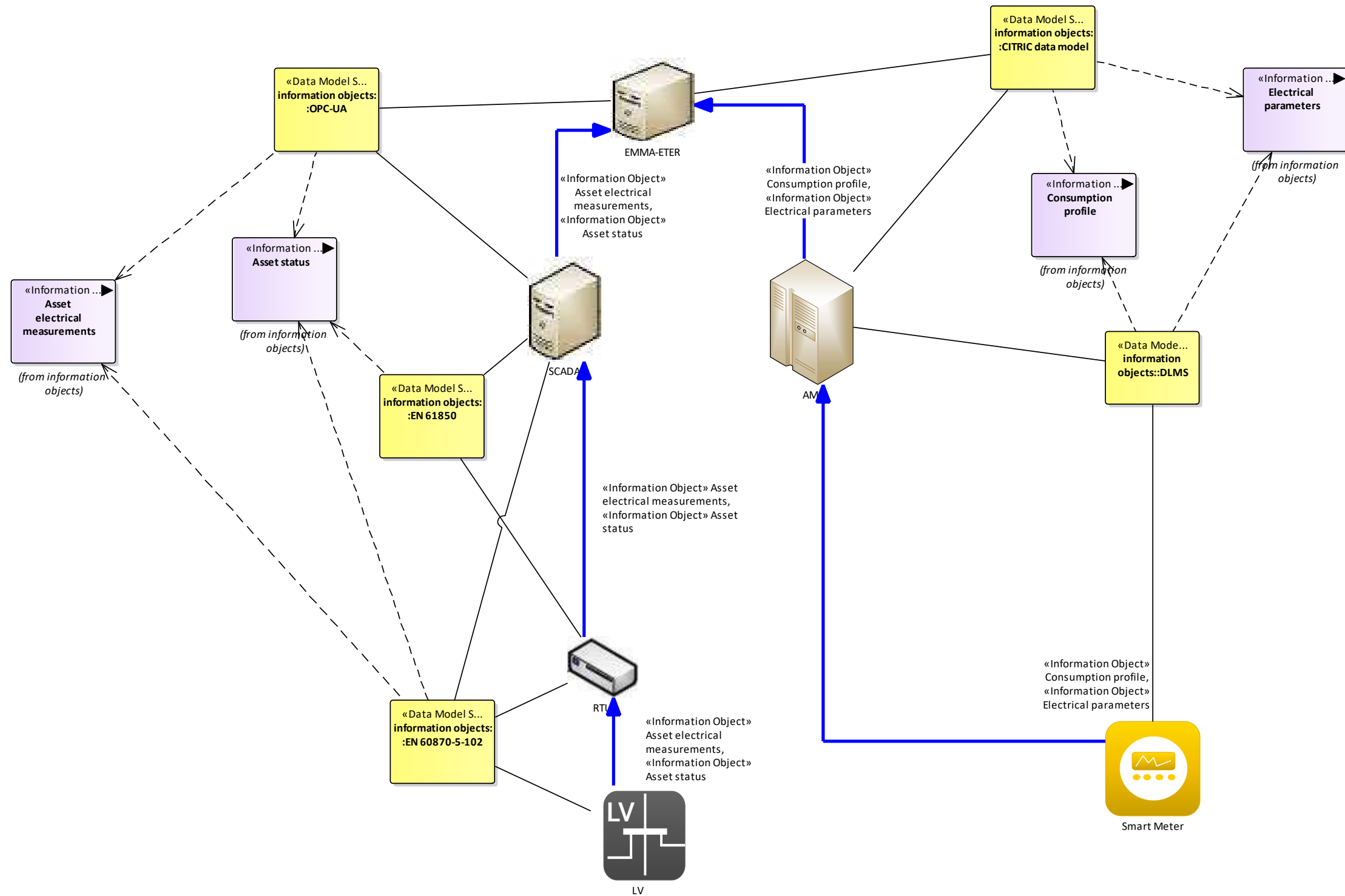


Figure 285 - UC04 Information Object Mapping

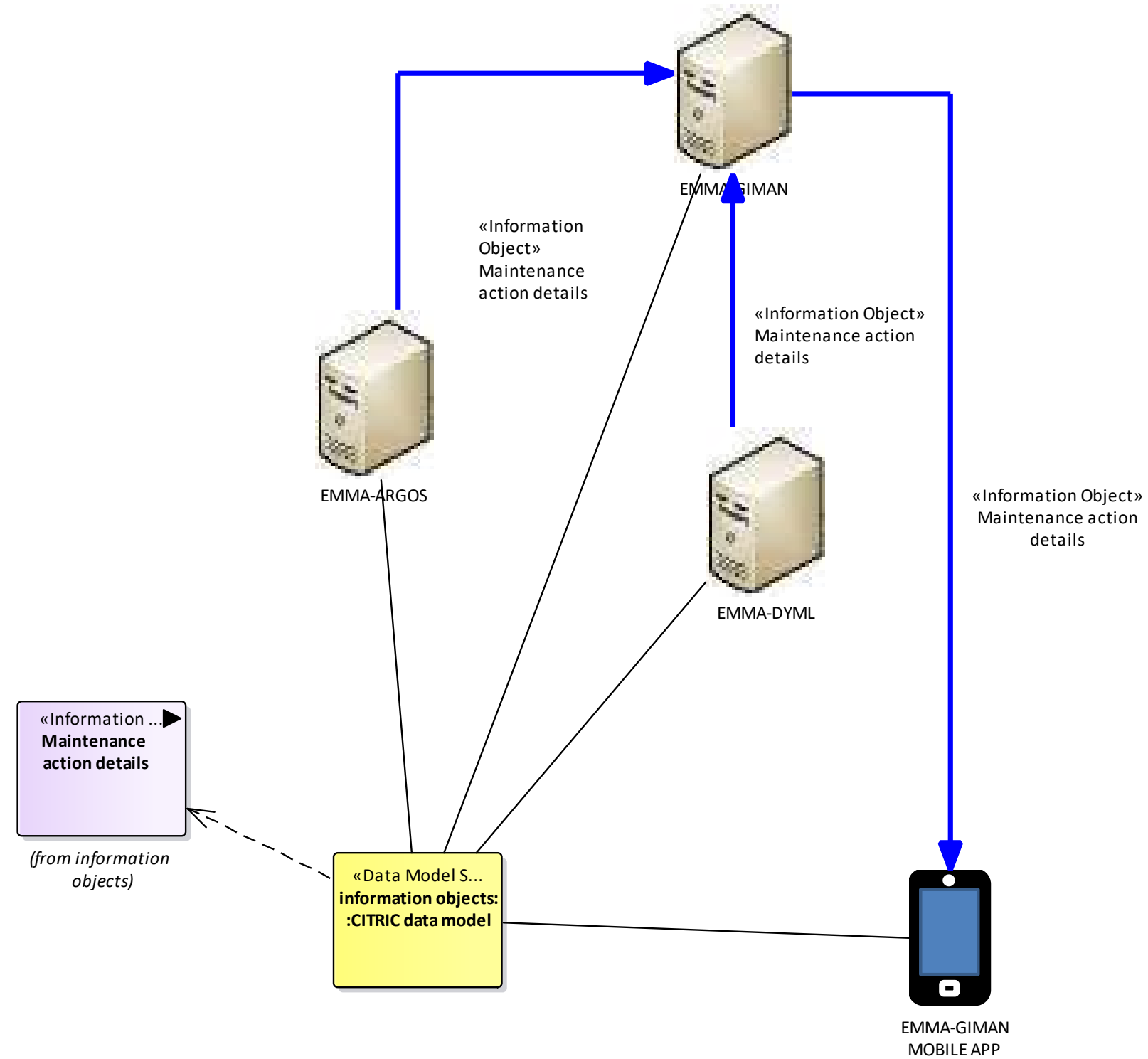
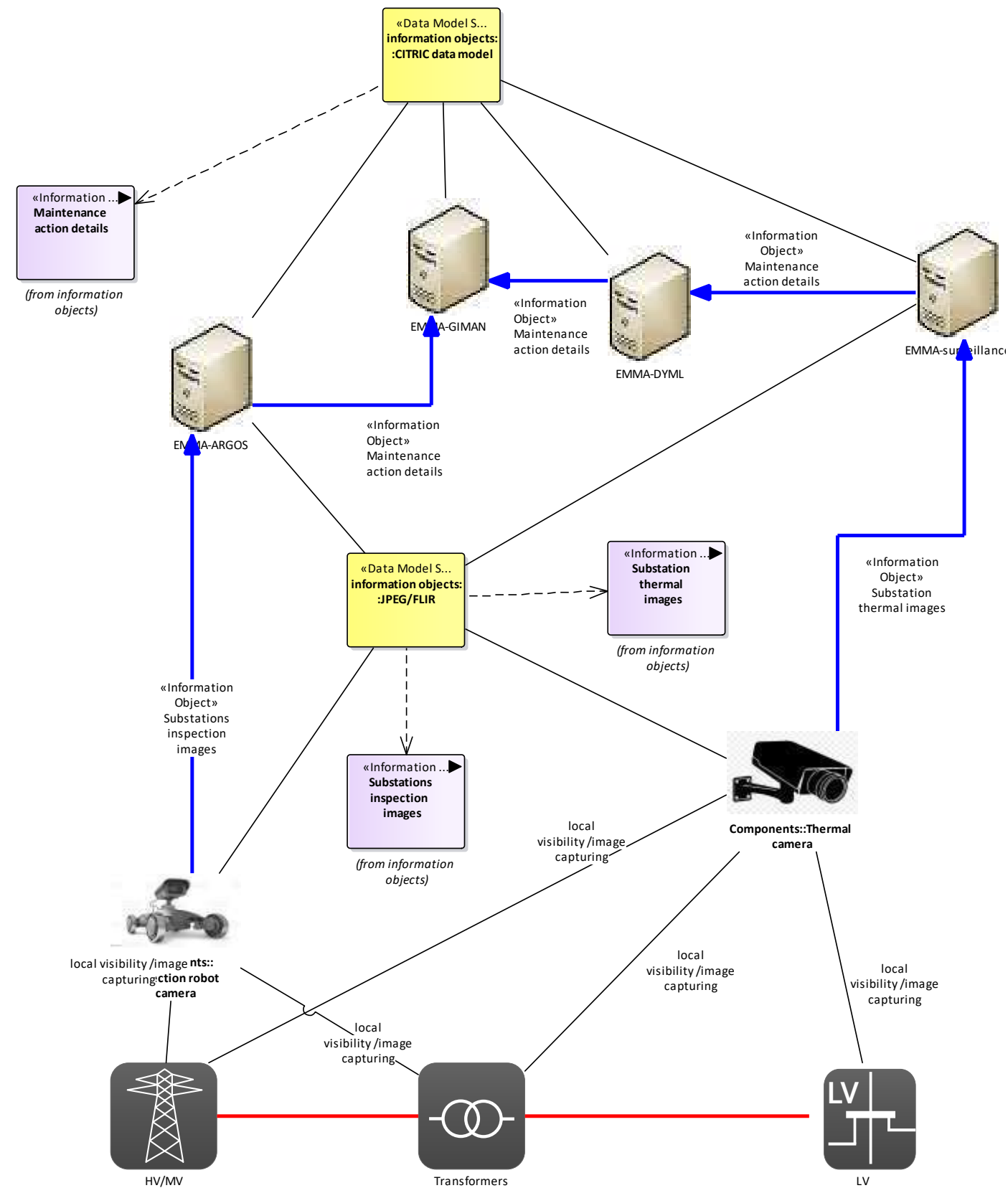


Figure 286 - UC05 Information Object Mapping



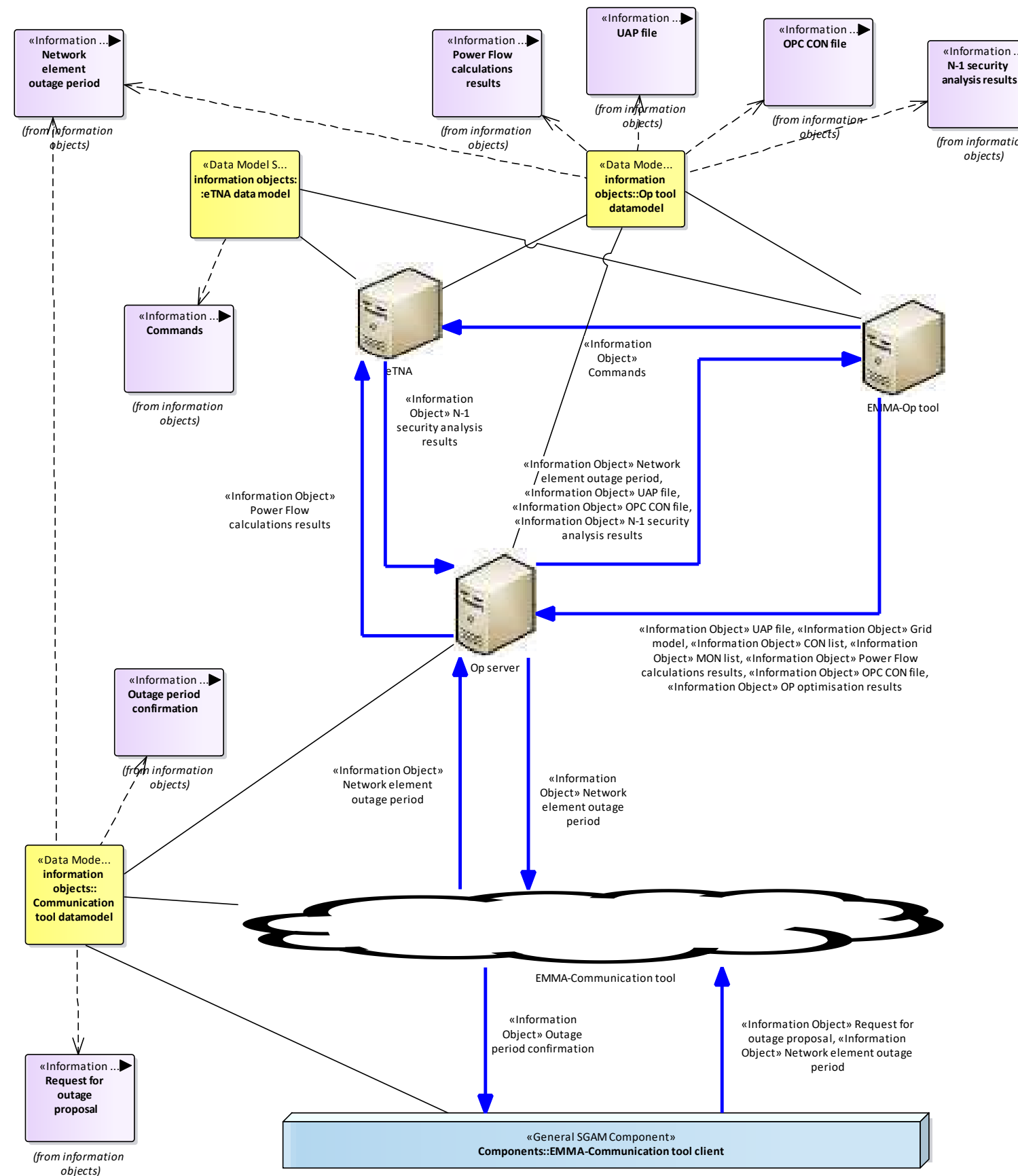


Figure 288 - UC08 Information Object Mapping

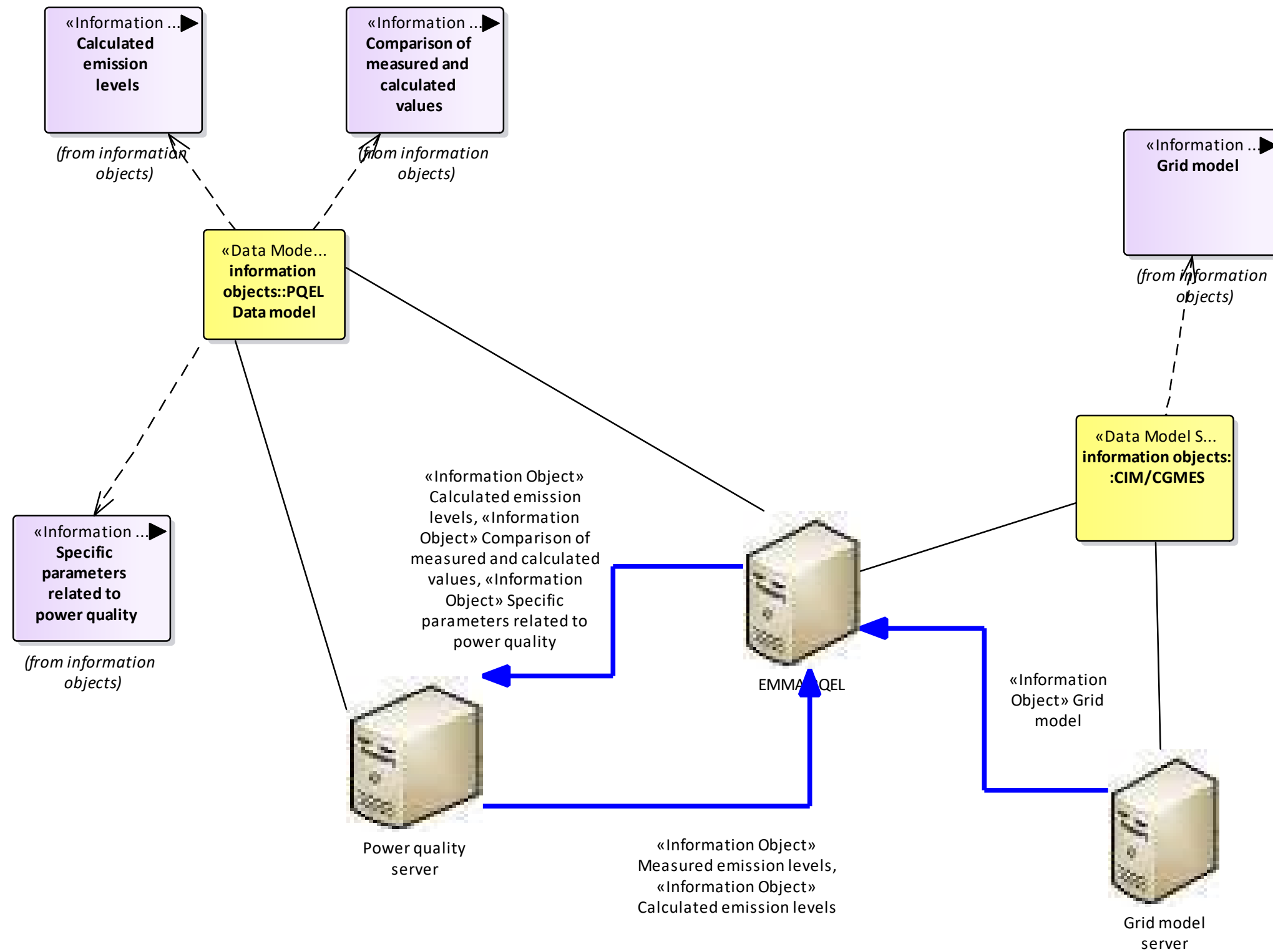


Figure 289 - UC09 Information Object Mapping

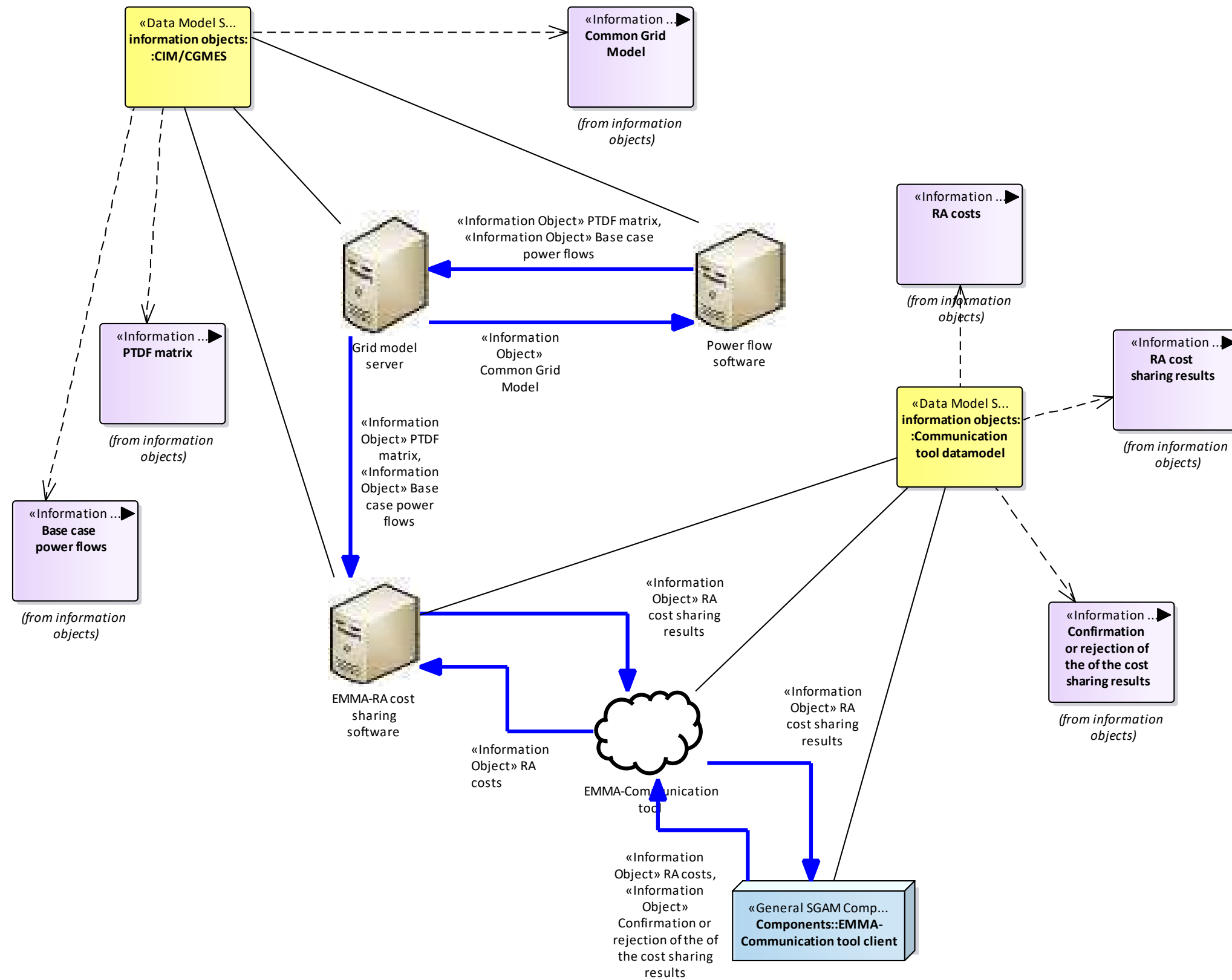


Figure 290 - UC13 Information Object Mapping

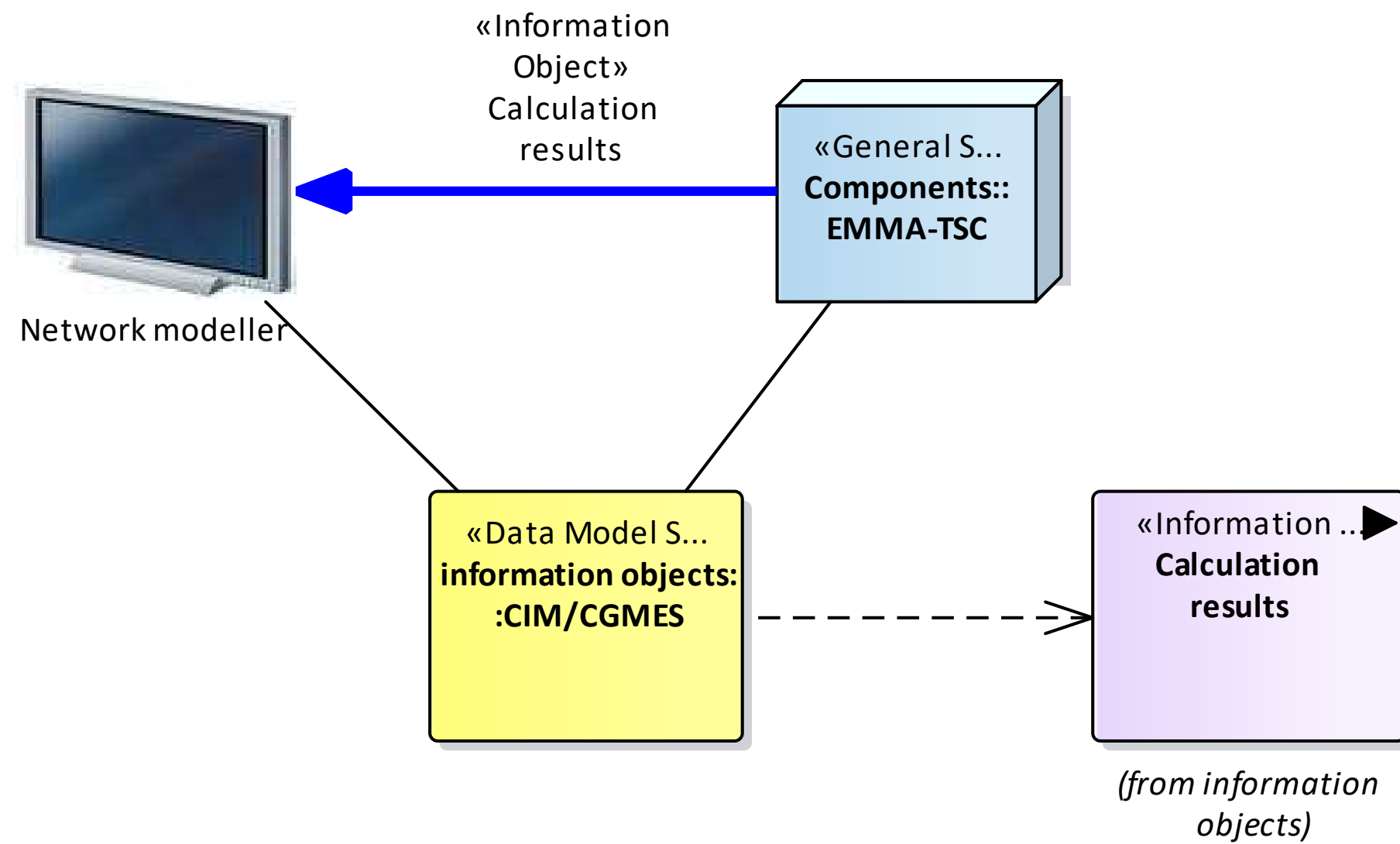


Figure 291 - UC14 Information Object Mapping

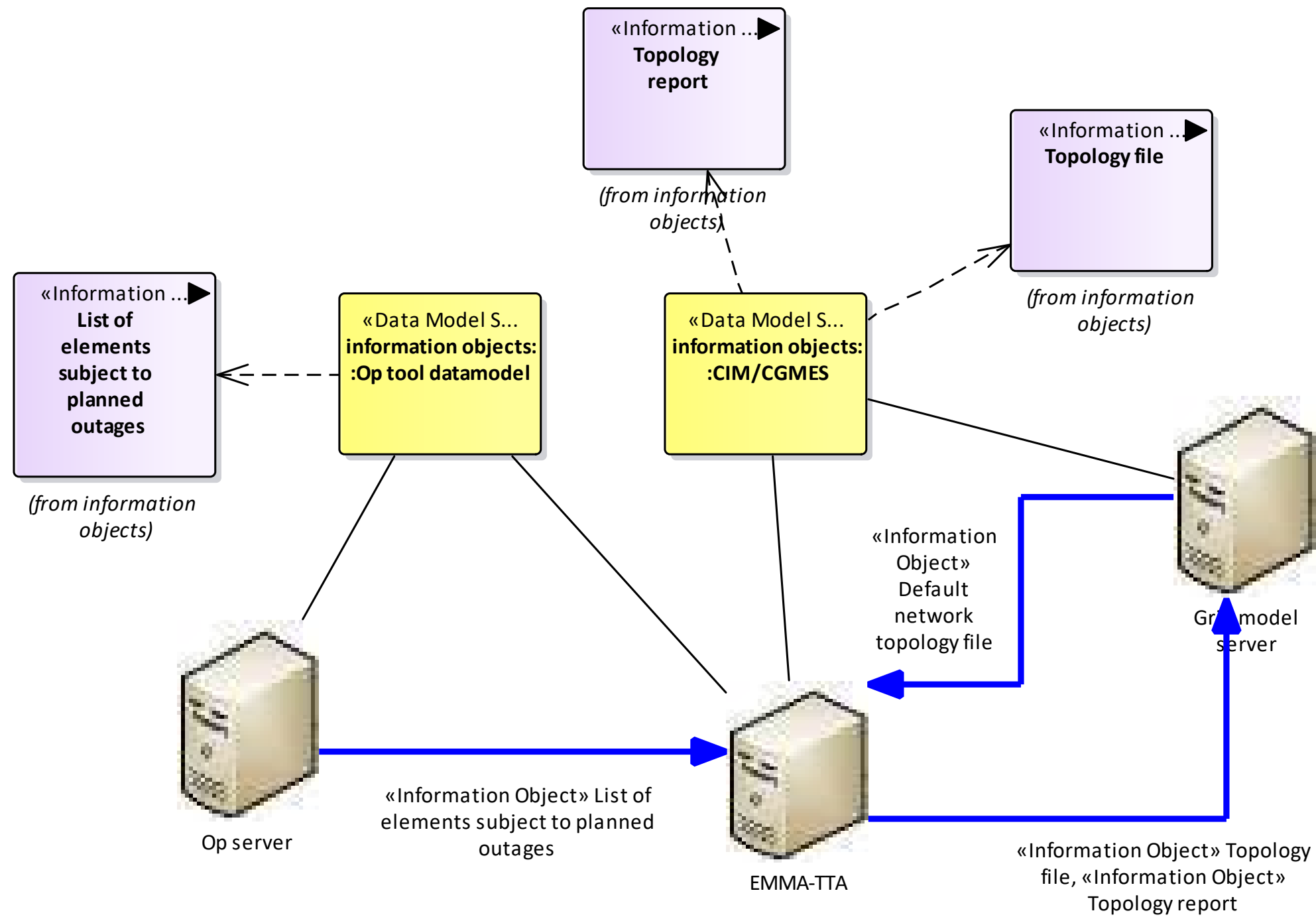


Figure 292 - UC17 Information Object Mapping



D2.3 - Requirements and Detailed Architecture Design

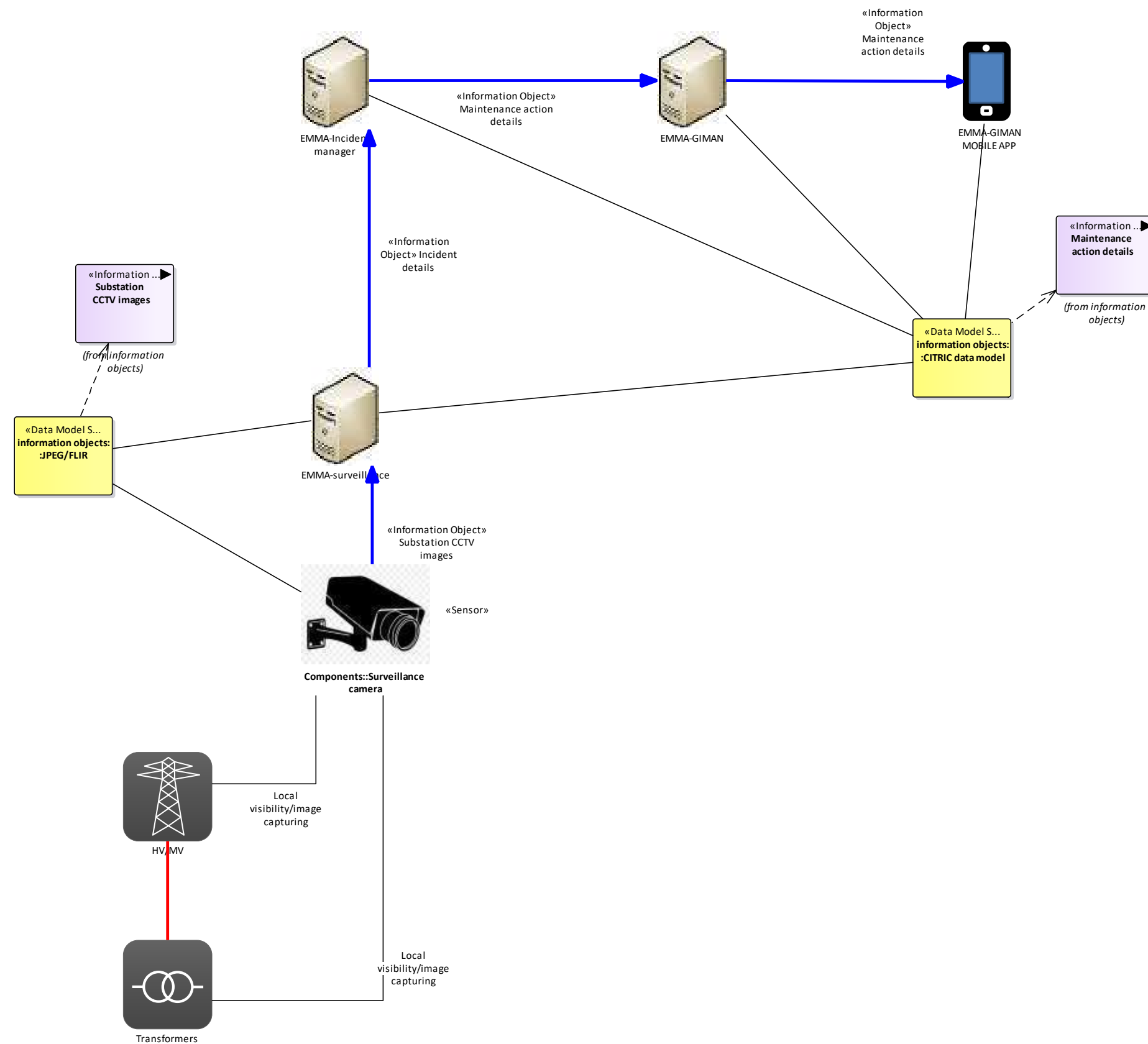


Figure 293 - UC20 Information Object Mapping

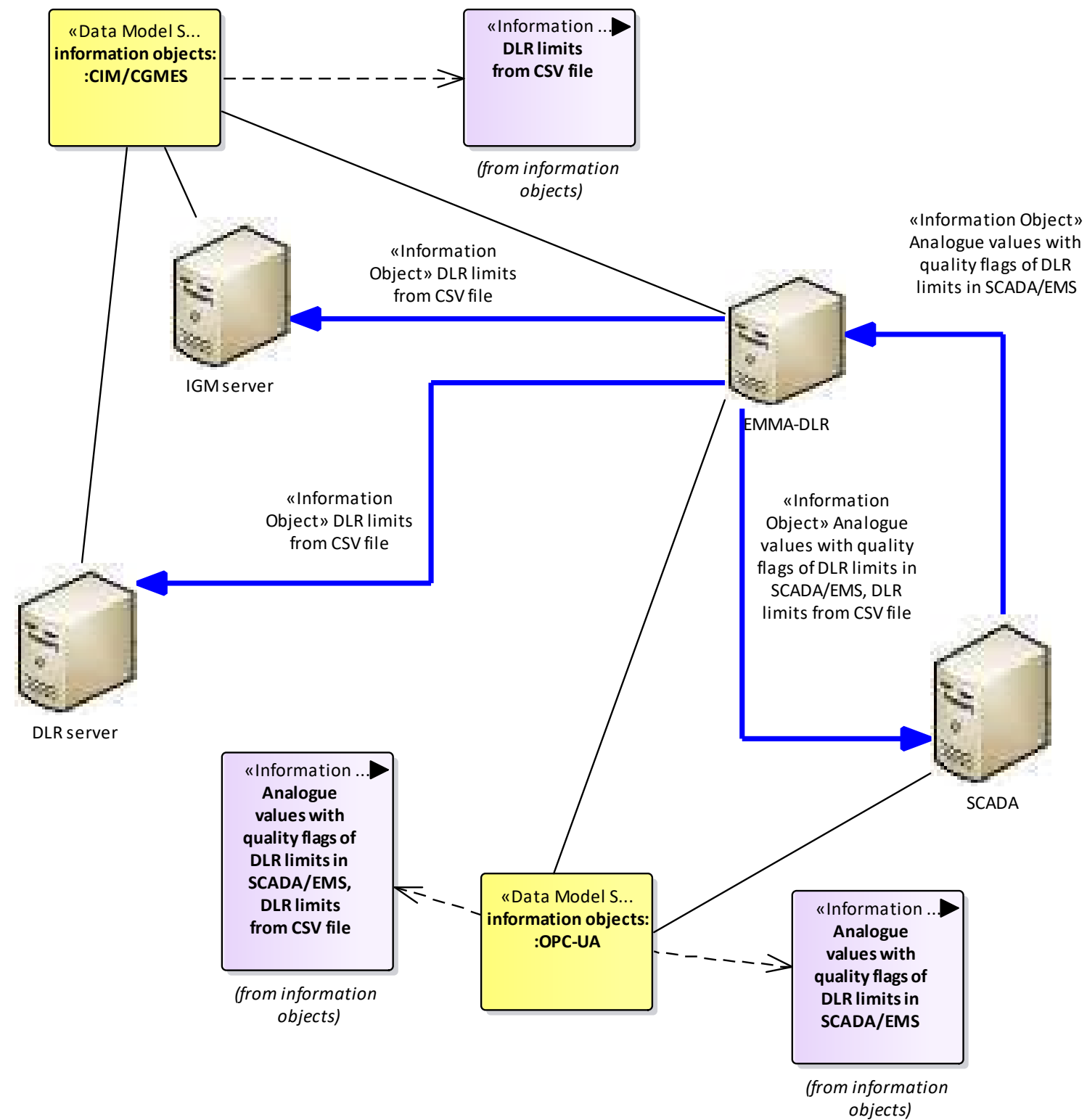


Figure 294 - UC31 Information Object Mapping

13.3 SGAM COMMUNICATION LAYER

13.3.1 WP3-C3P0

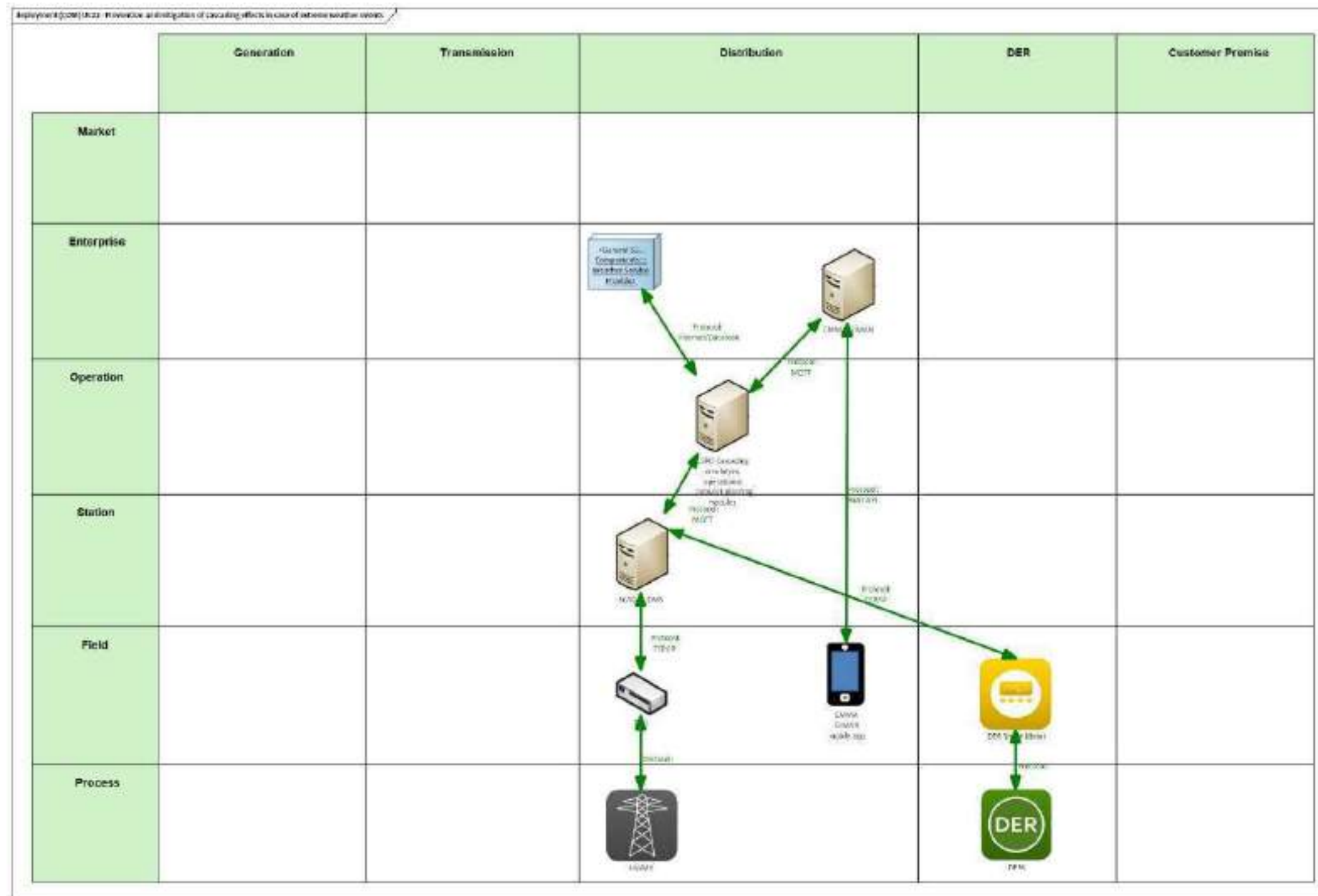


Figure 295 - UC22 Communication Layer

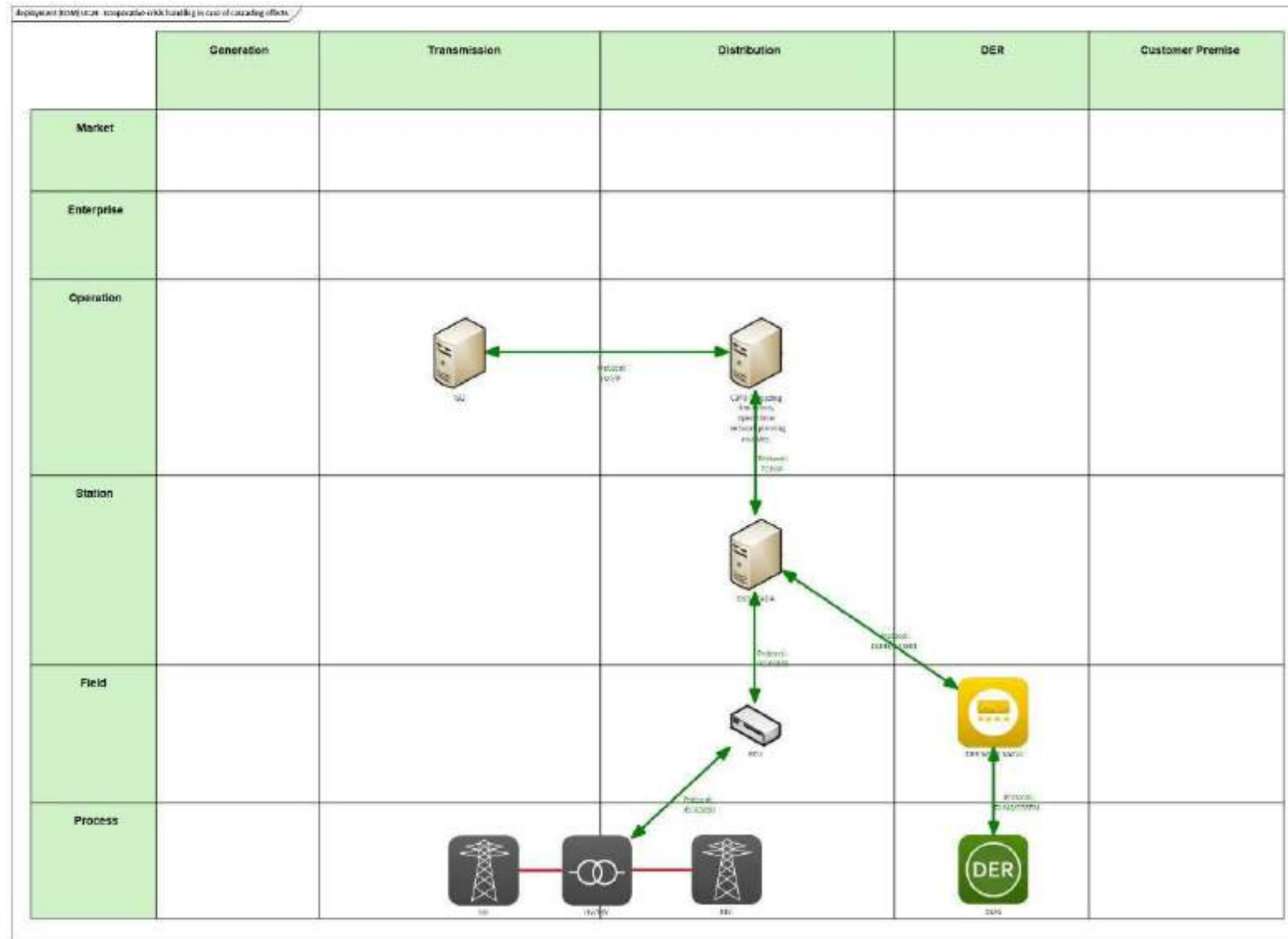


Figure 296 - UC23 Communication Layer

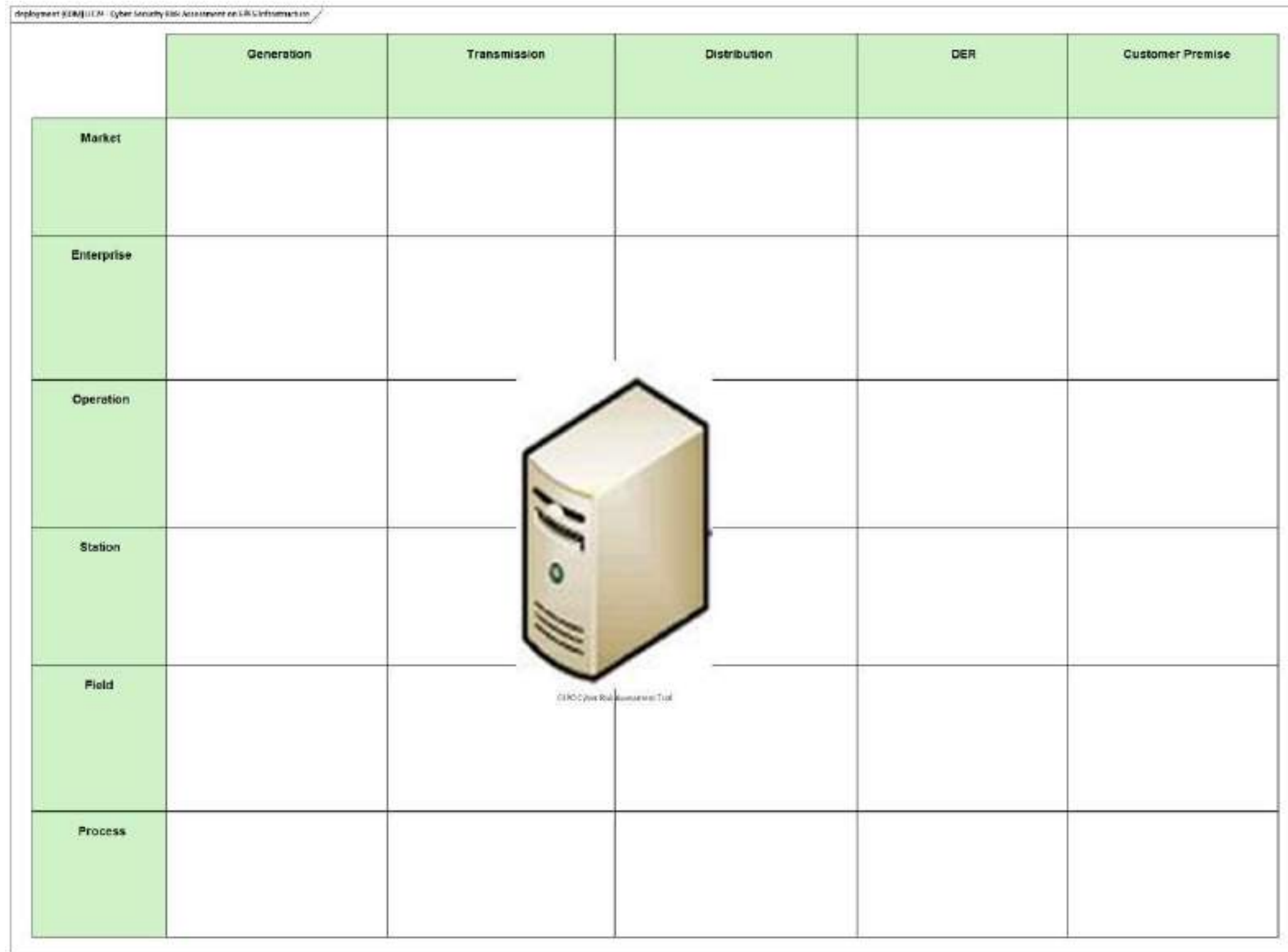


Figure 297 - UC24 Communication Layer

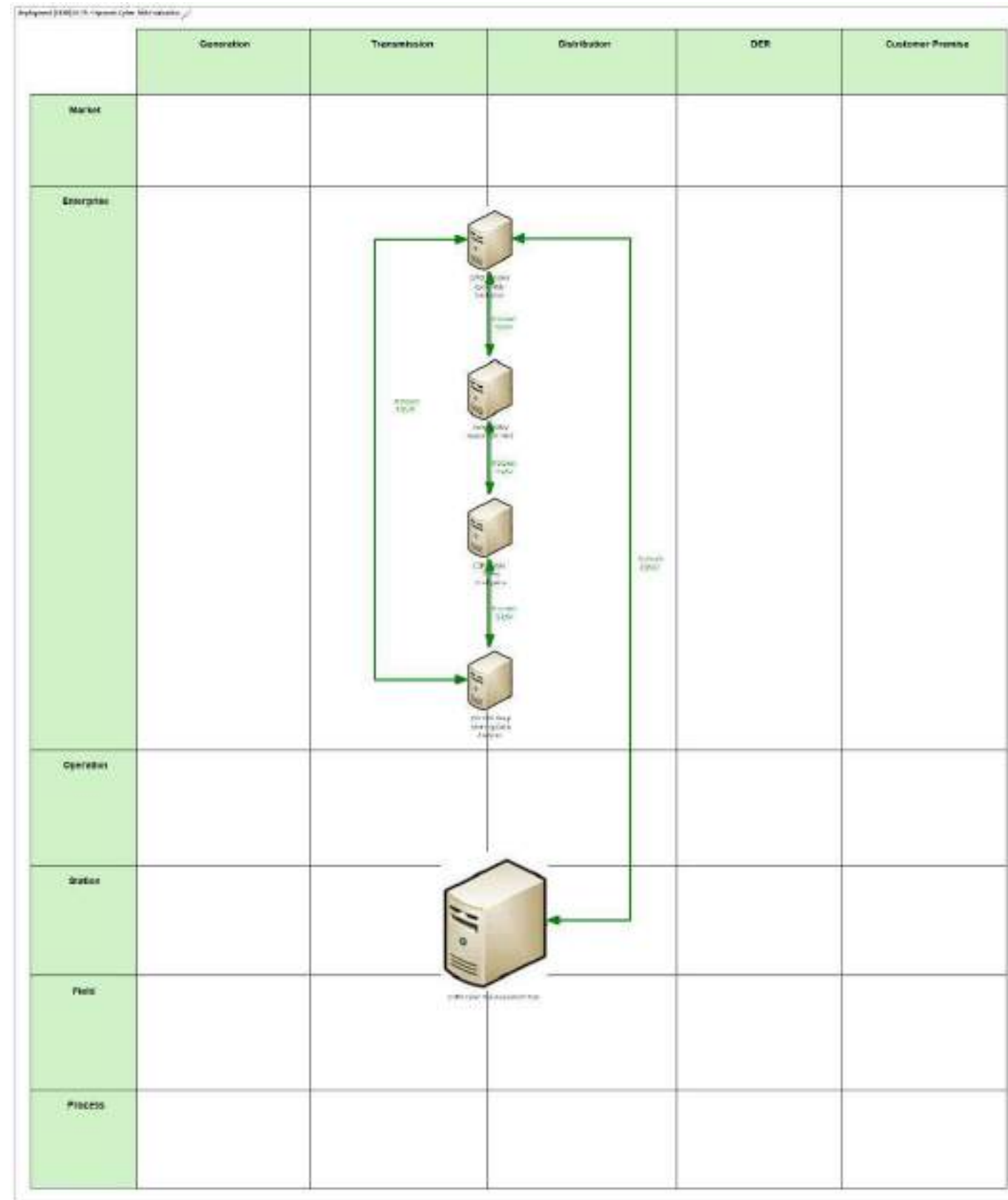


Figure 298 - UC25 Communication Layer

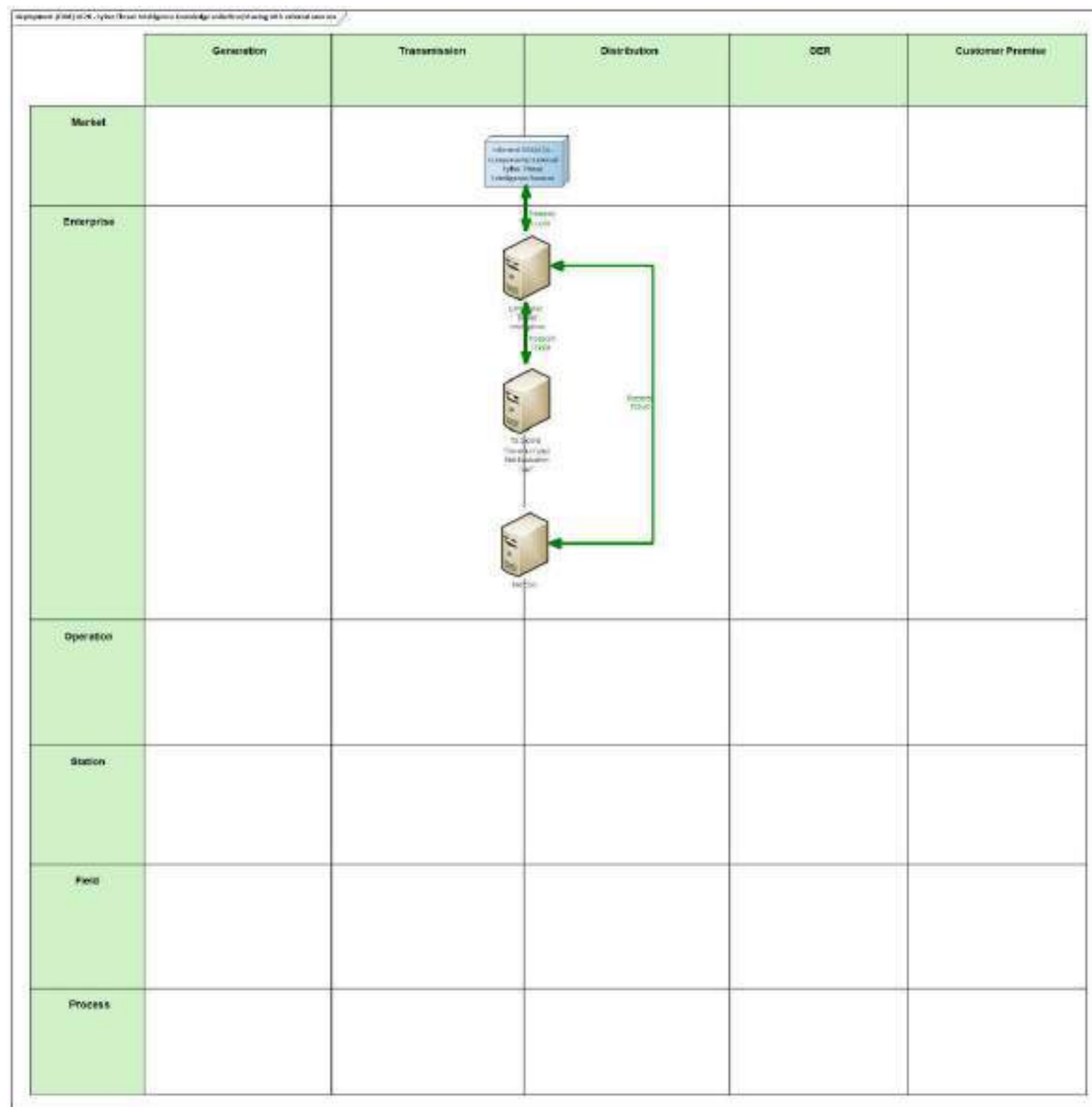


Figure 299 - UC26 Communication Layer

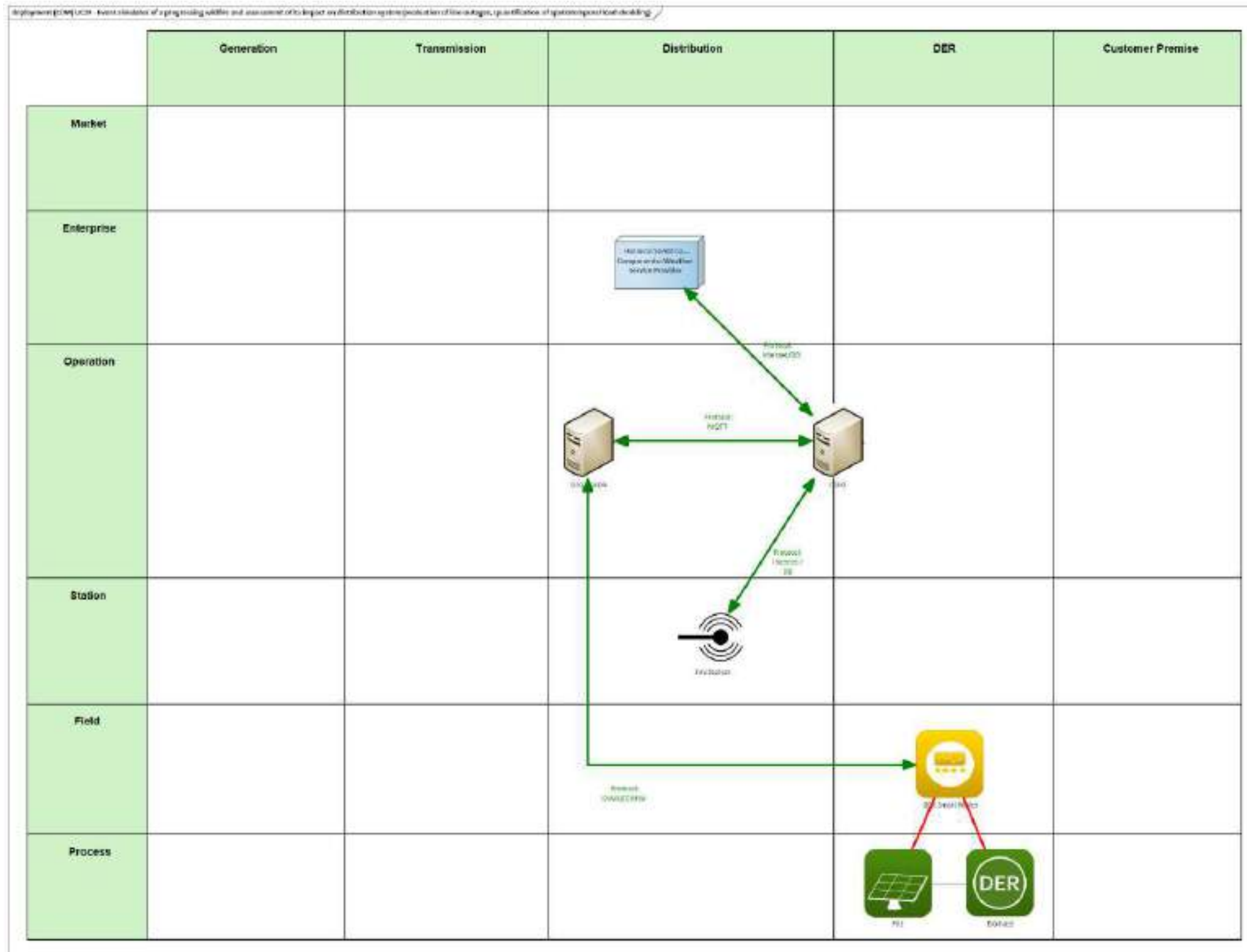


Figure 300 - UC29 Communication Layer

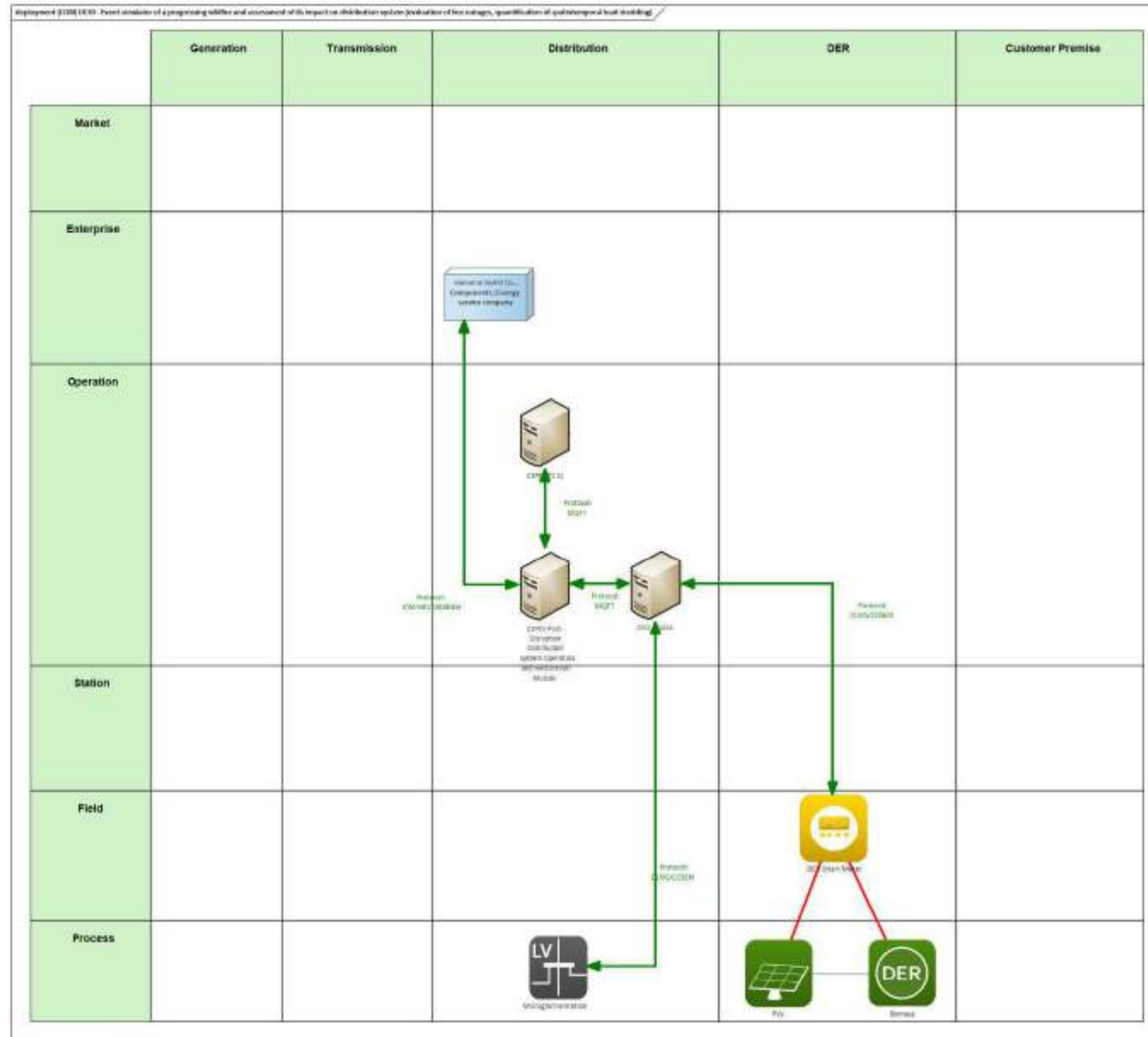


Figure 301 - UC30 Communication Layer

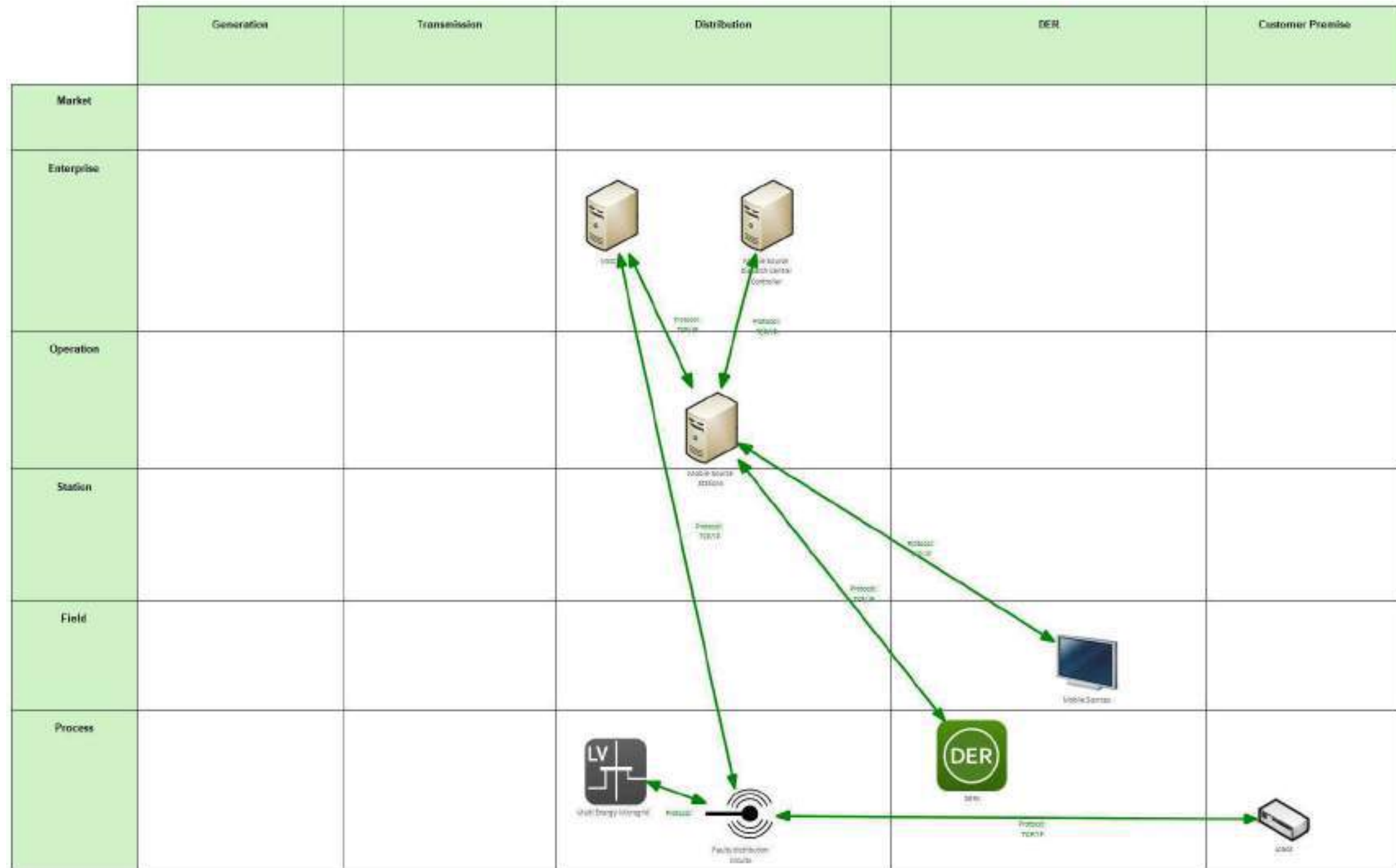


Figure 302 - UC32 Communication Layer

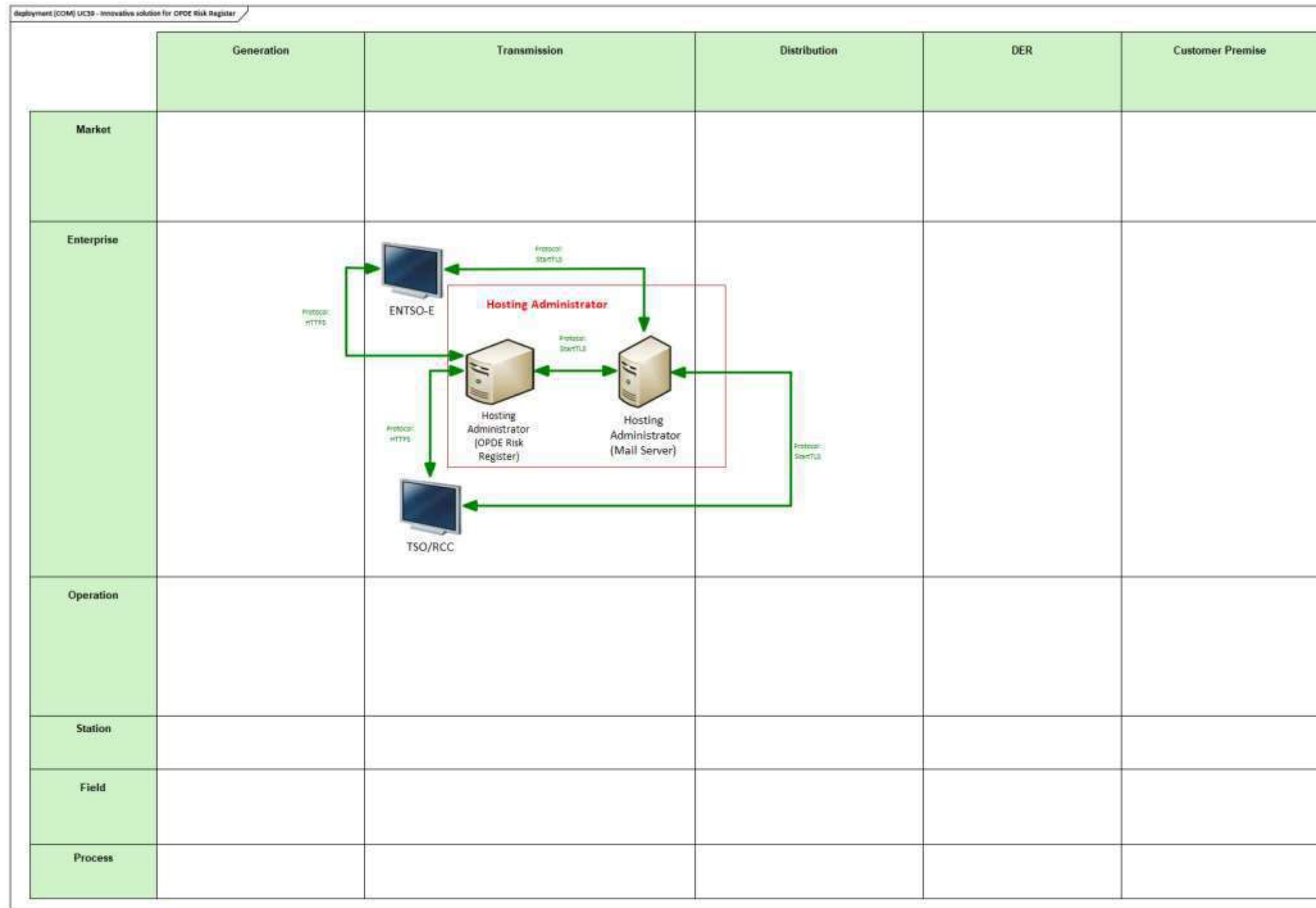


Figure 303 - UC39 Communication Layer



13.3.2 WP4-IRIS

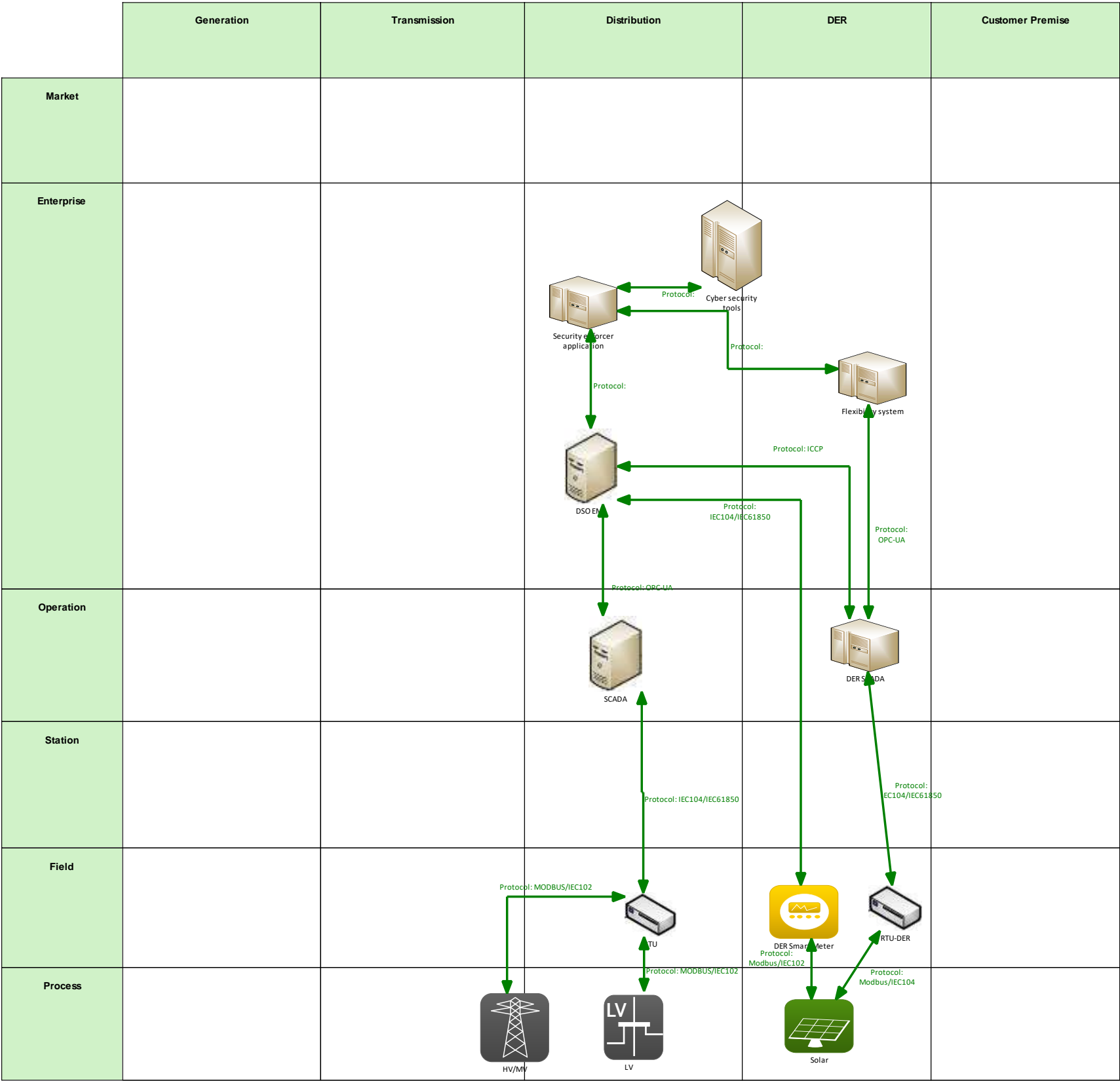


Figure 304 - UC07 Communication Layer

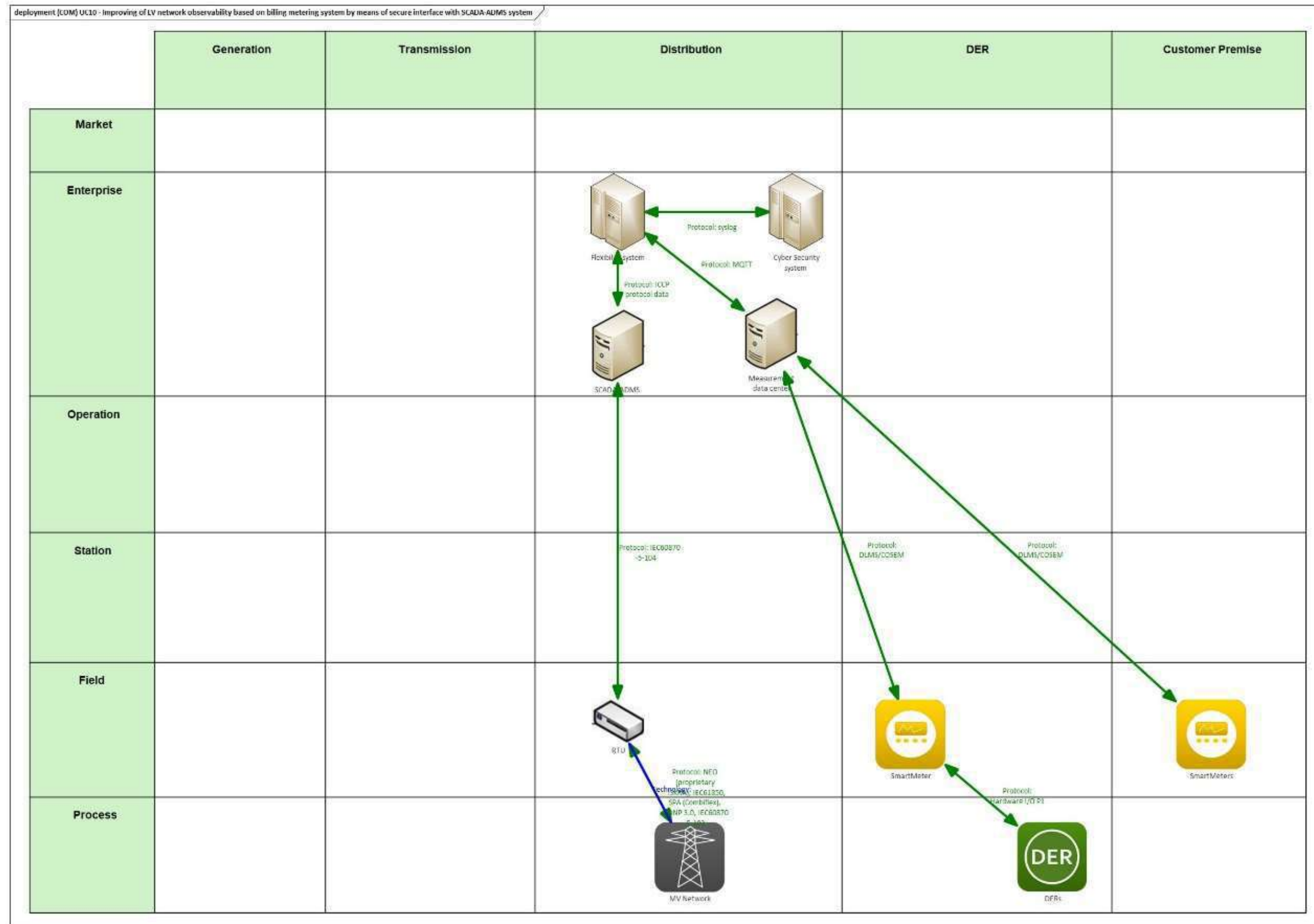


Figure 305 - UC10 Communication Layer

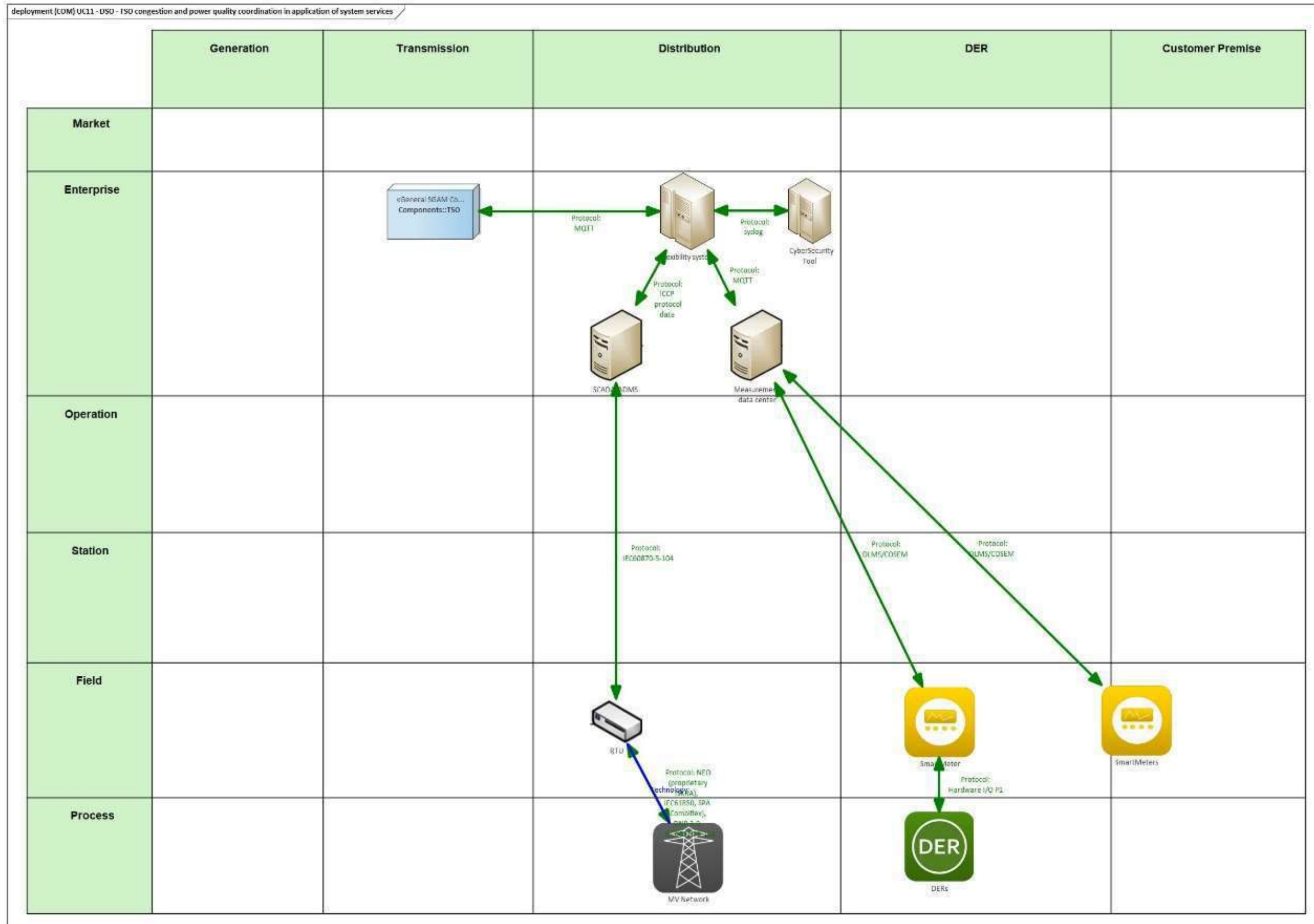


Figure 306 - UC11 Communication Layer

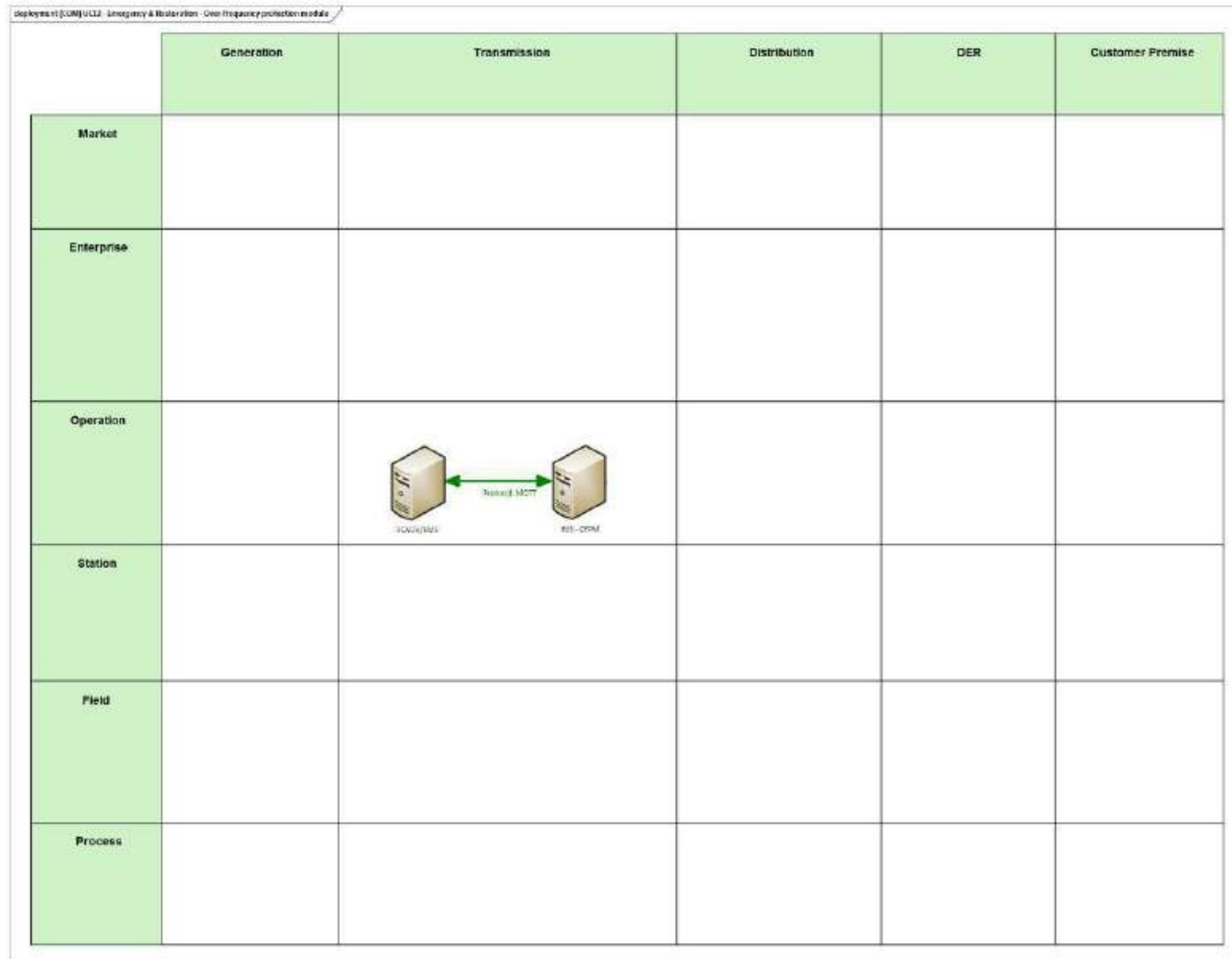


Figure 307 - UC12 Communication Layer

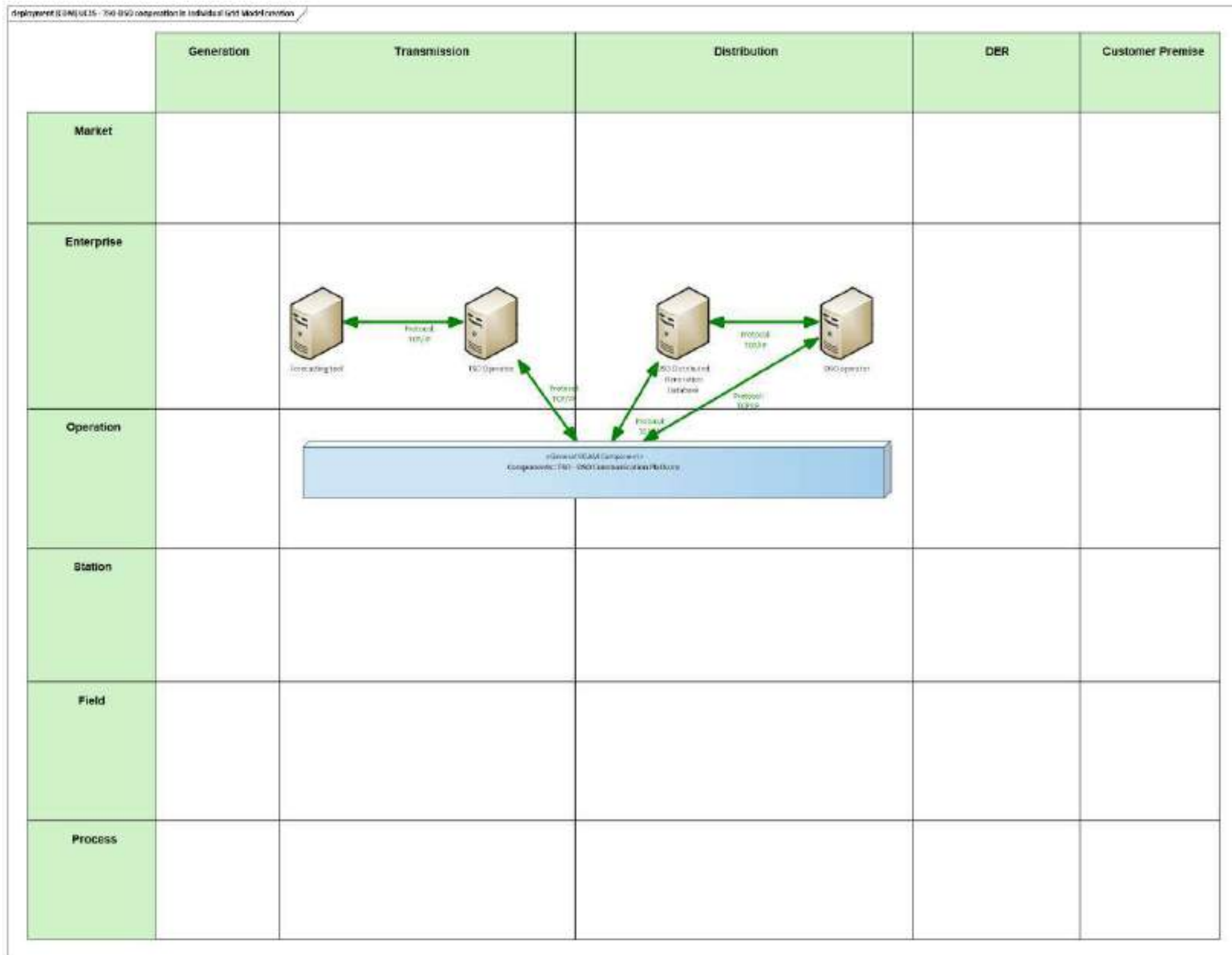


Figure 308 - UC15 Communication Layer

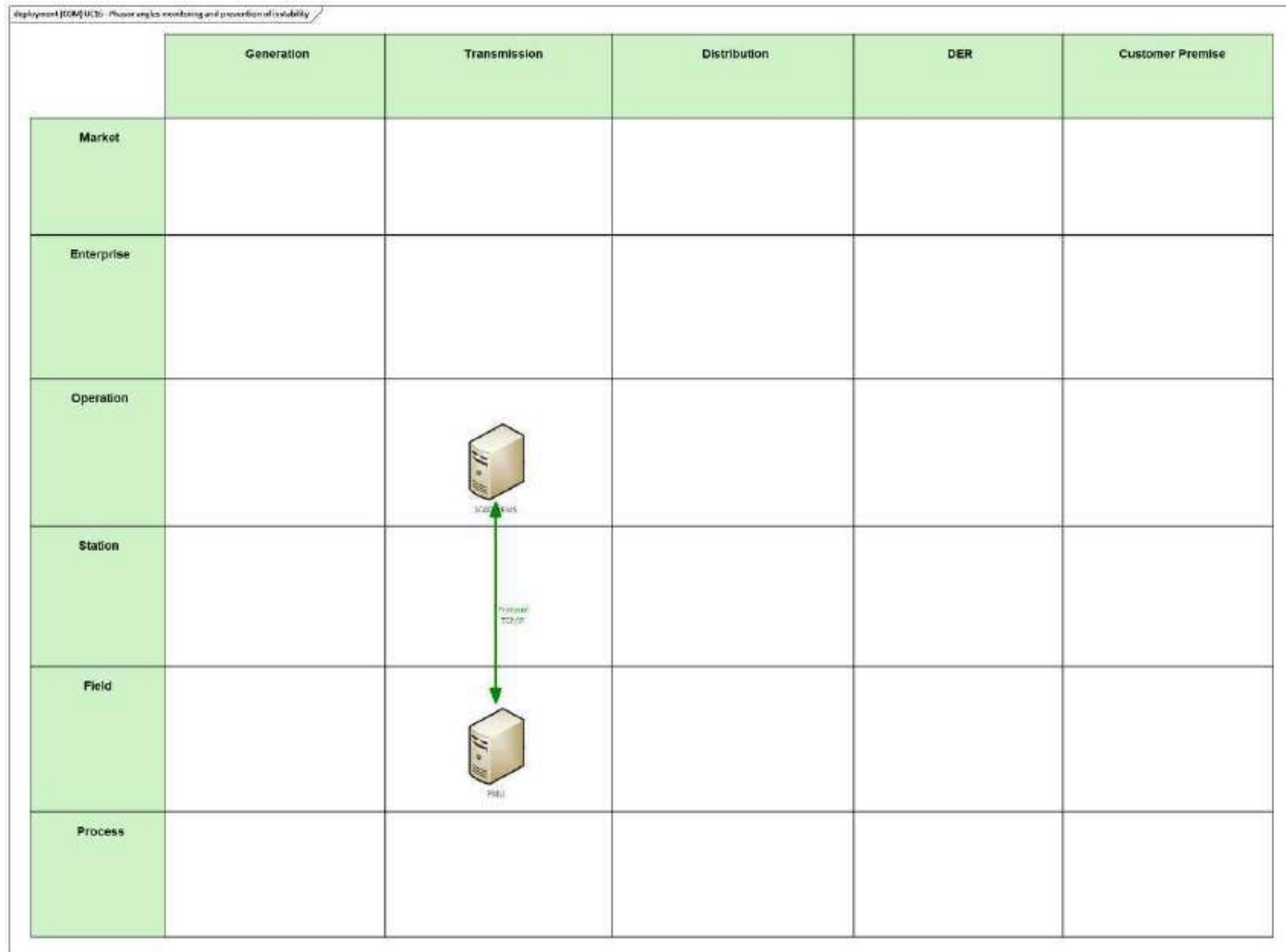


Figure 309 - UC16 Communication Layer

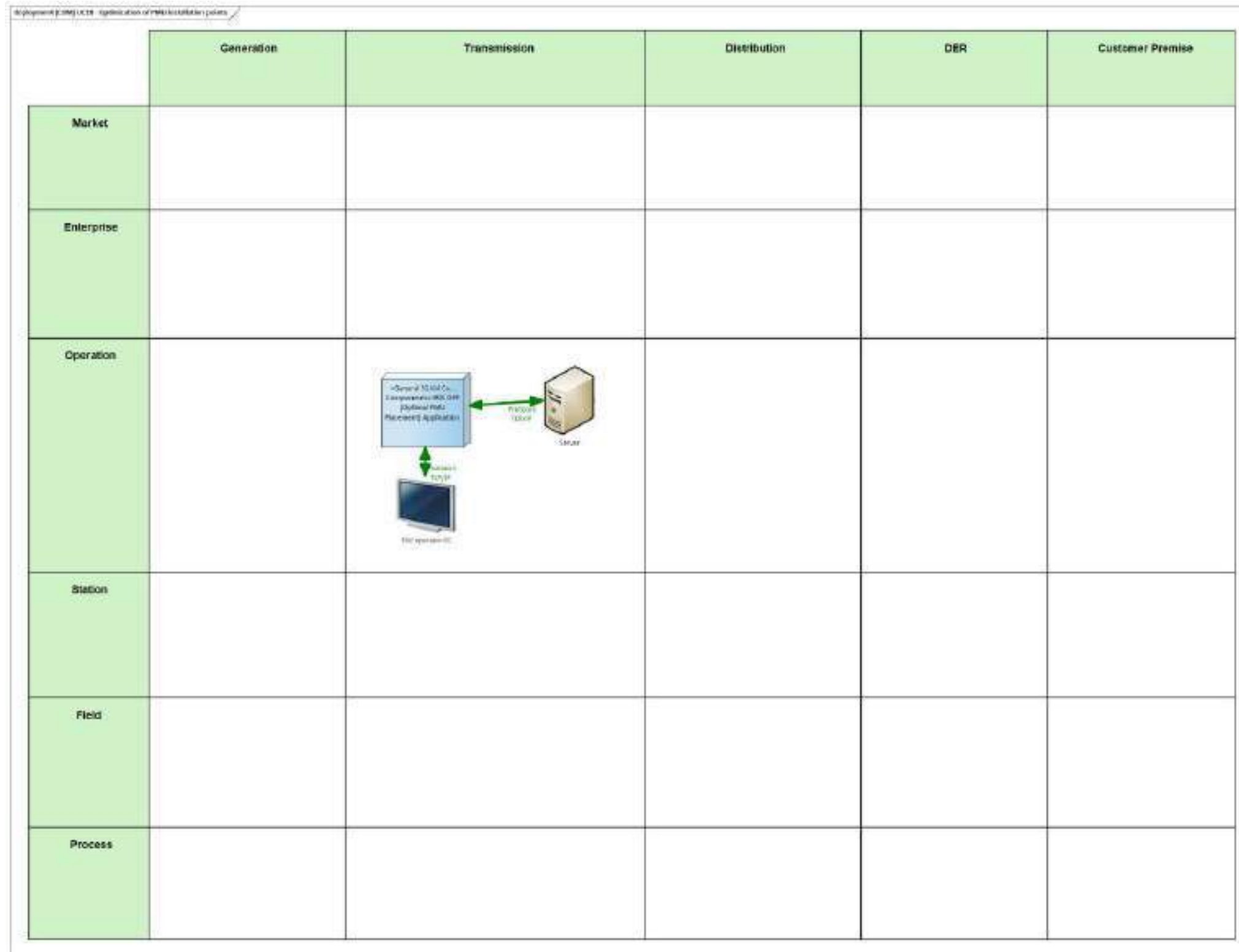


Figure 310 - UC18 Communication Layer

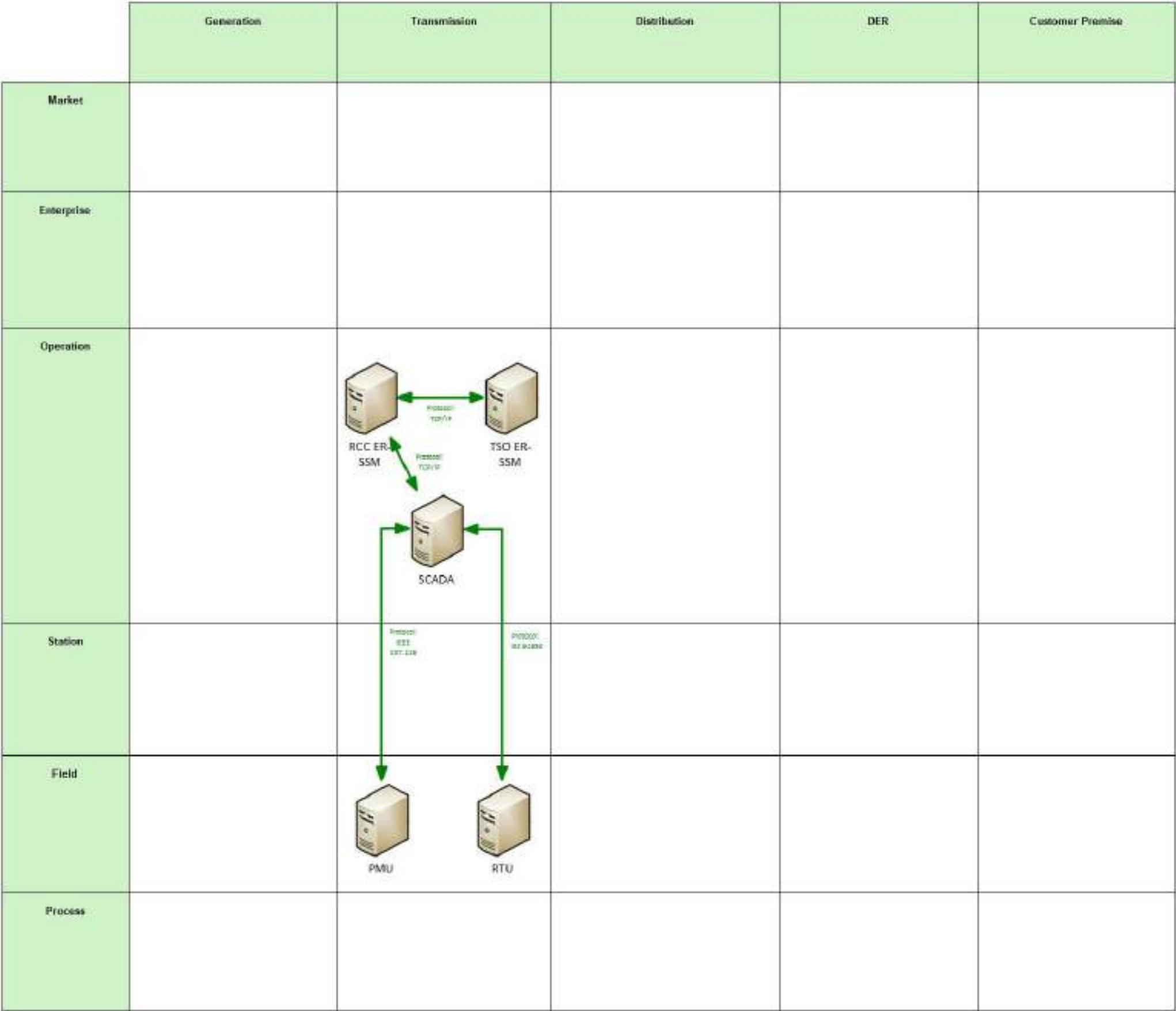


Figure 311 - UC19 Communication Layer

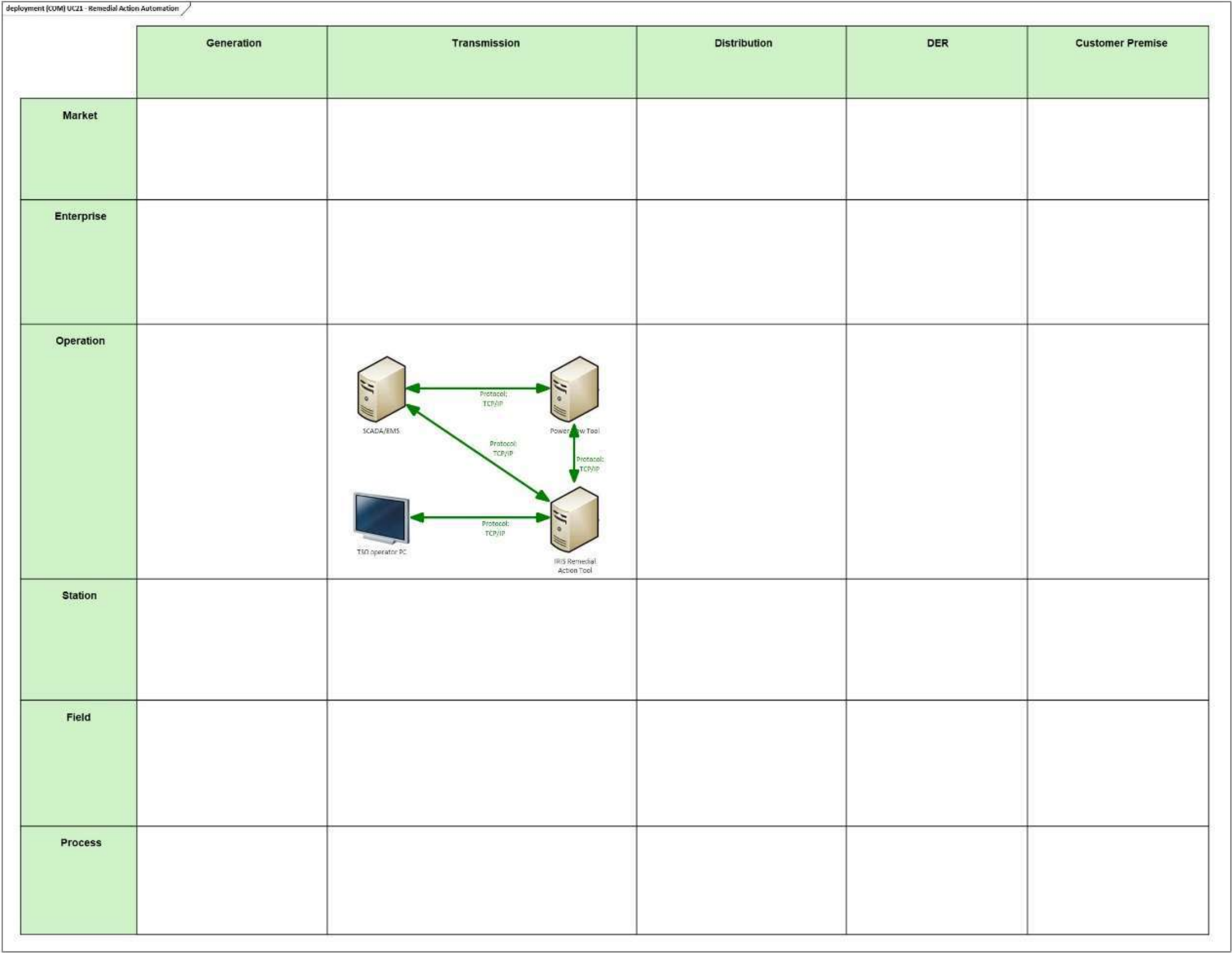
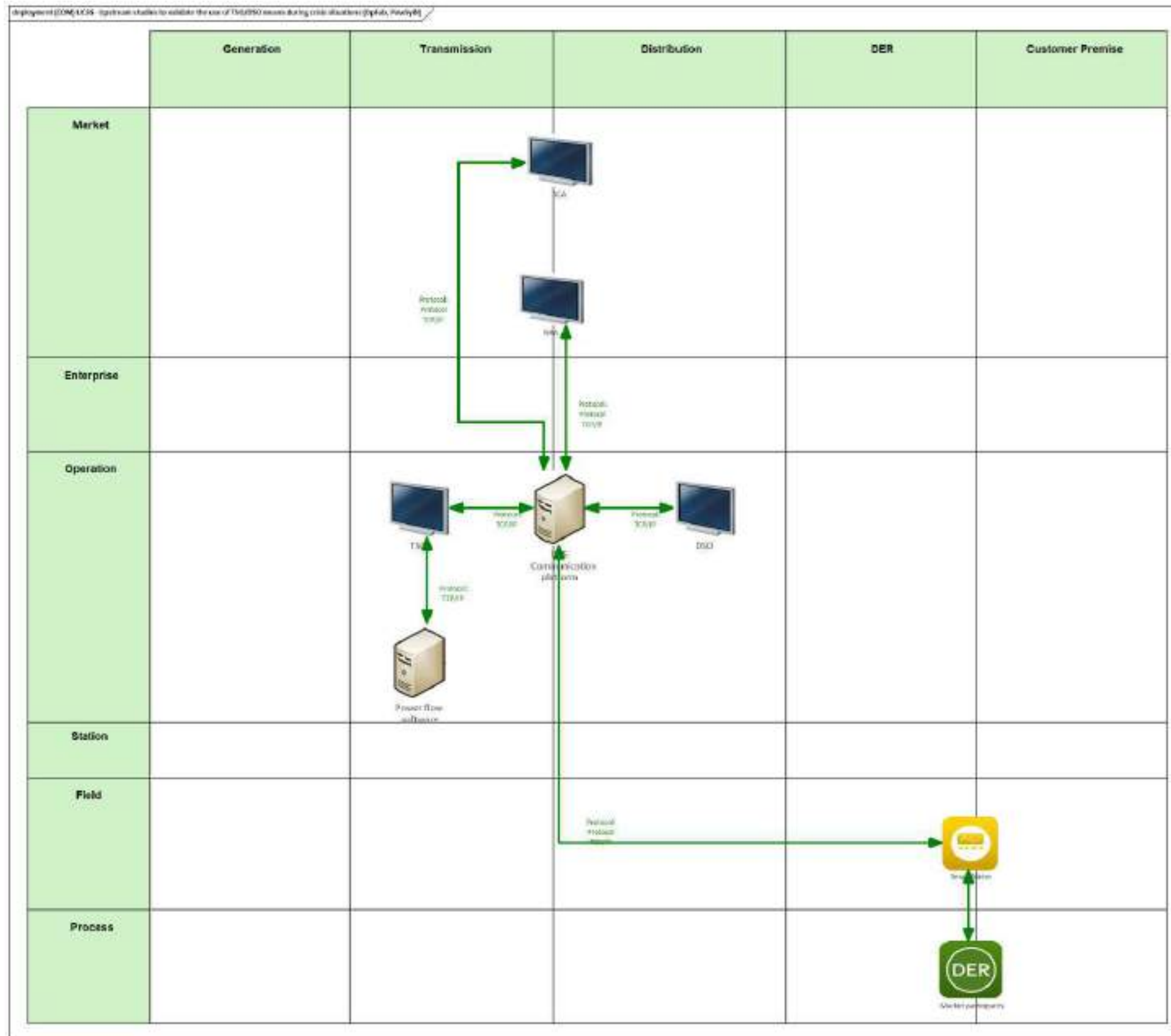


Figure 312 - UC21 Communication Layer





13.3.3 WP5-PRECOG

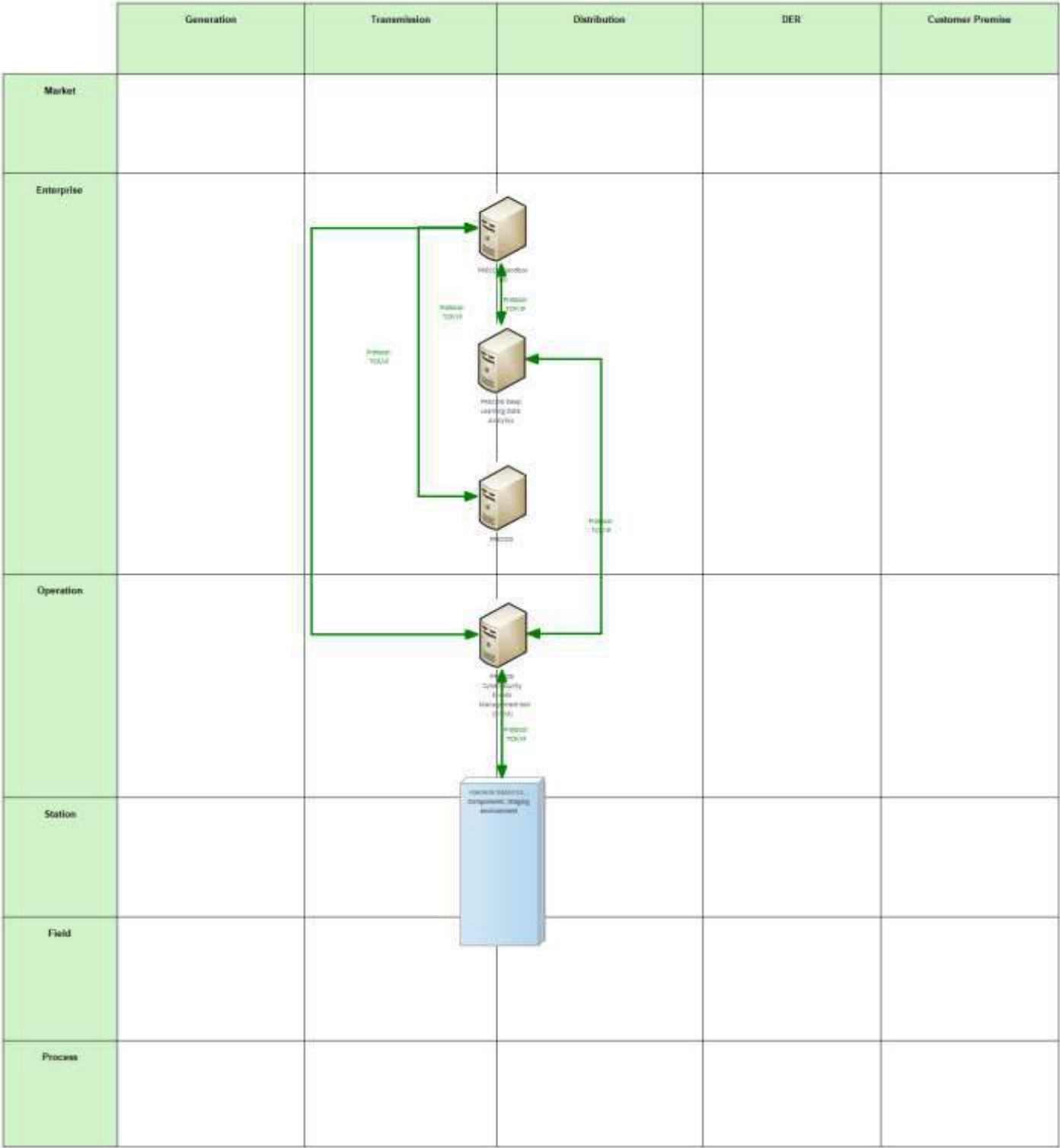


Figure 314 - UC27 Communication Layer

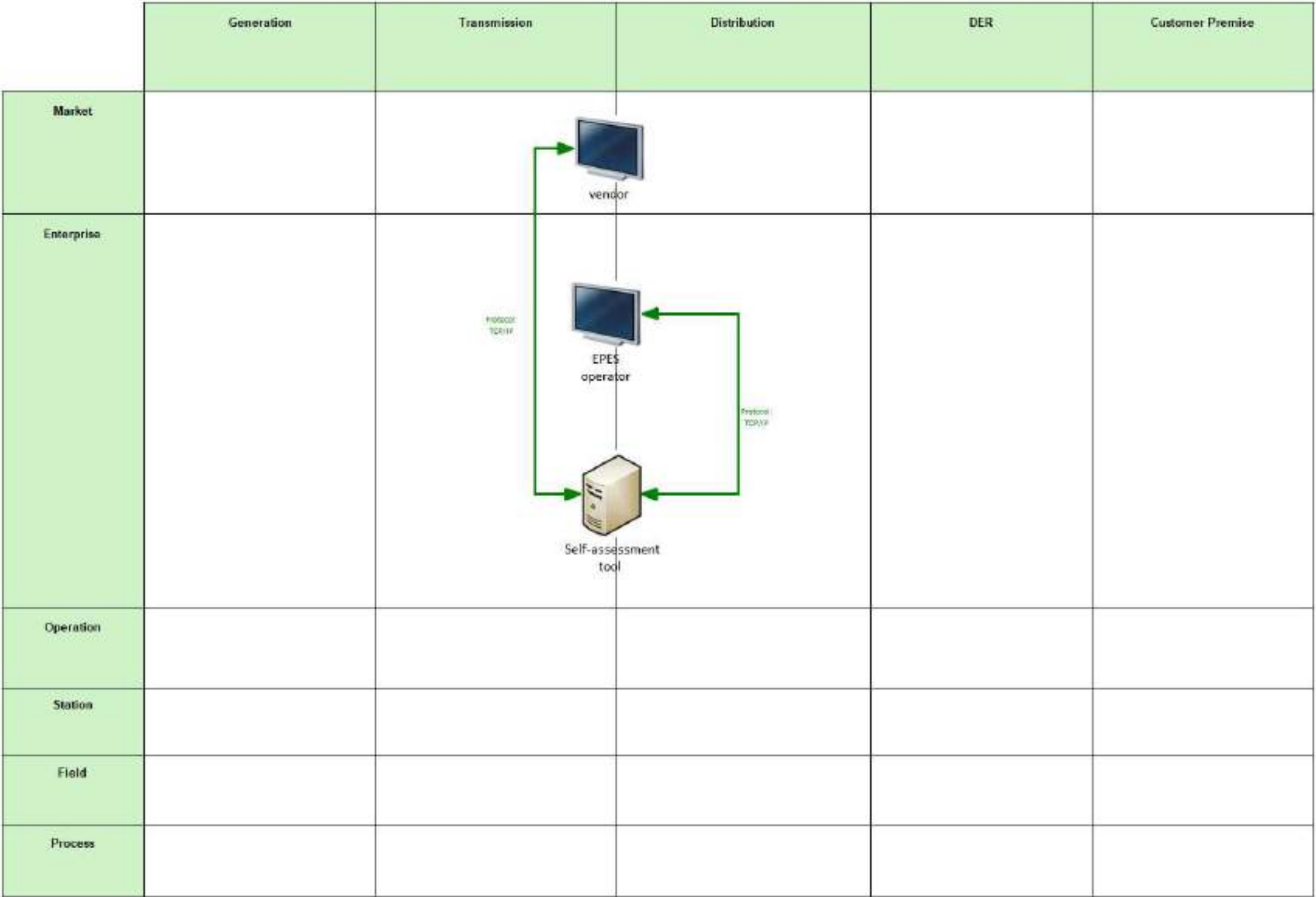


Figure 315 - UC28 Communication Layer

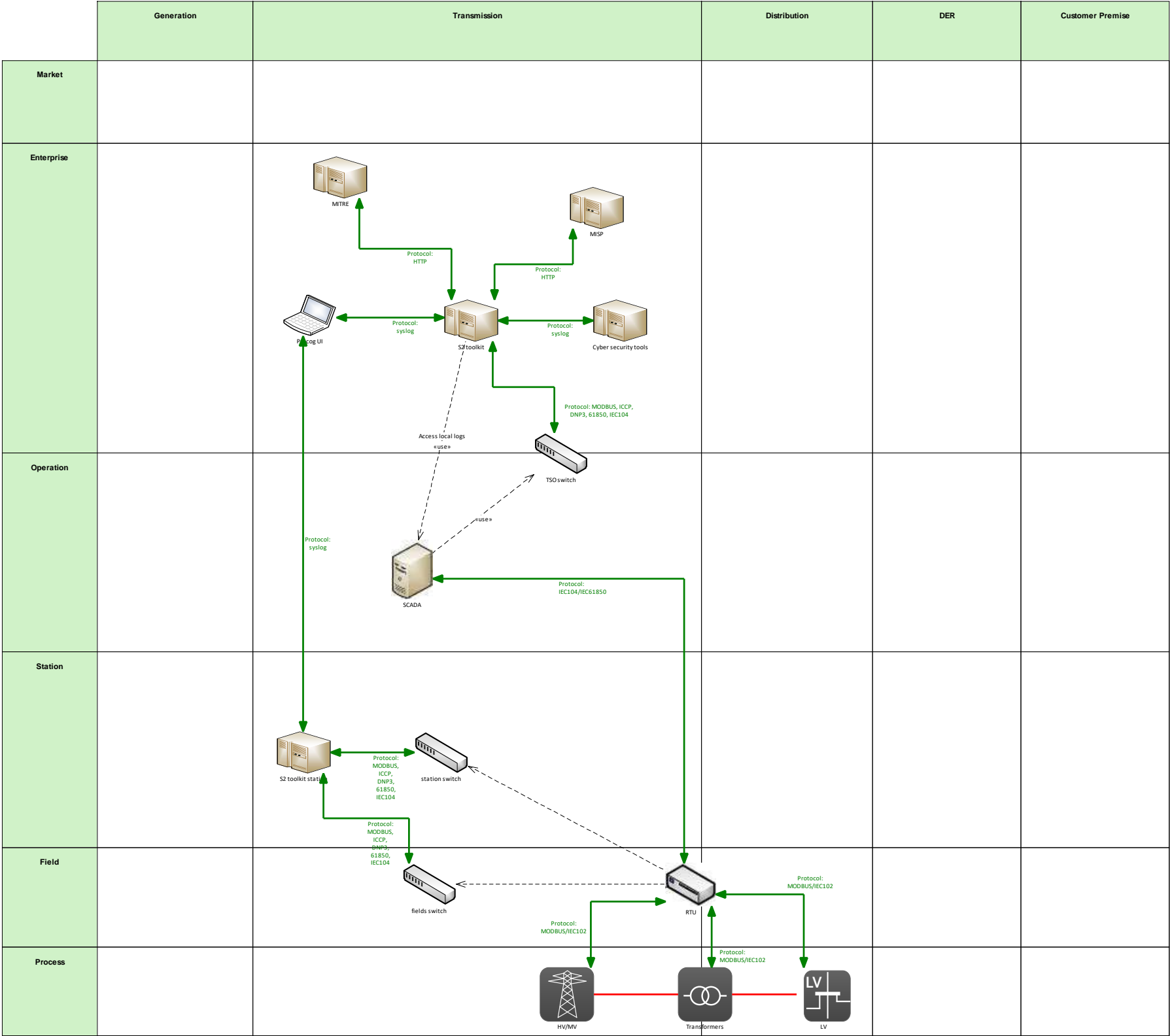


Figure 316 - UC33 Communication Layer

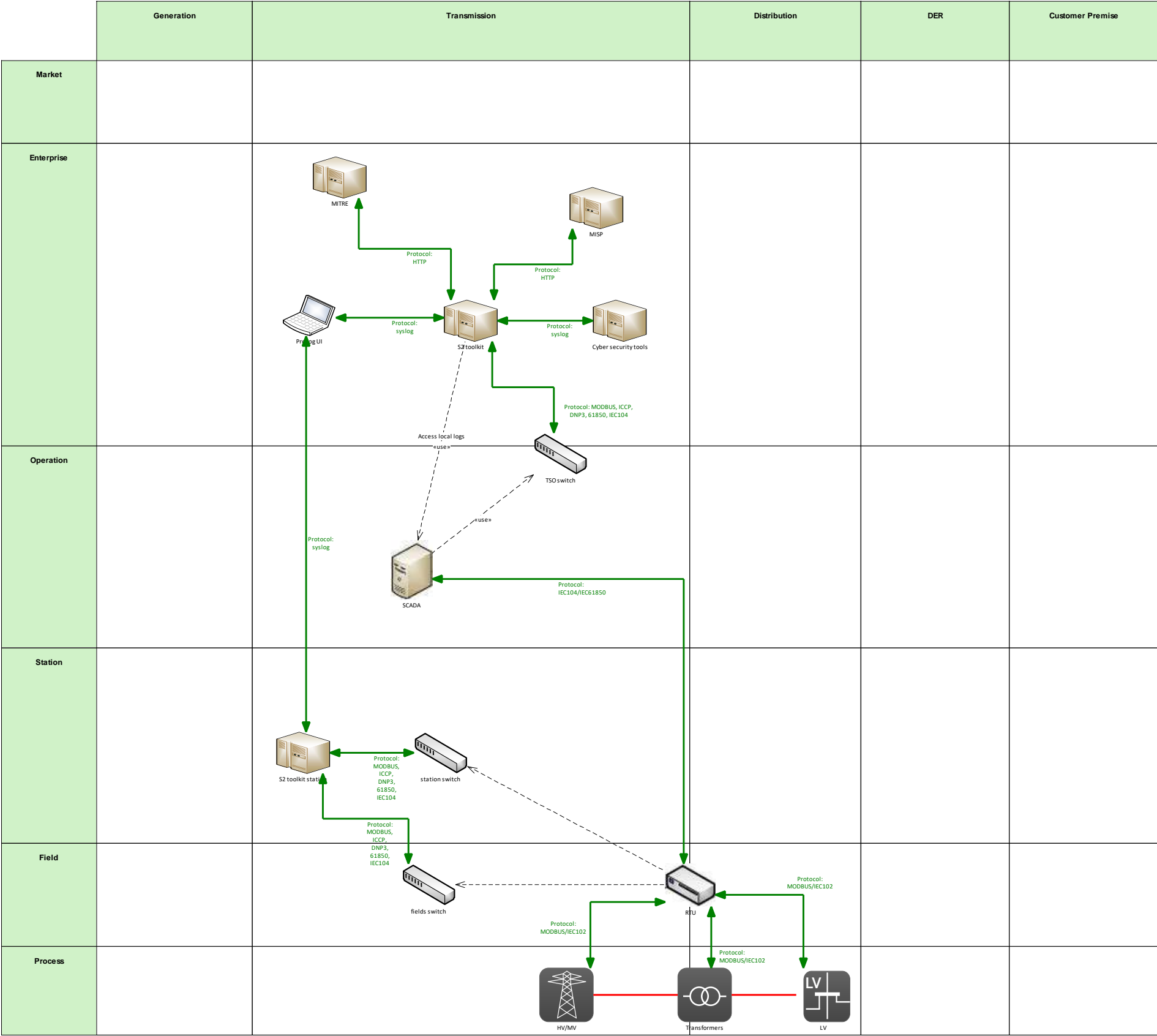


Figure 317 - UC35 Communication Layer



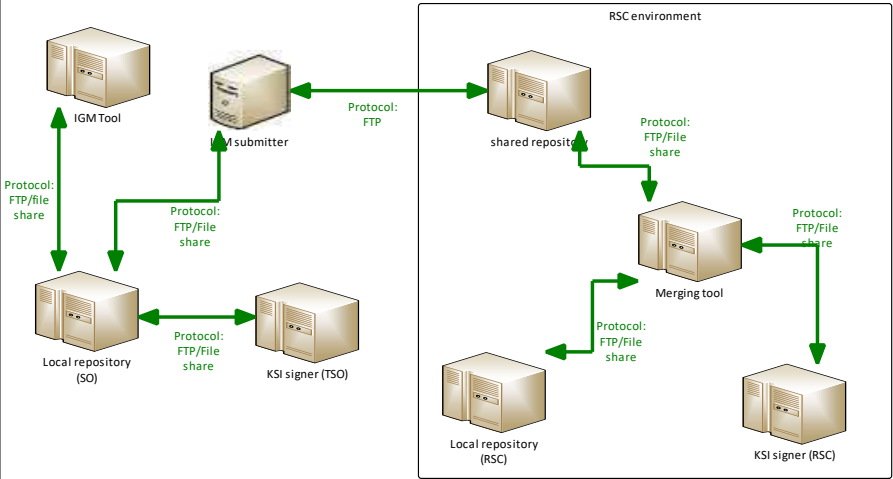
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 318 - UC36 Communication Layer

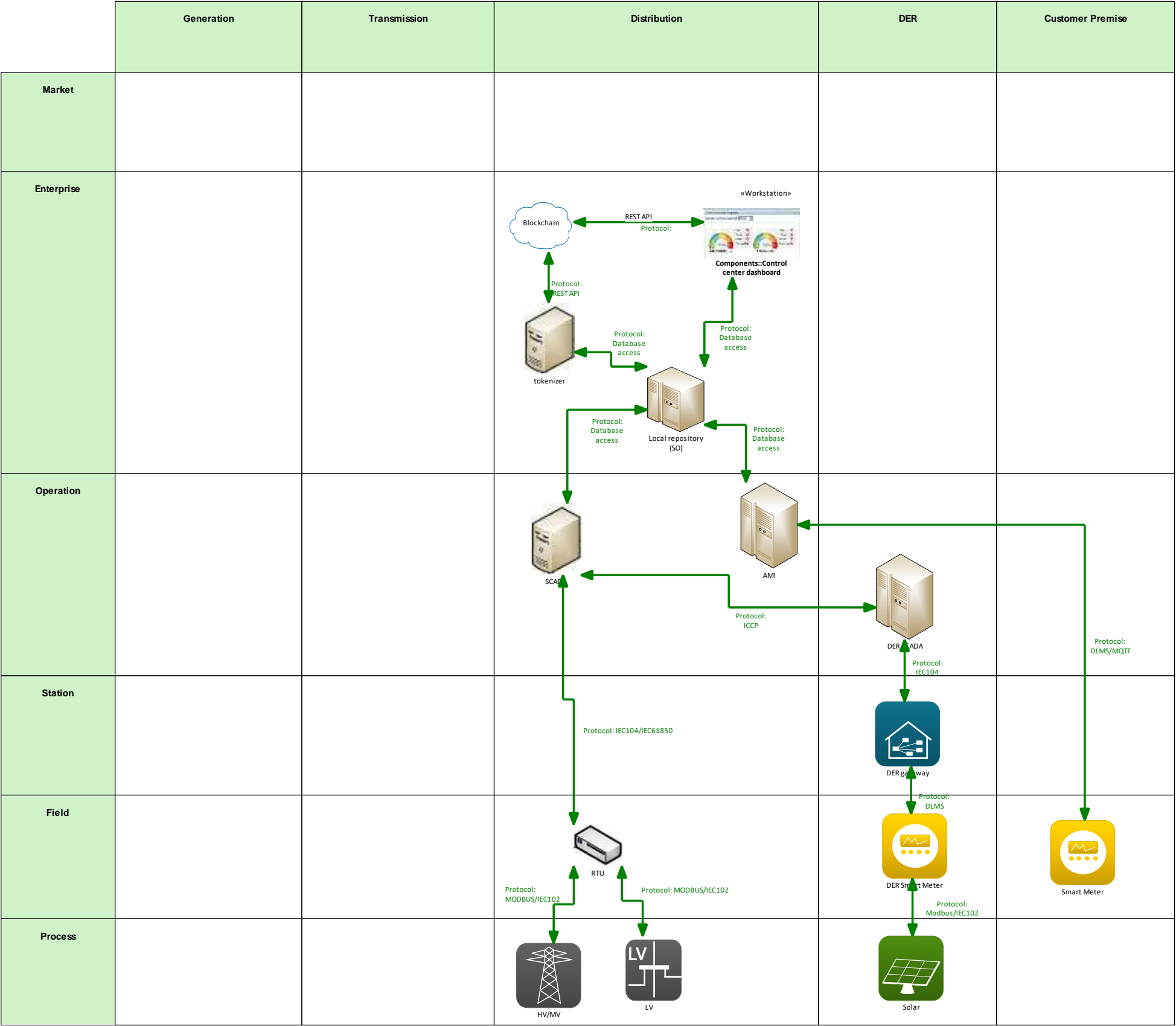


Figure 319 - UC37 Communication Layer

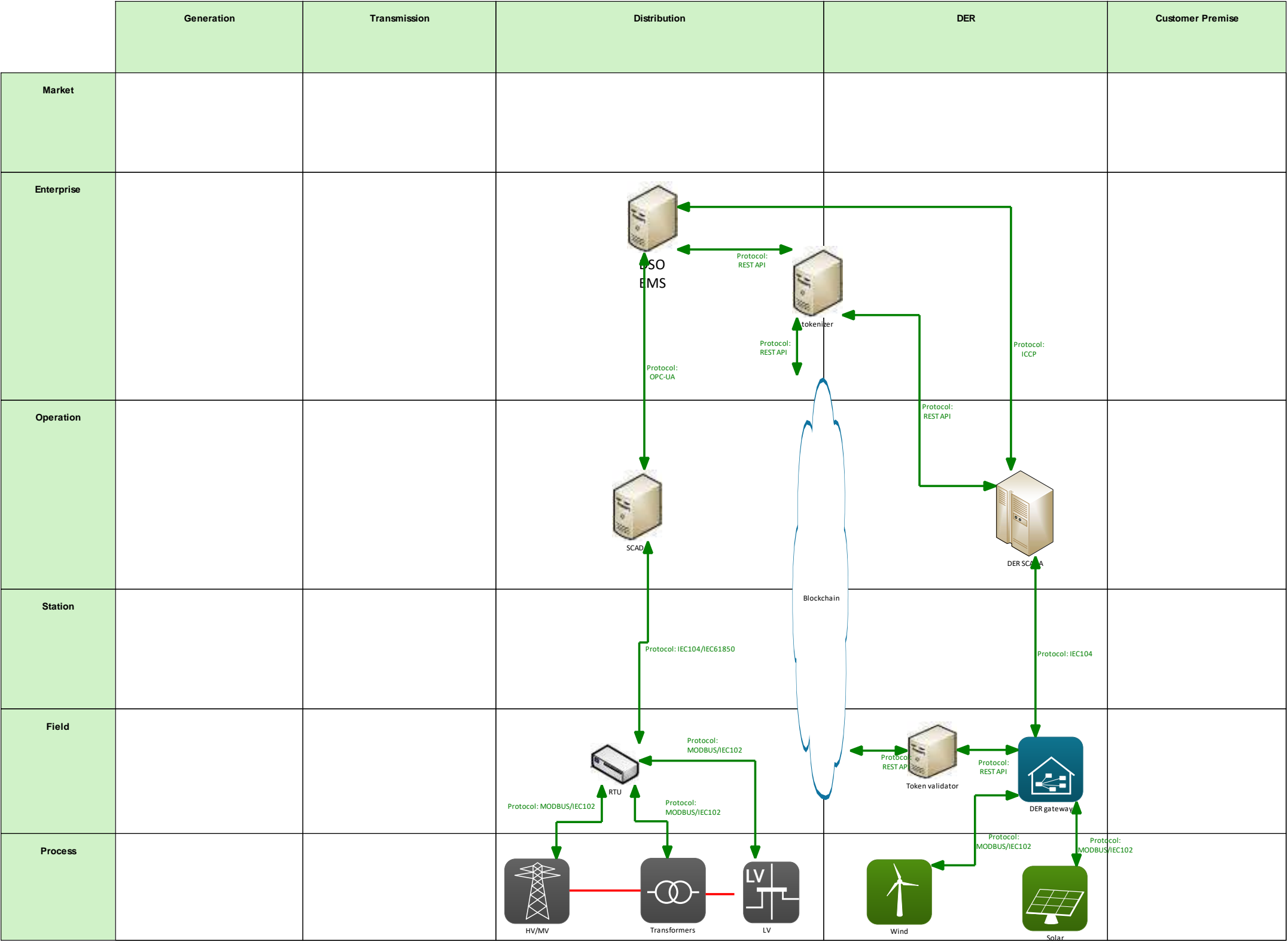


Figure 320 - UC38 Communication Layer

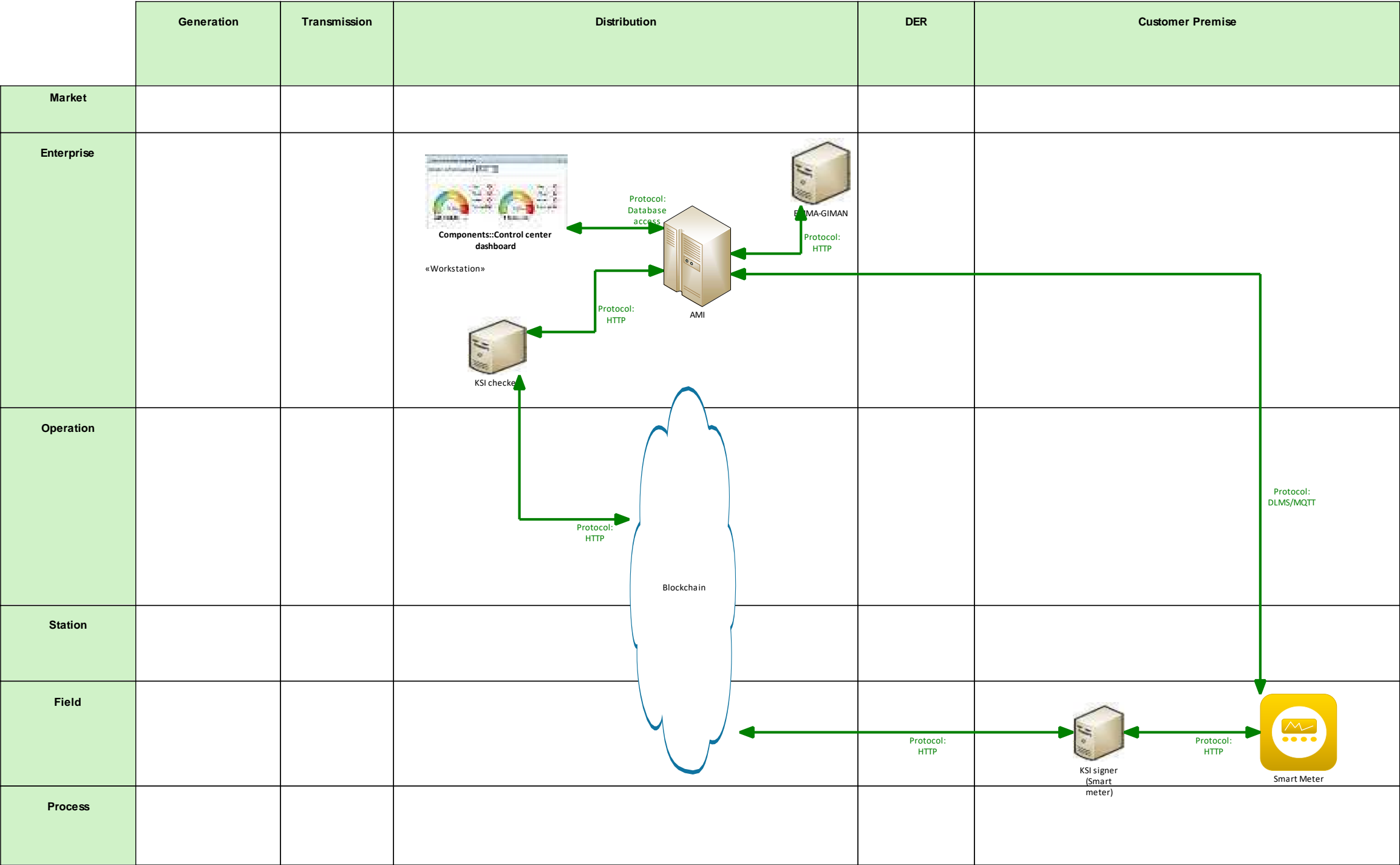


Figure 321 - UC40 Communication Layer



13.3.4 WP6-EMMA

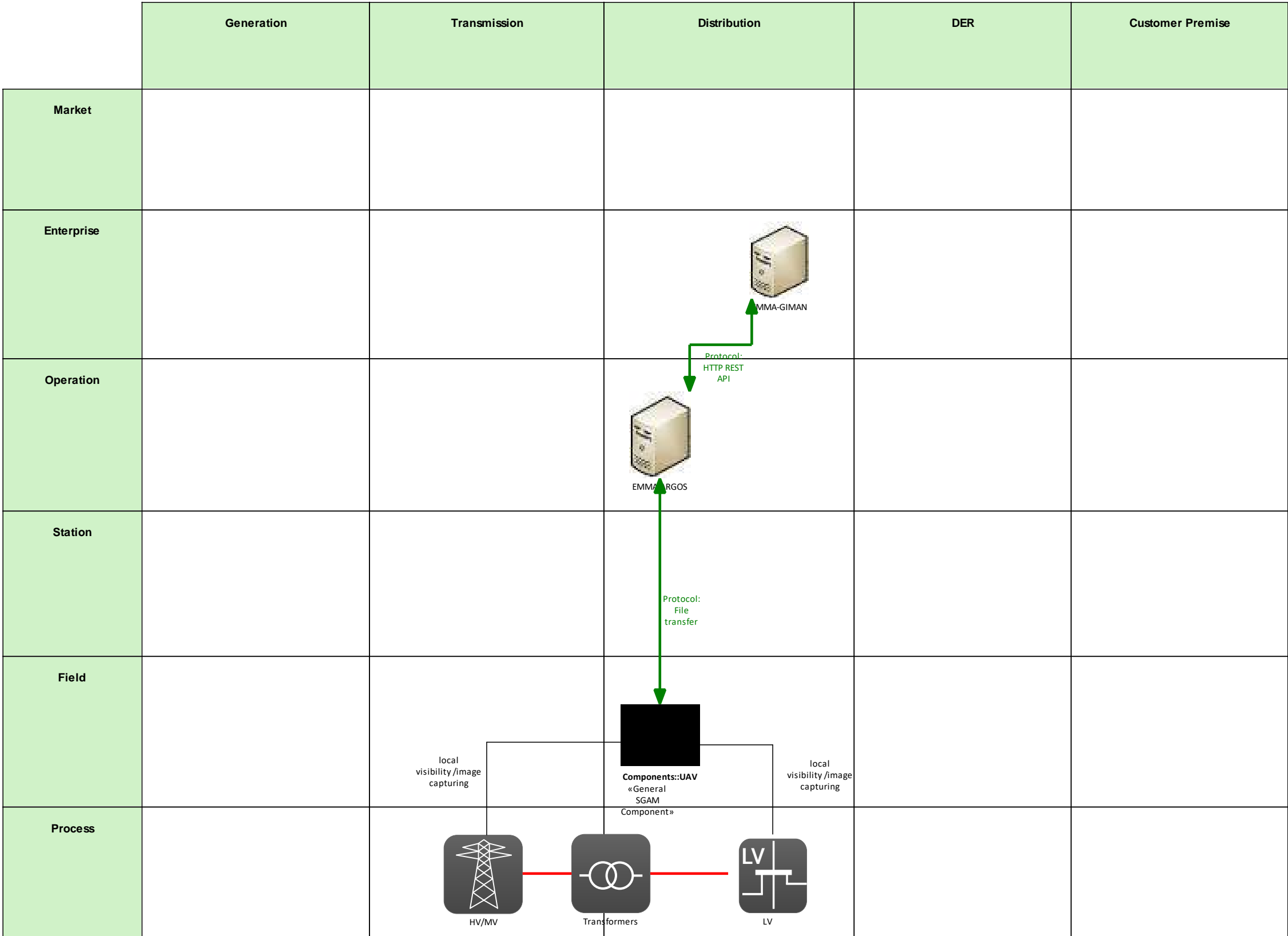


Figure 322 - UC01 Communication Layer

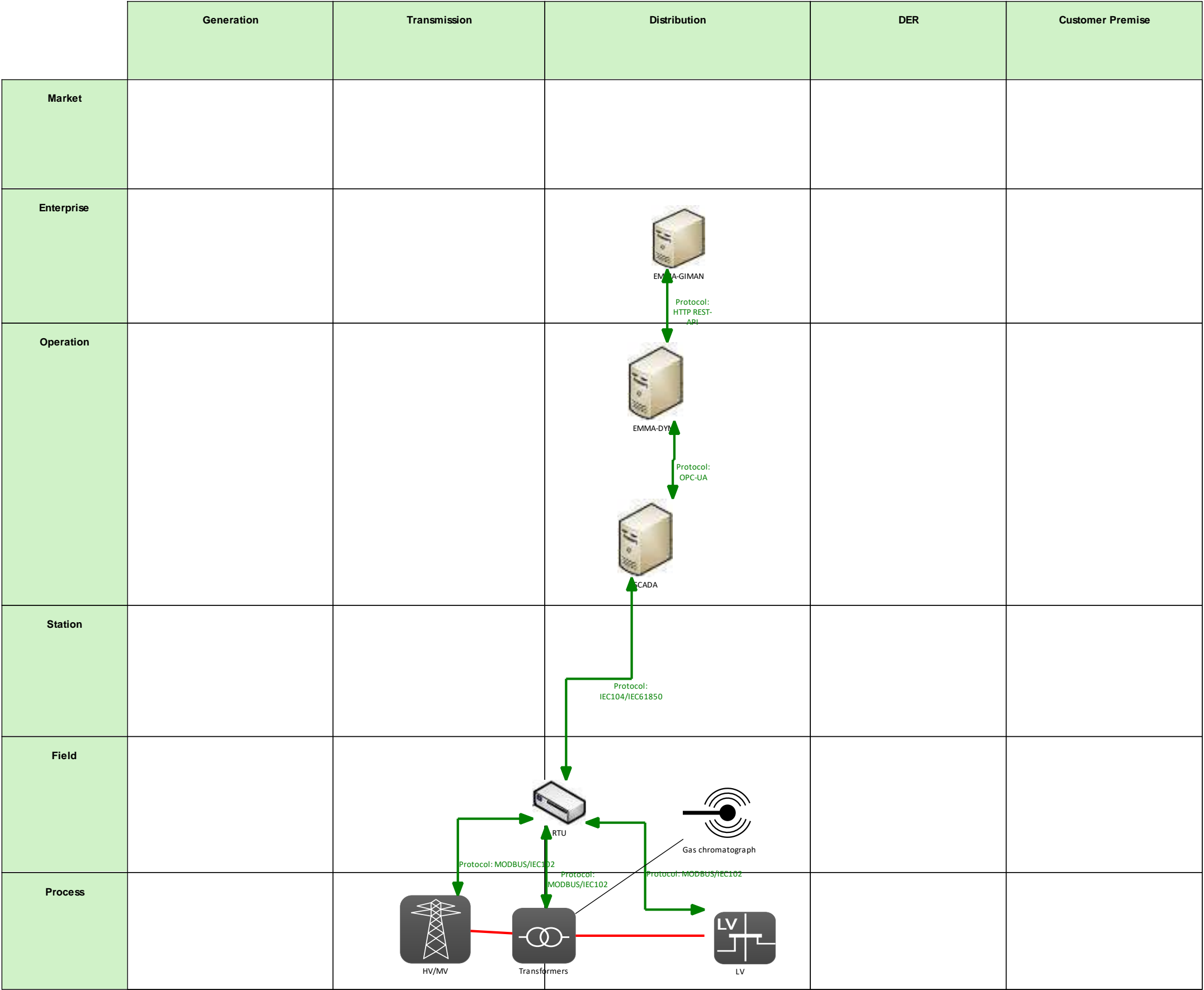


Figure 323 - UC02 Communication Layer

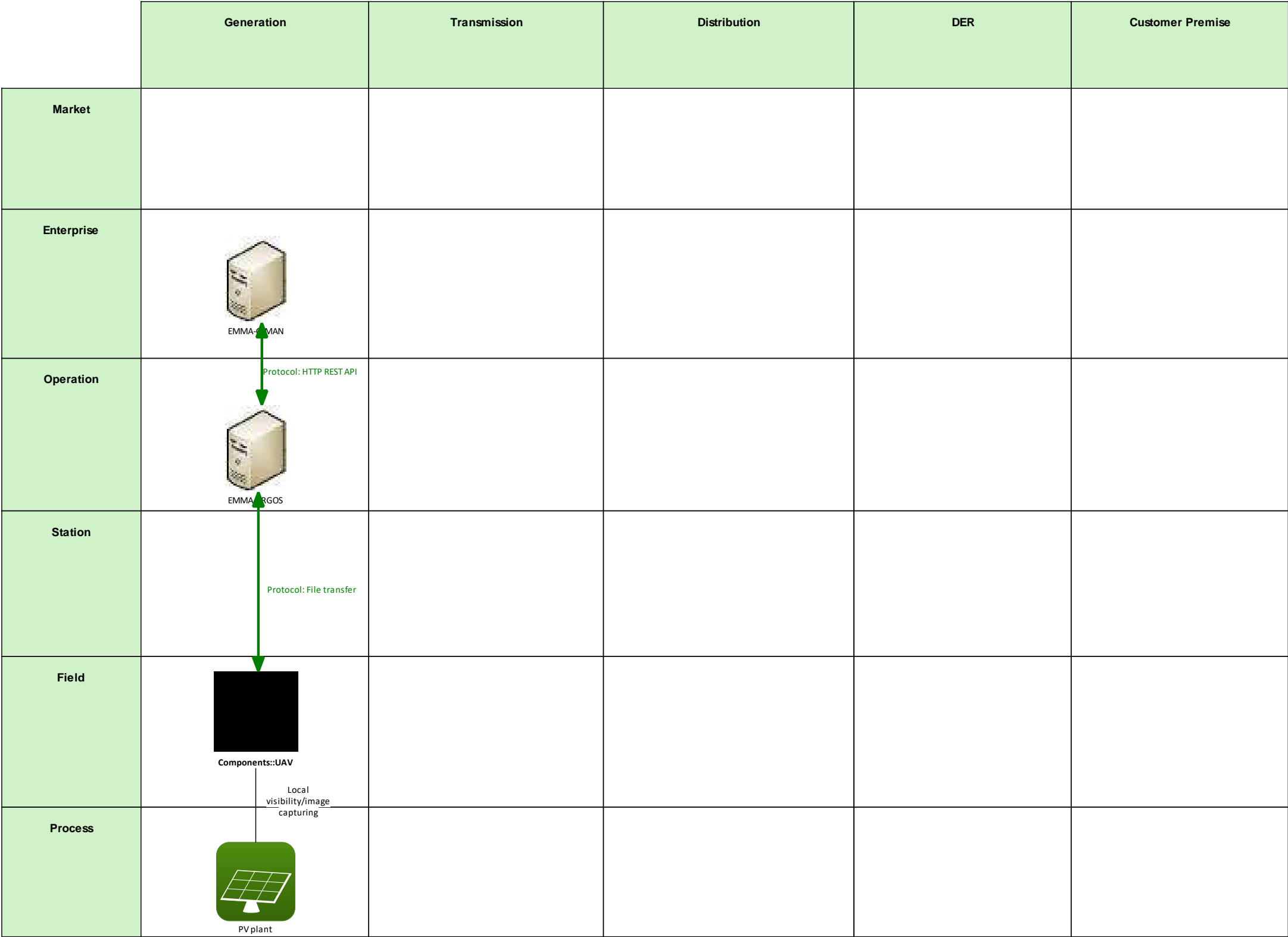


Figure 324 - UC03 Communication Layer

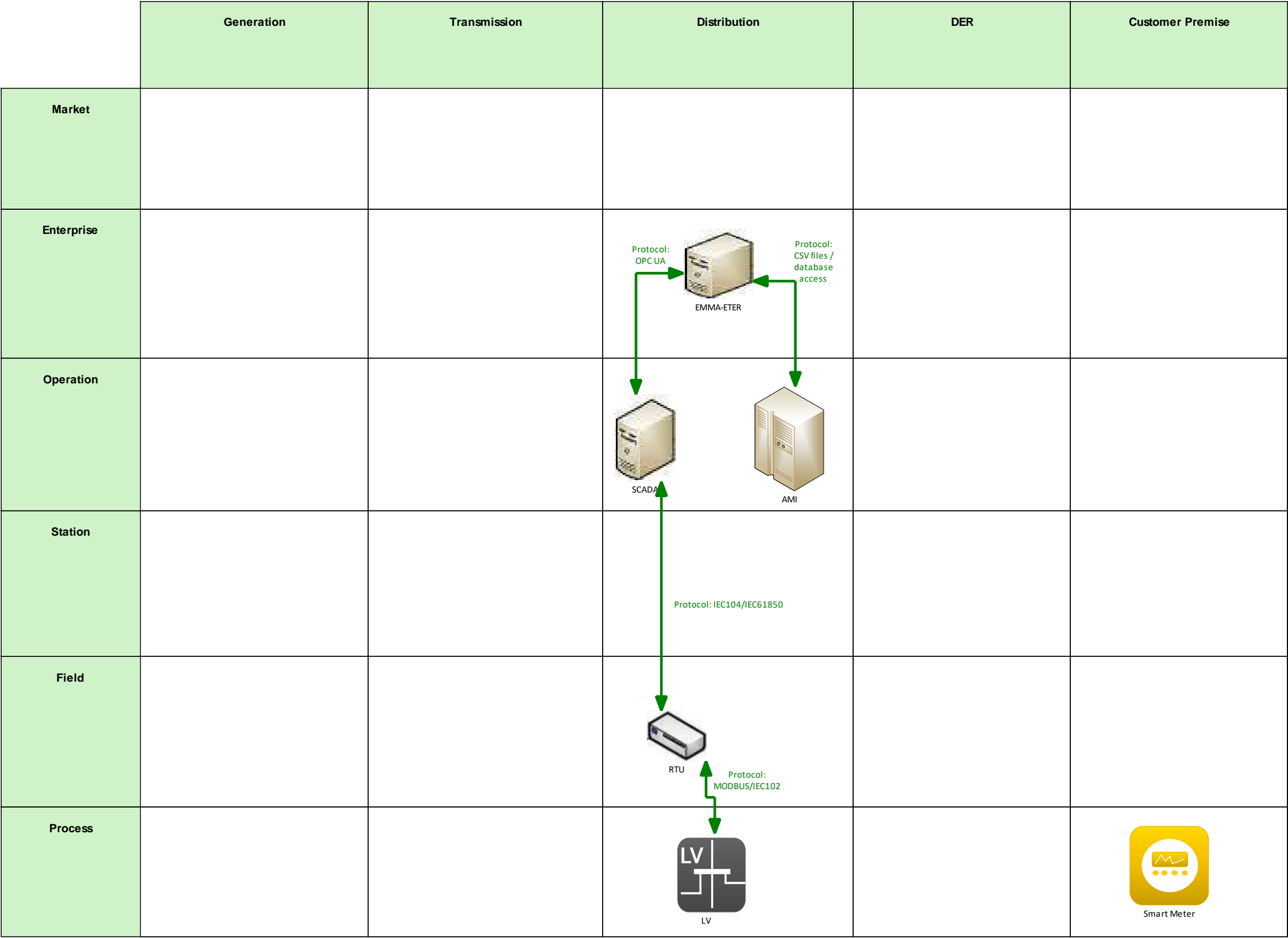


Figure 325 - UC04 Communication Layer

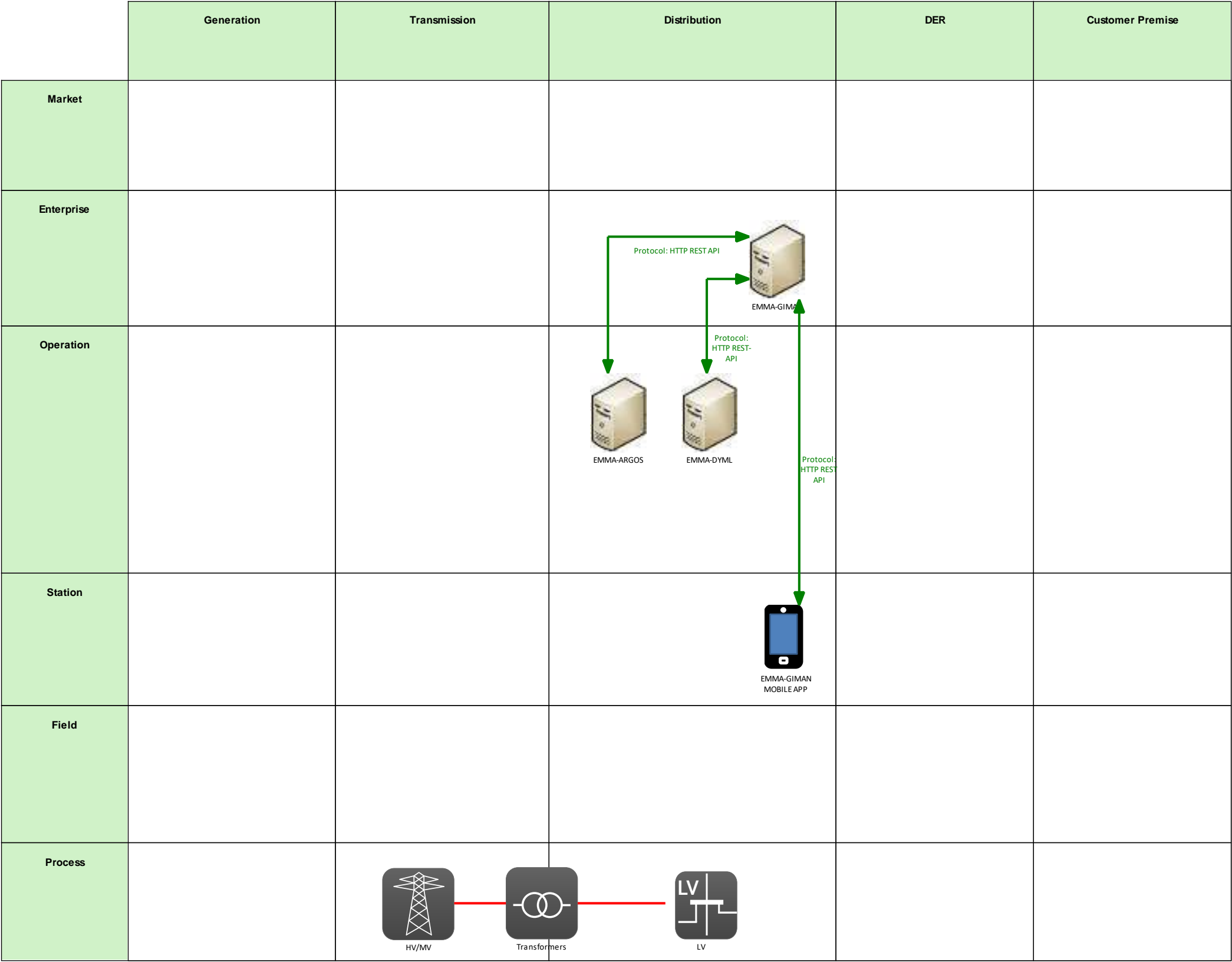


Figure 326 - UC05 Communication Layer

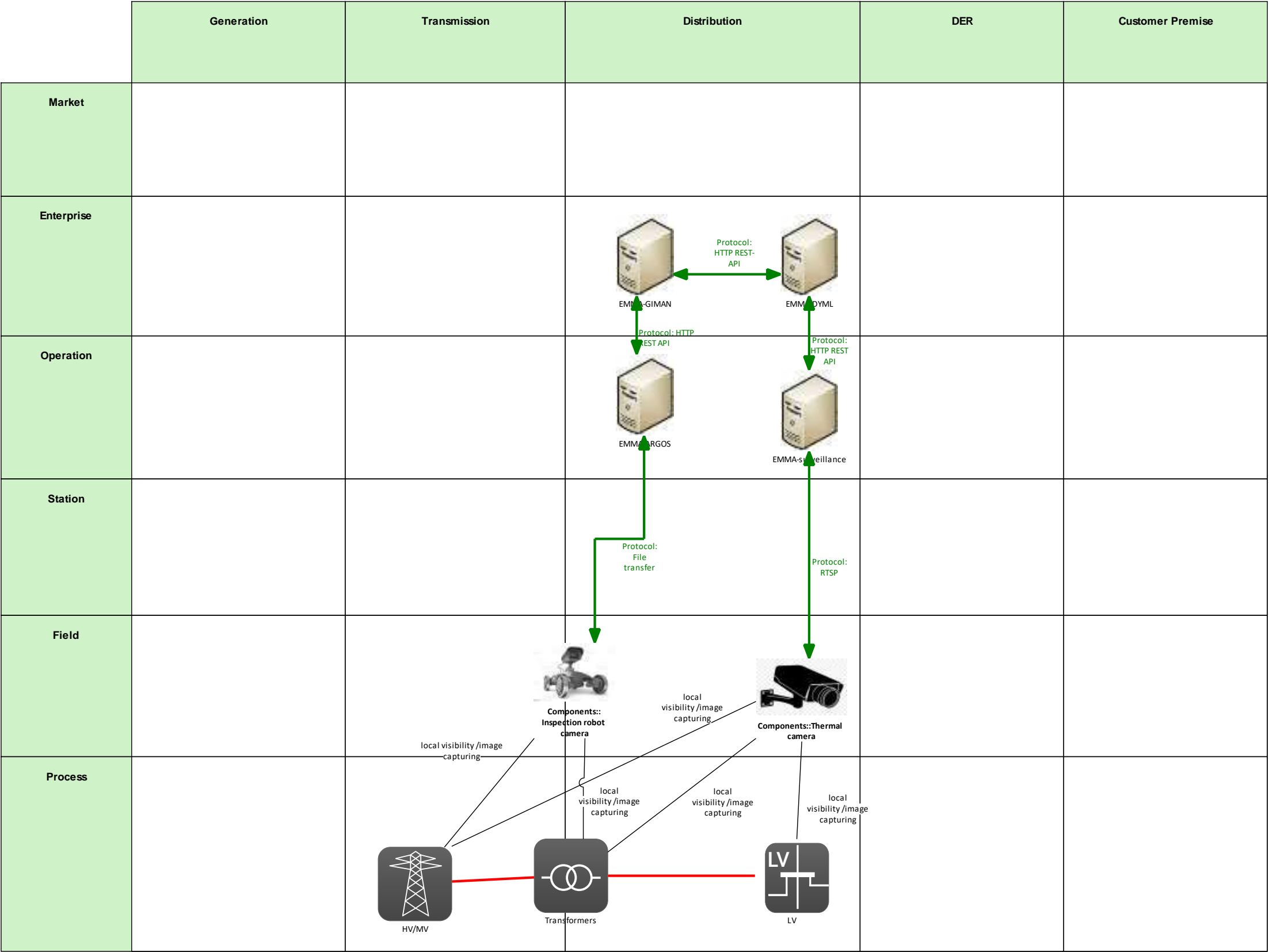


Figure 327 - UC06 Communication Layer

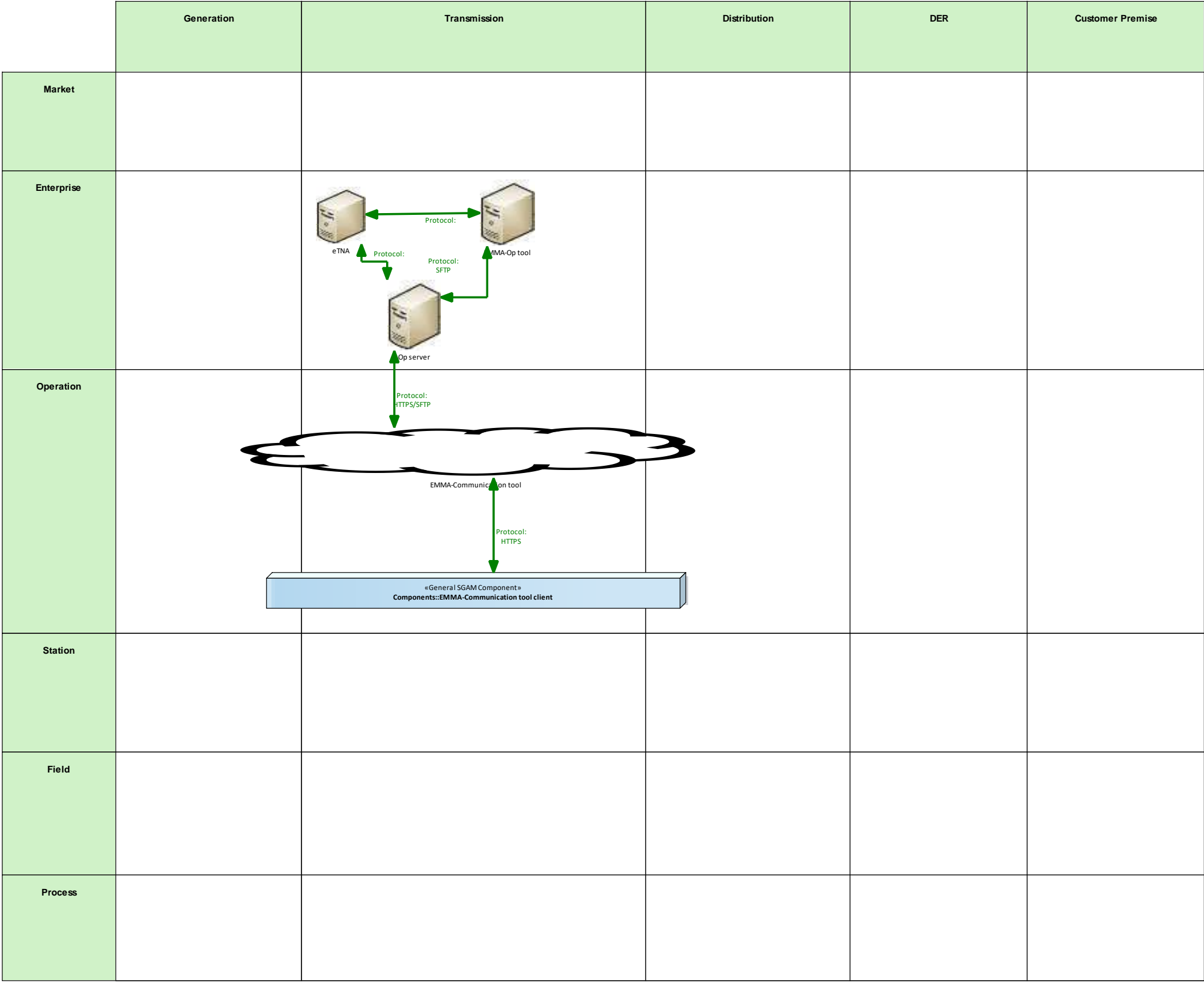


Figure 328 - UC08 Communication Layer



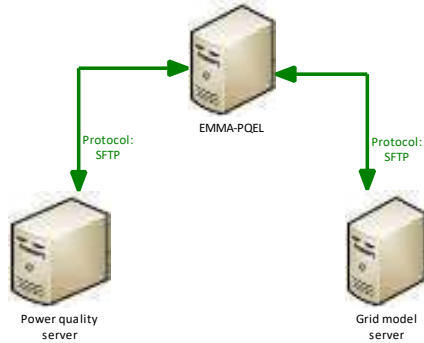
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 329 - UC09 Communication Layer

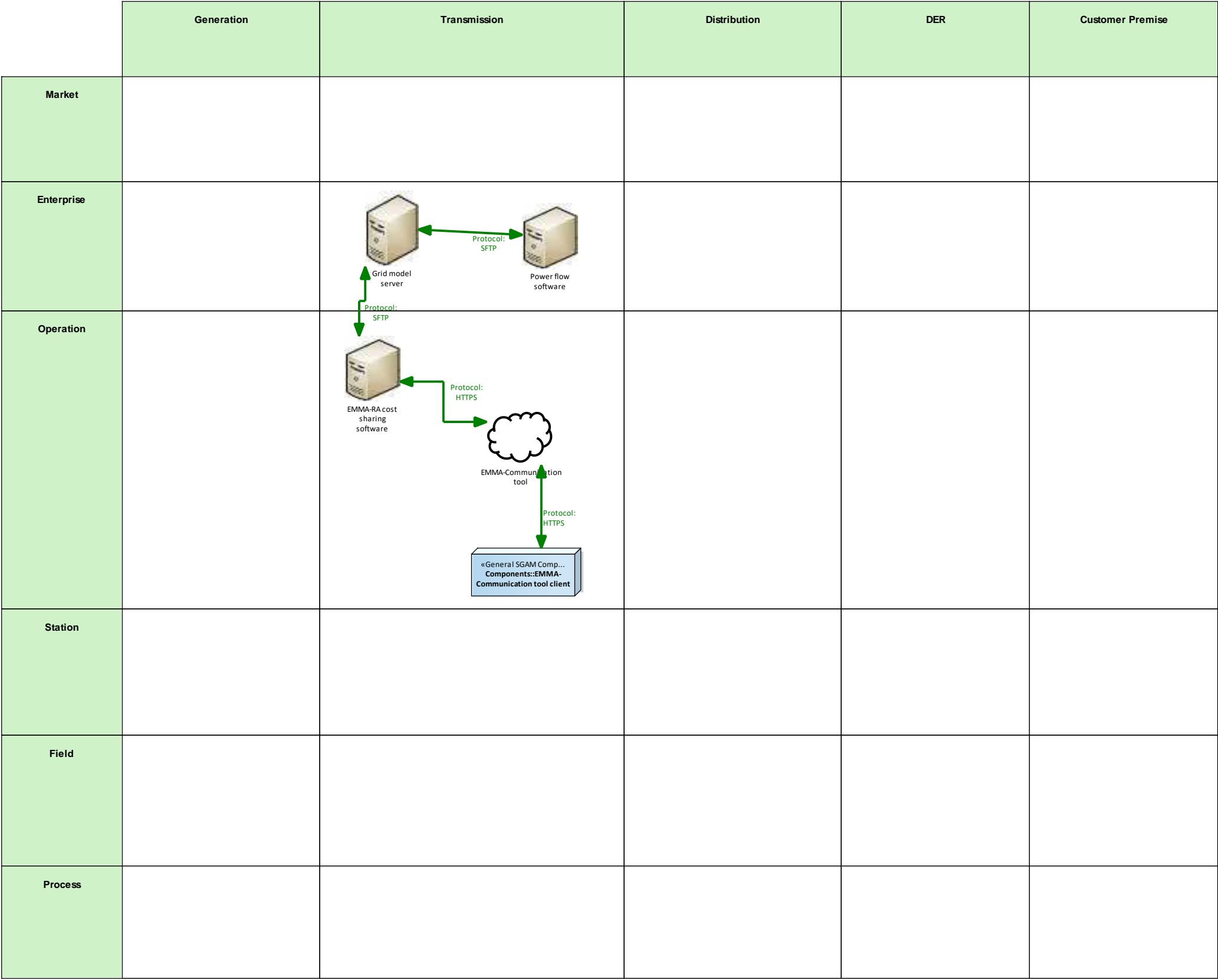


Figure 330 - UC13 Communication Layer




	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 331 - UC 14 Communication Layer



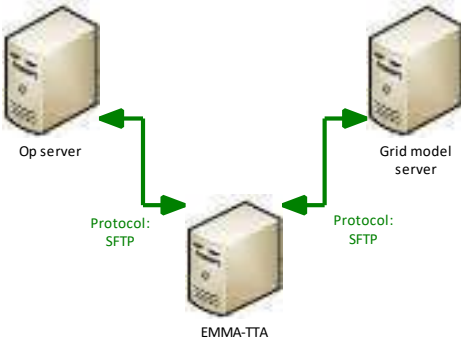
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 332 - UC17 Communication Layer

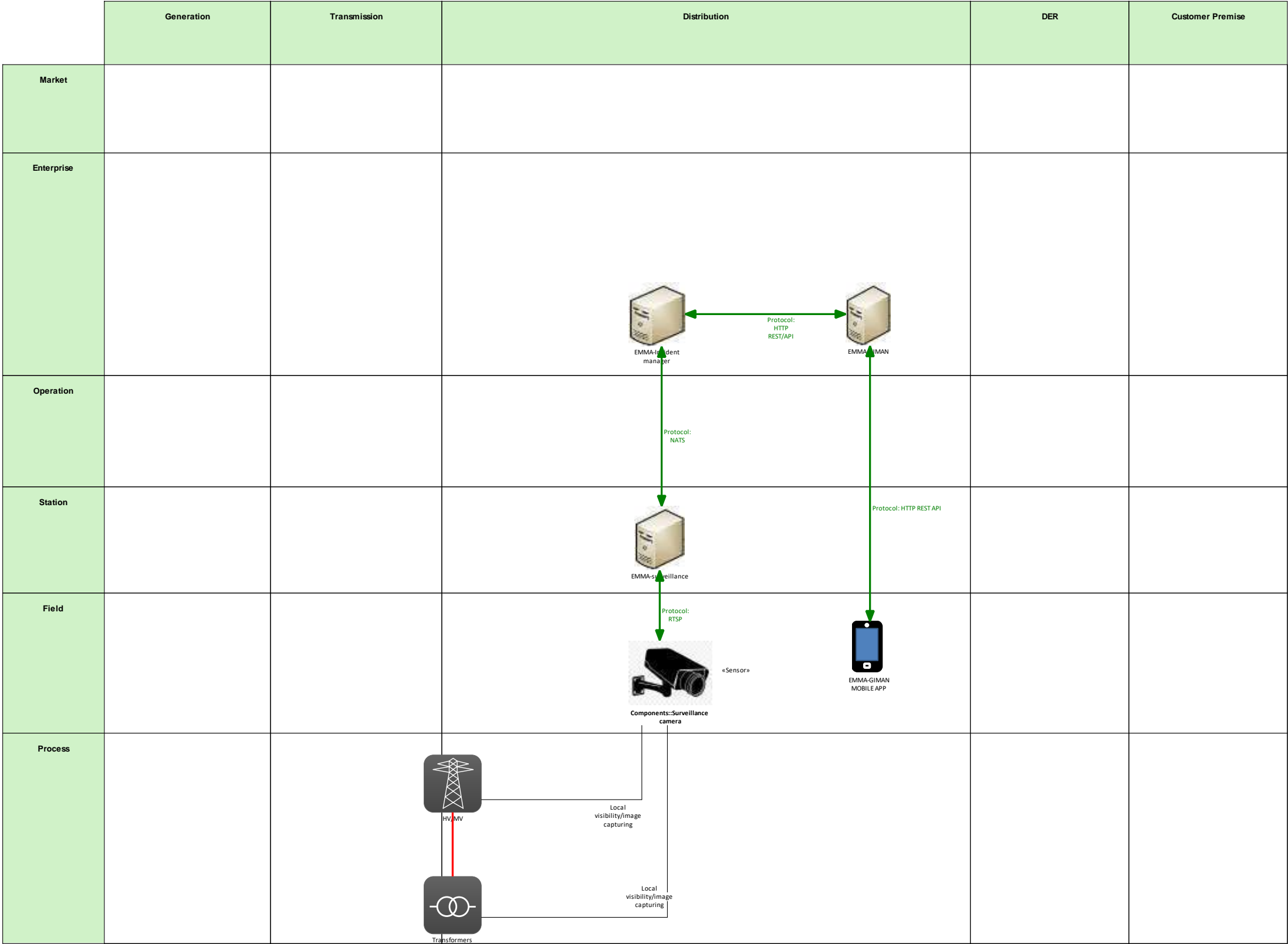


Figure 333 - UC20 Communication Layer

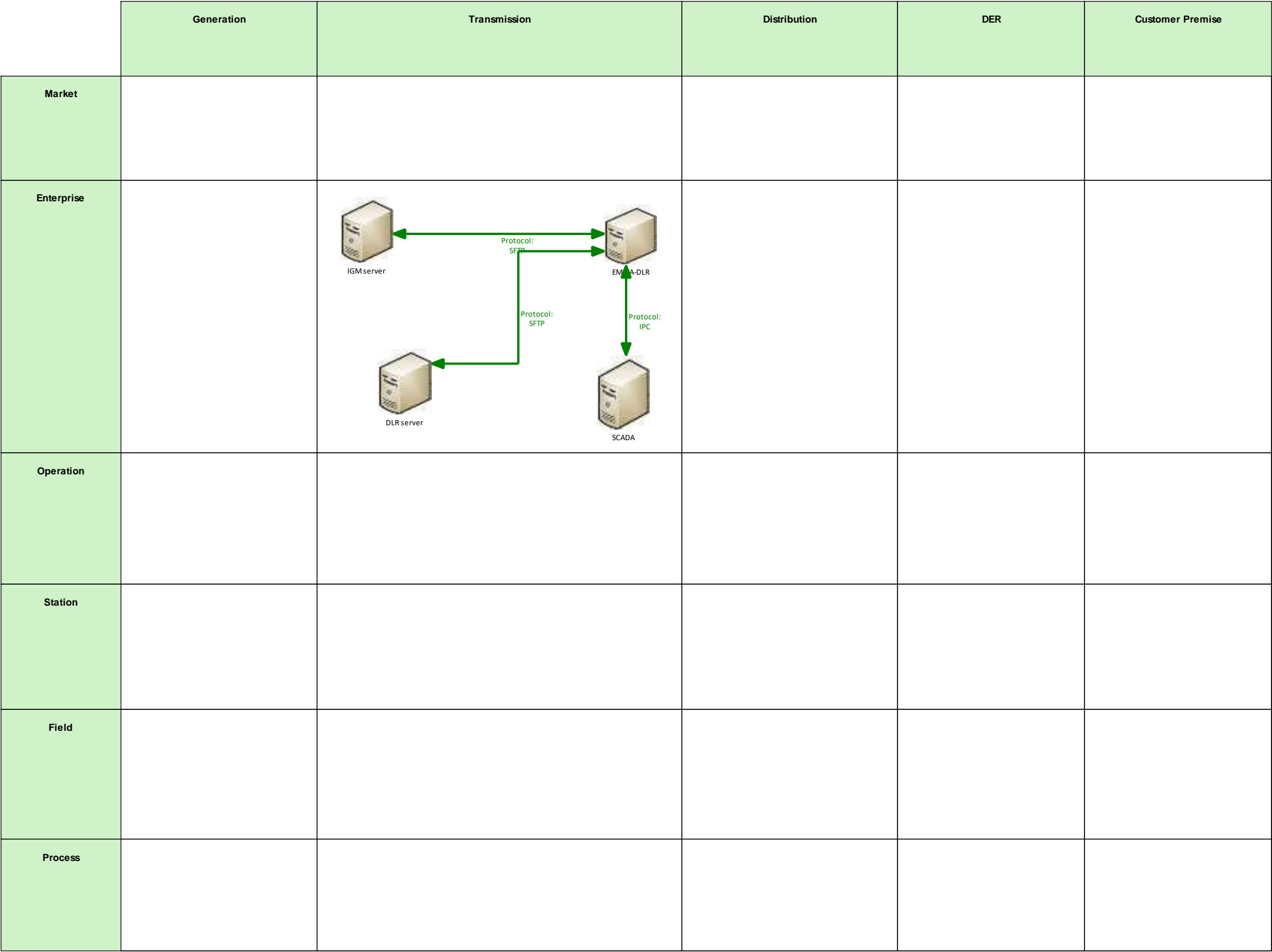


Figure 334 - UC31 Communication Layer

13.4 SGAM COMPONENT LAYER

13.4.1 WP3-C3P0

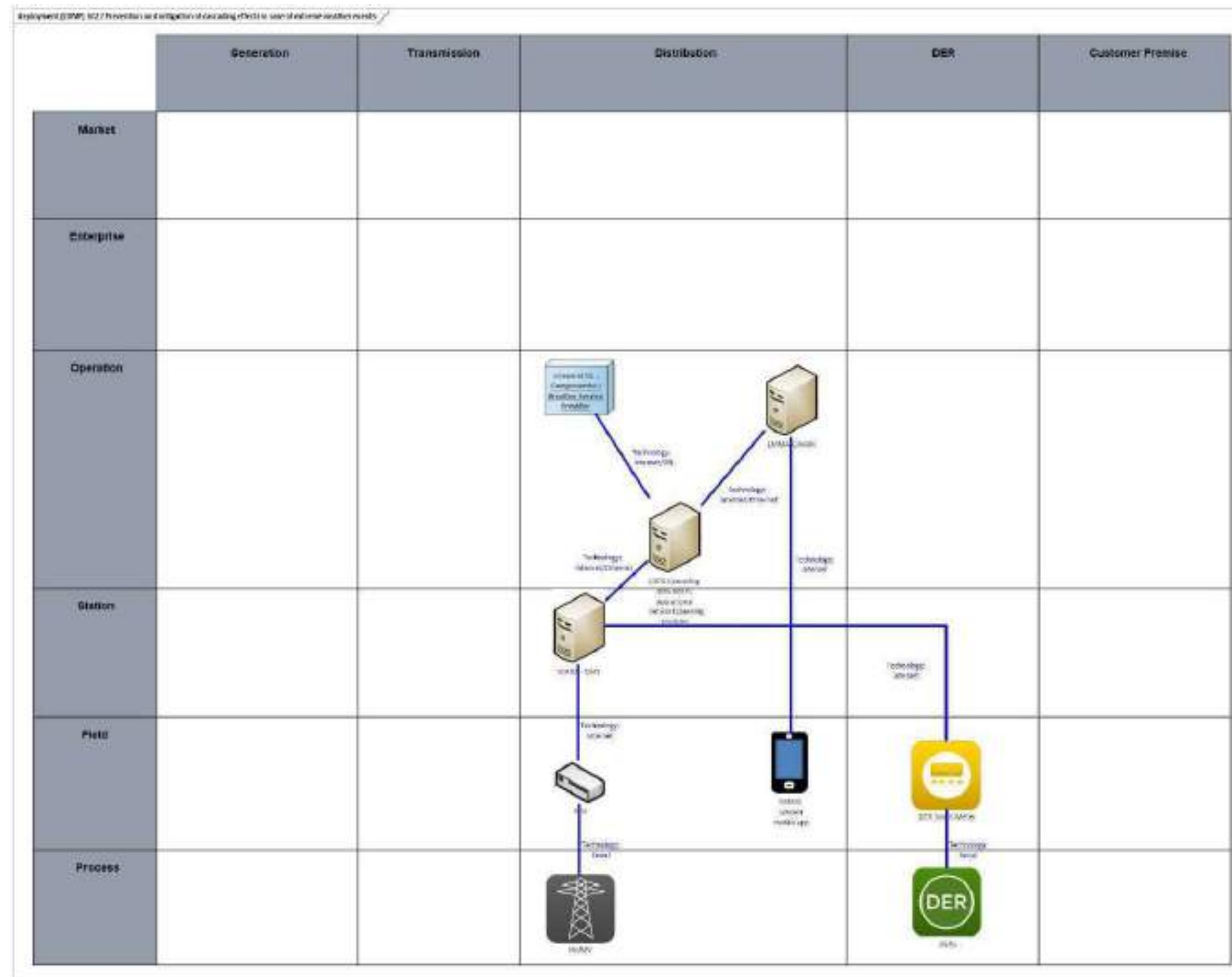


Figure 335 - UC22 Component Layer

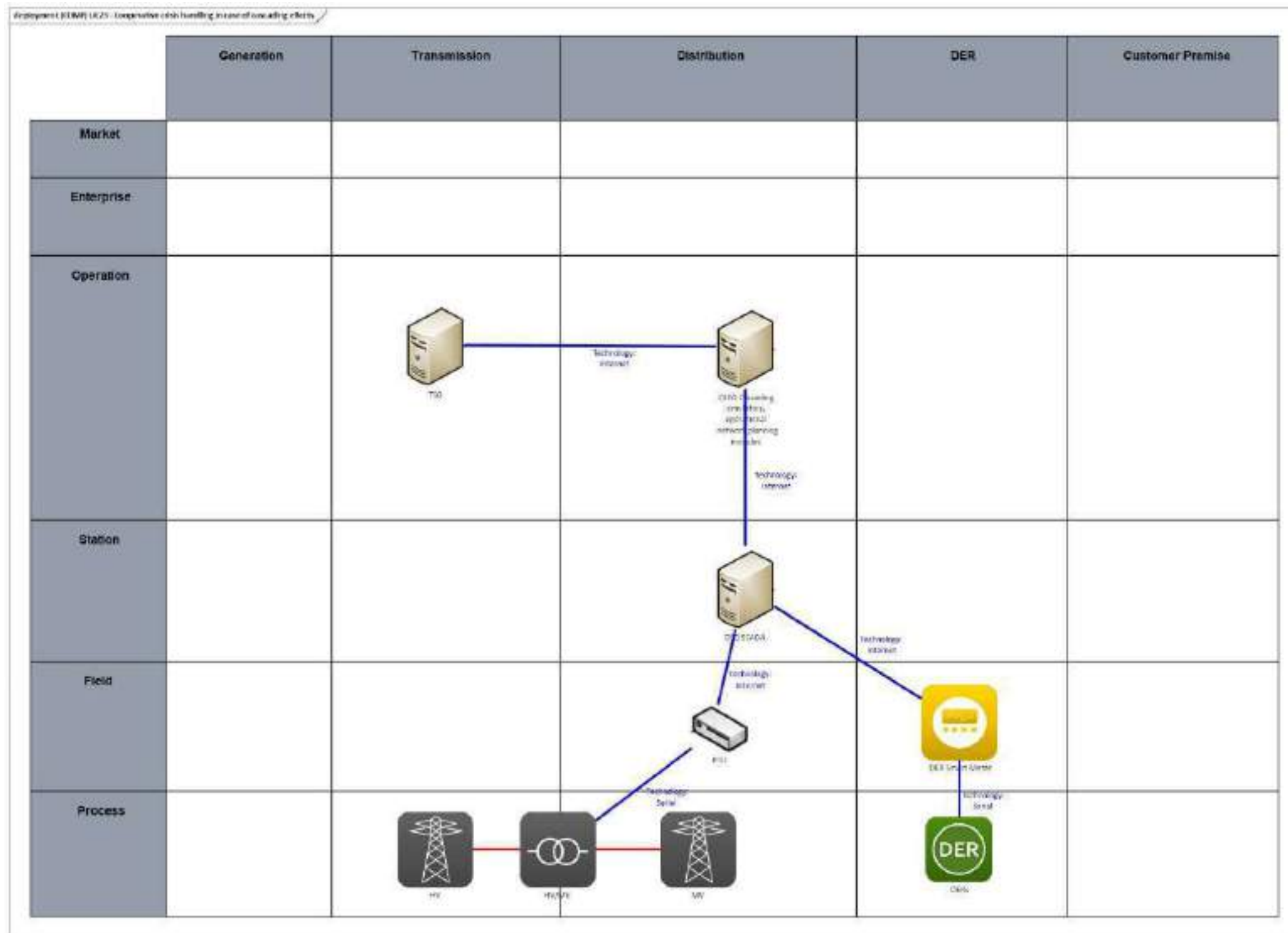


Figure 336 - UC23 Component Layer

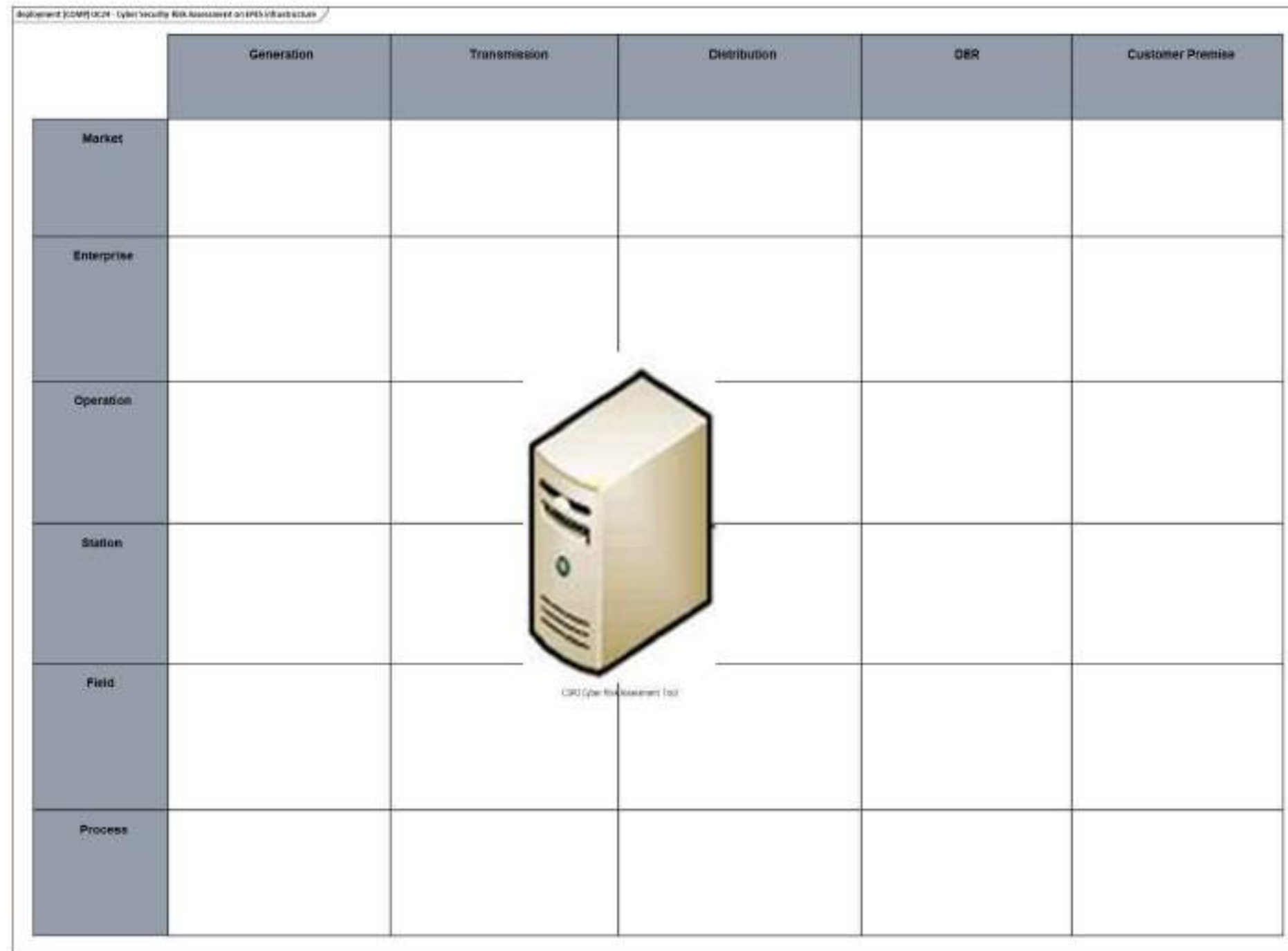


Figure 337 - UC24 Component Layer

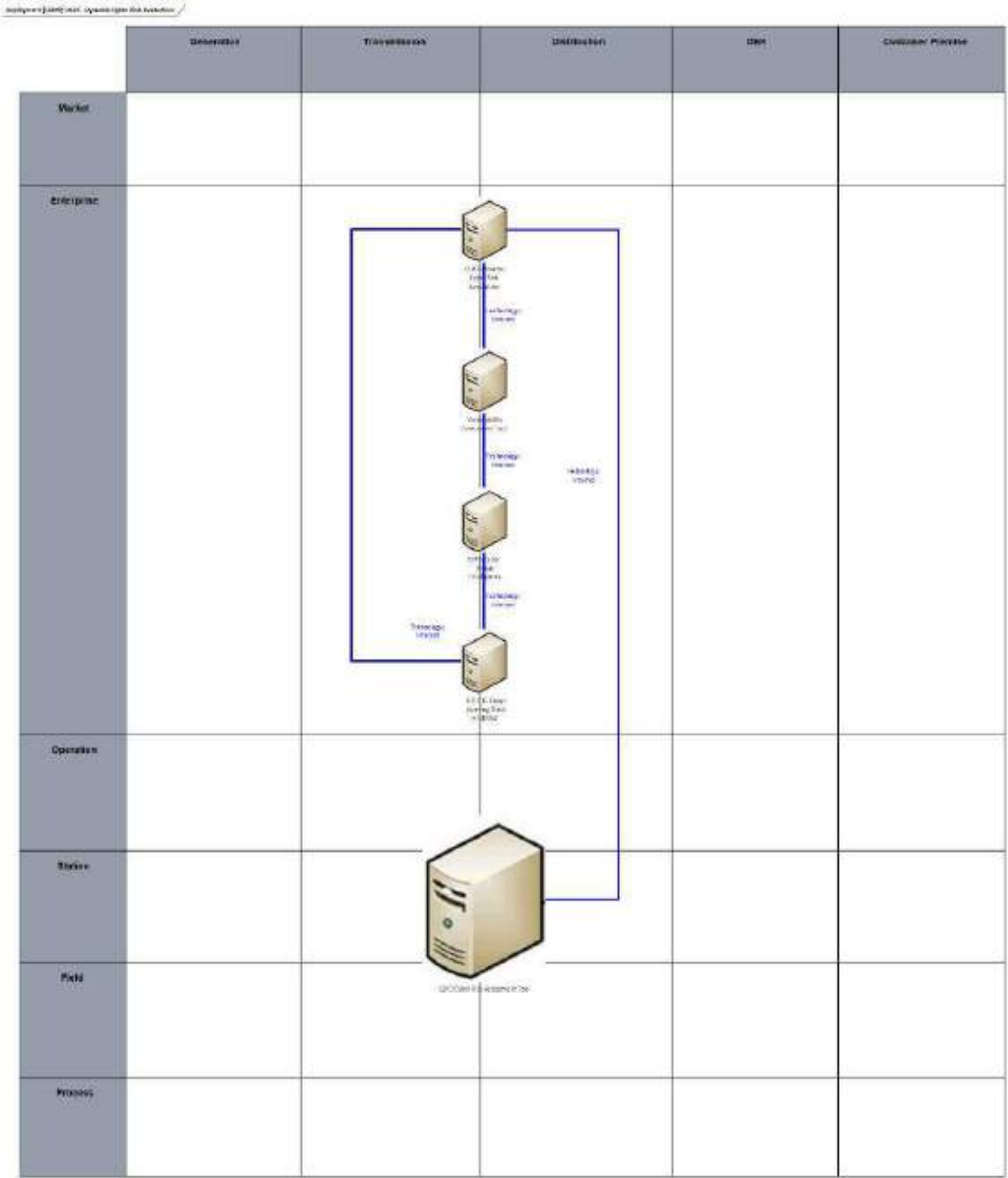


Figure 338 - UC25 Component Layer

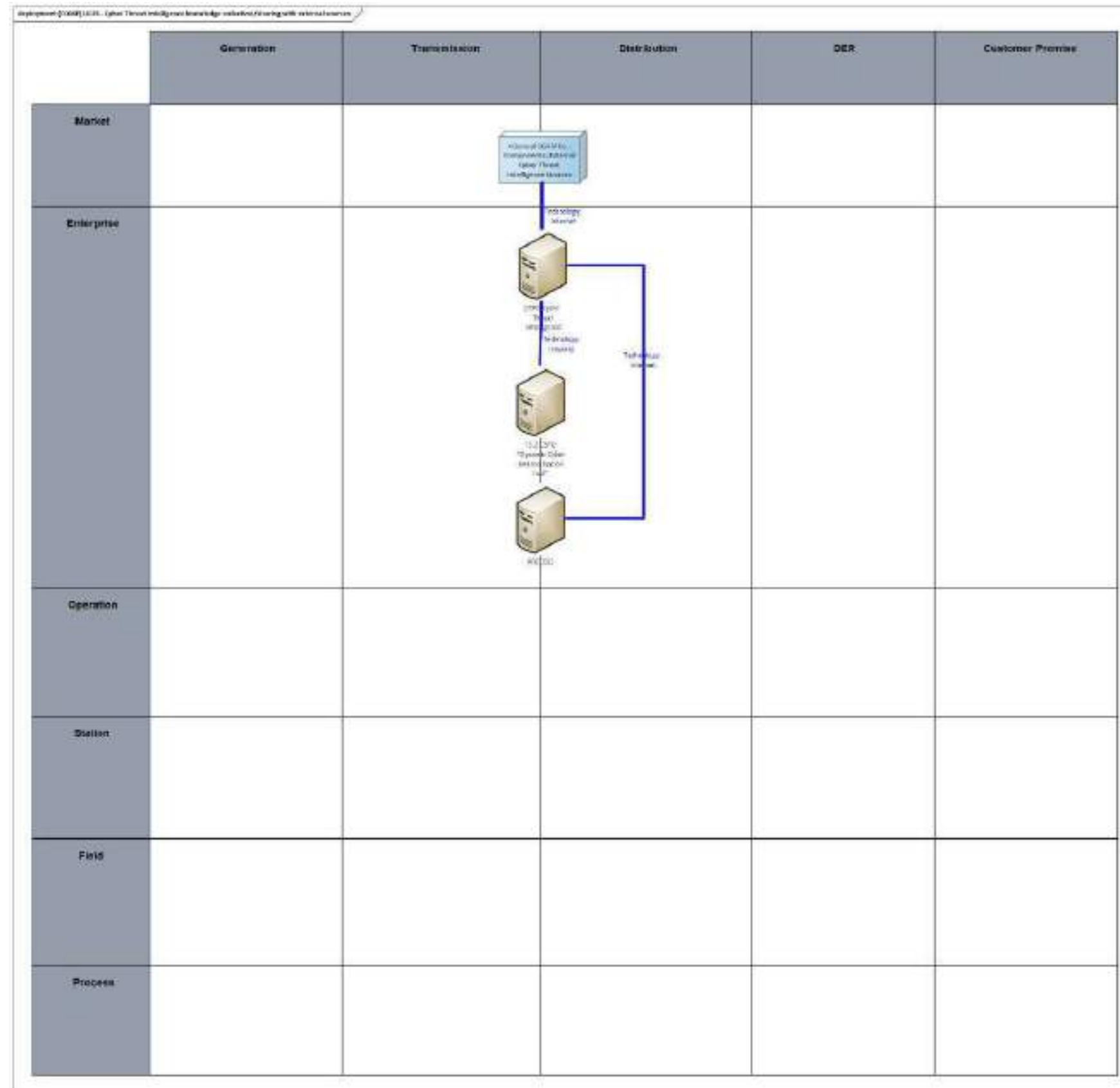


Figure 339 - UC26 Component Layer

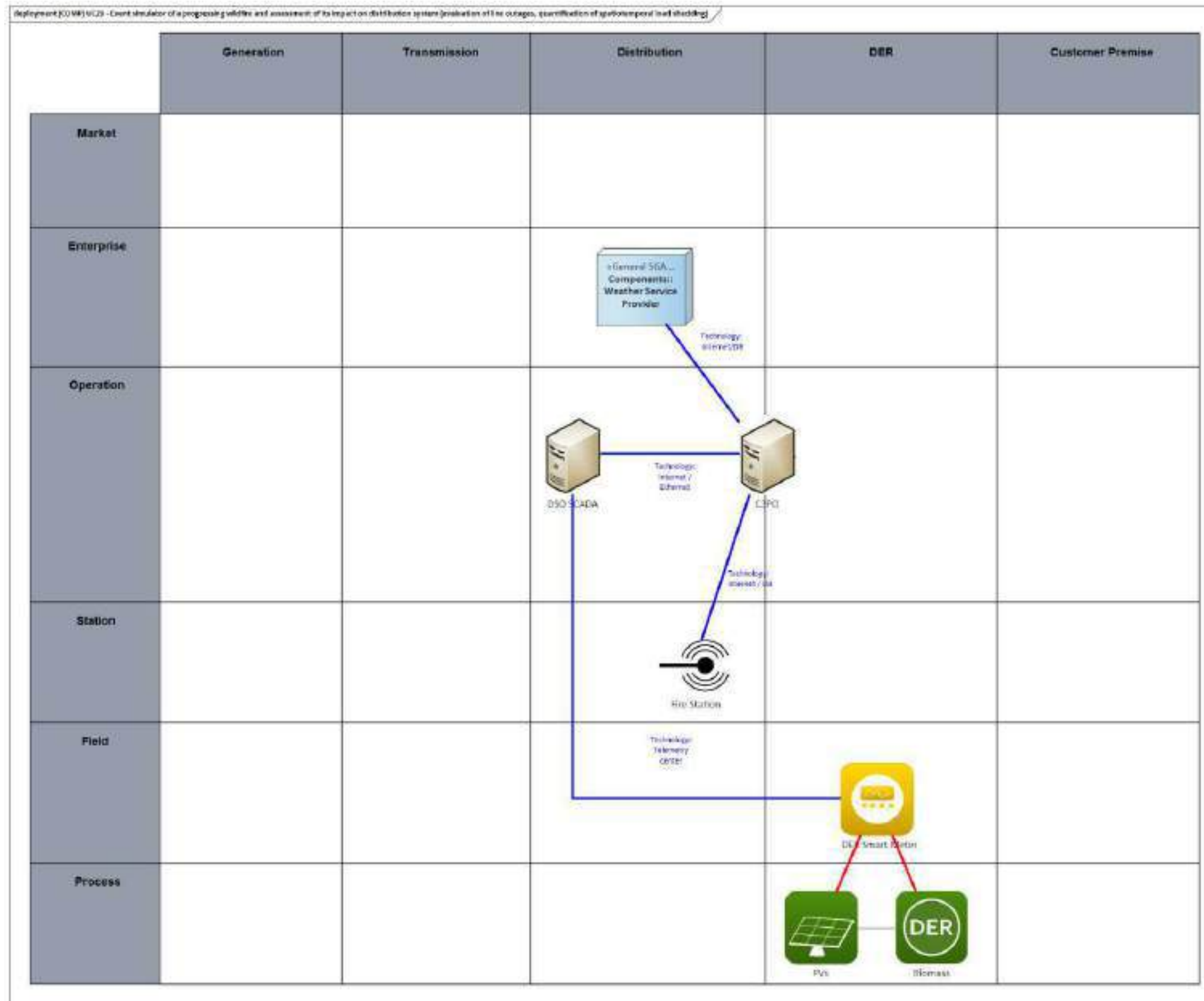


Figure 340 - UC29 Component Layer

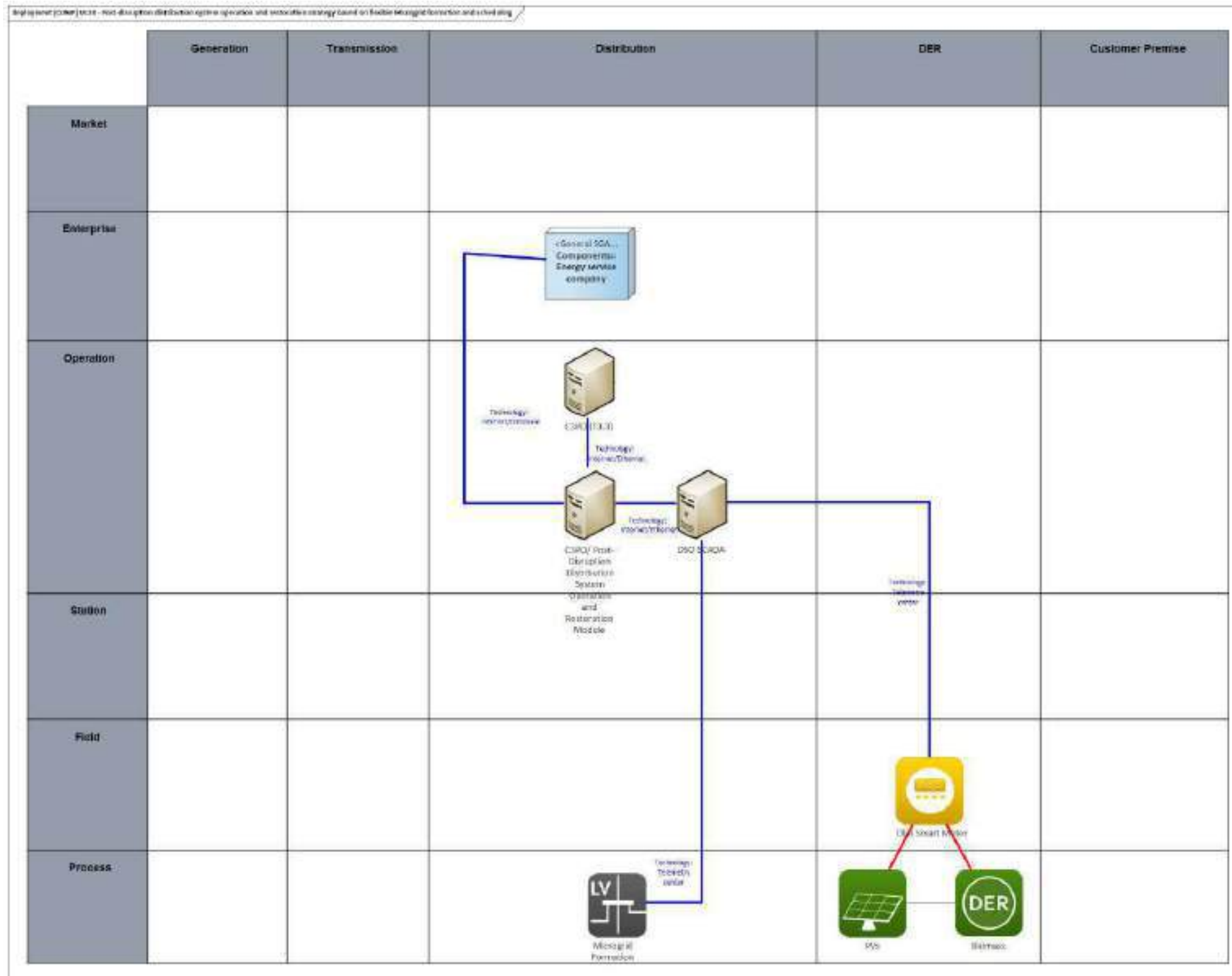


Figure 341 - UC30 Component Layer

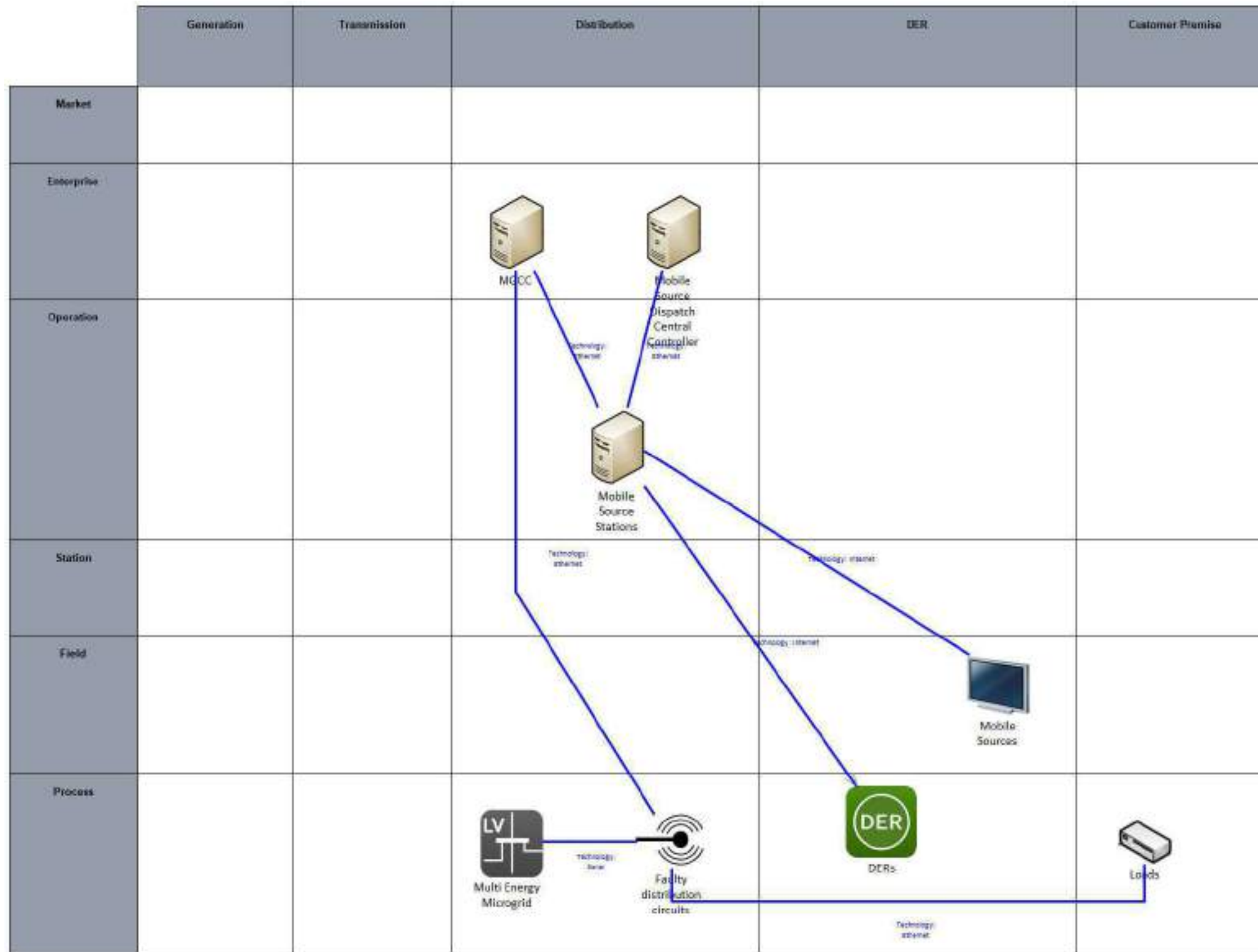


Figure 342 - UC32 Component Layer

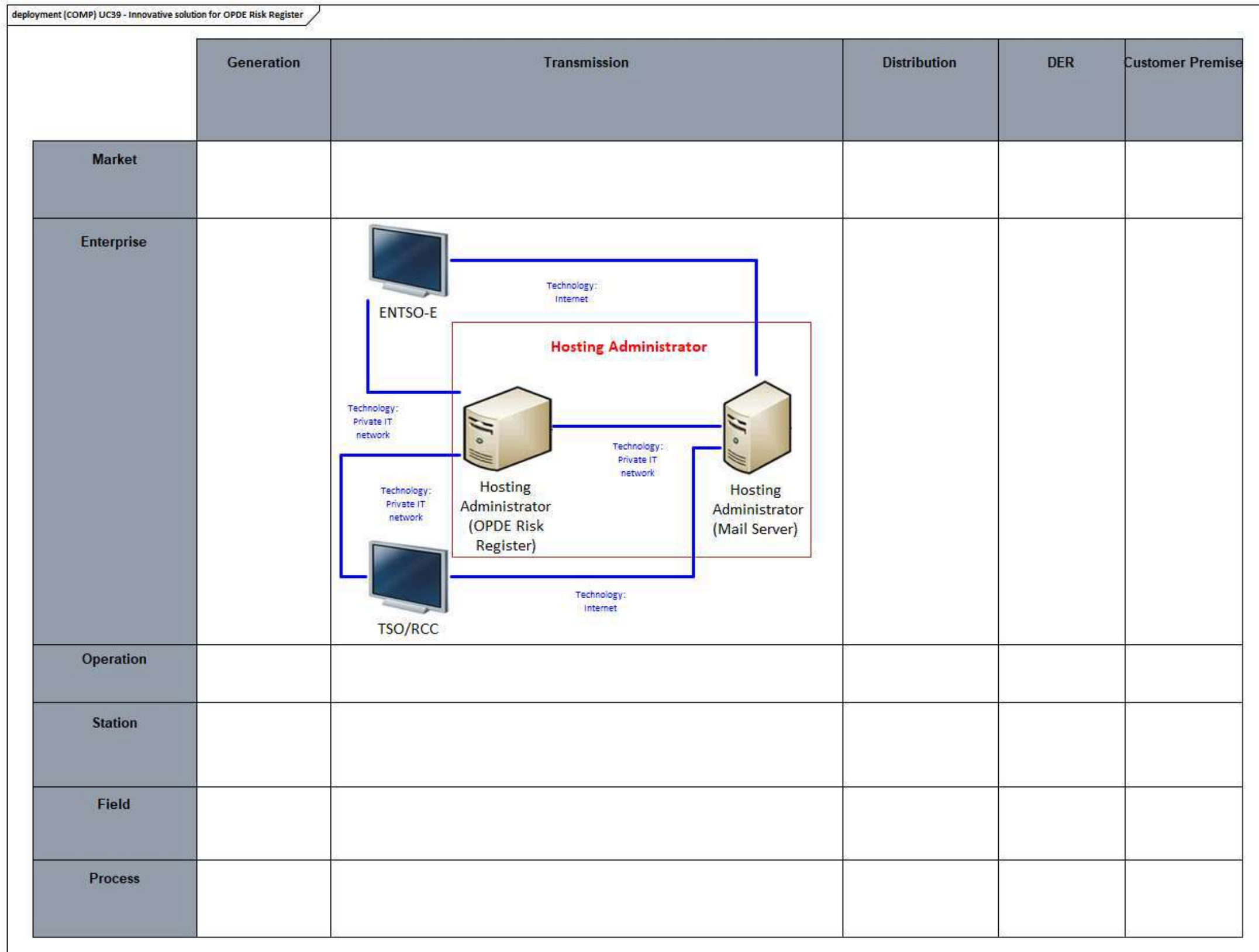


Figure 343 - UC39 Component Layer



13.4.2 WP4-IRIS

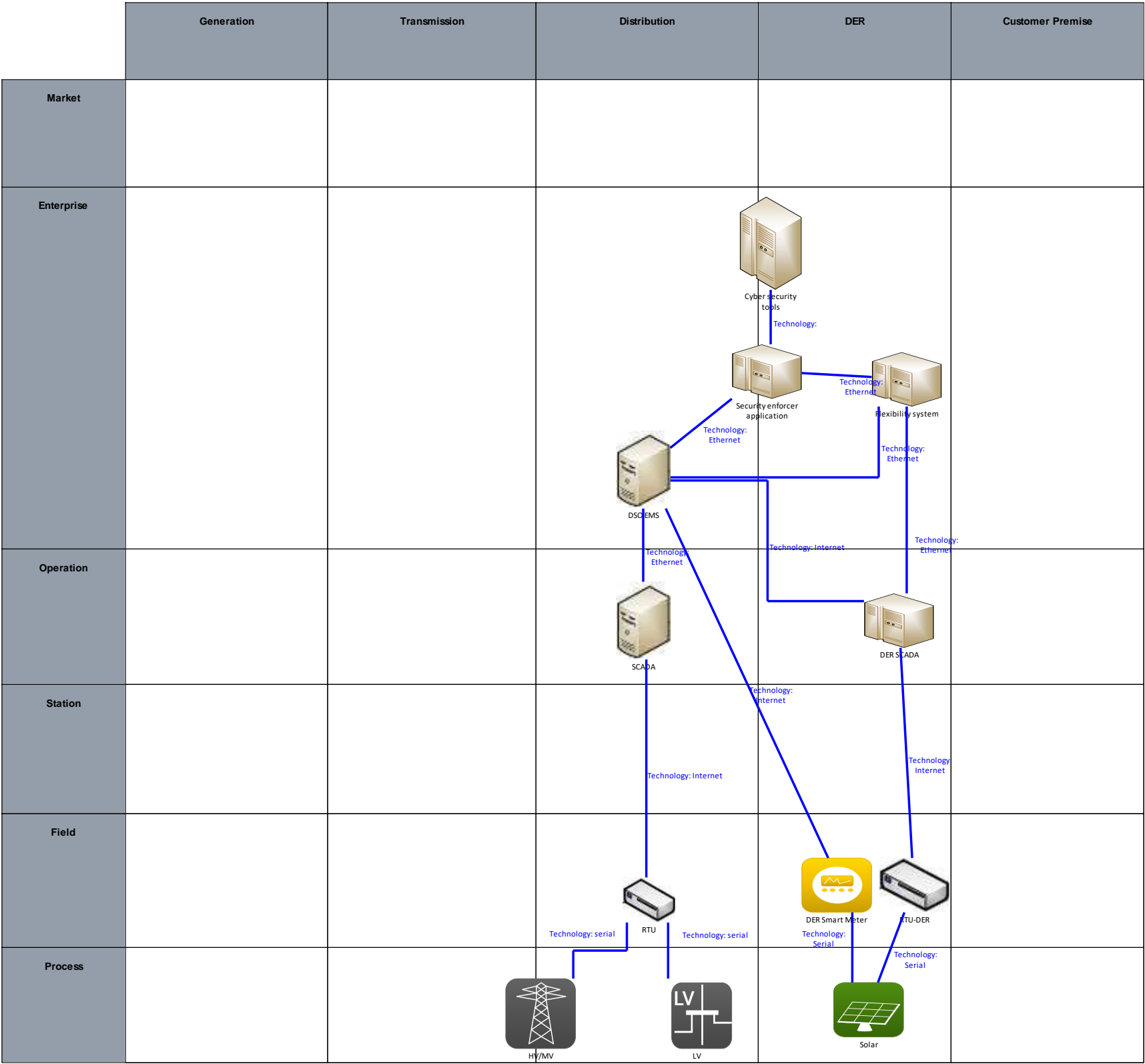


Figure 344 - UC07 Component Layer

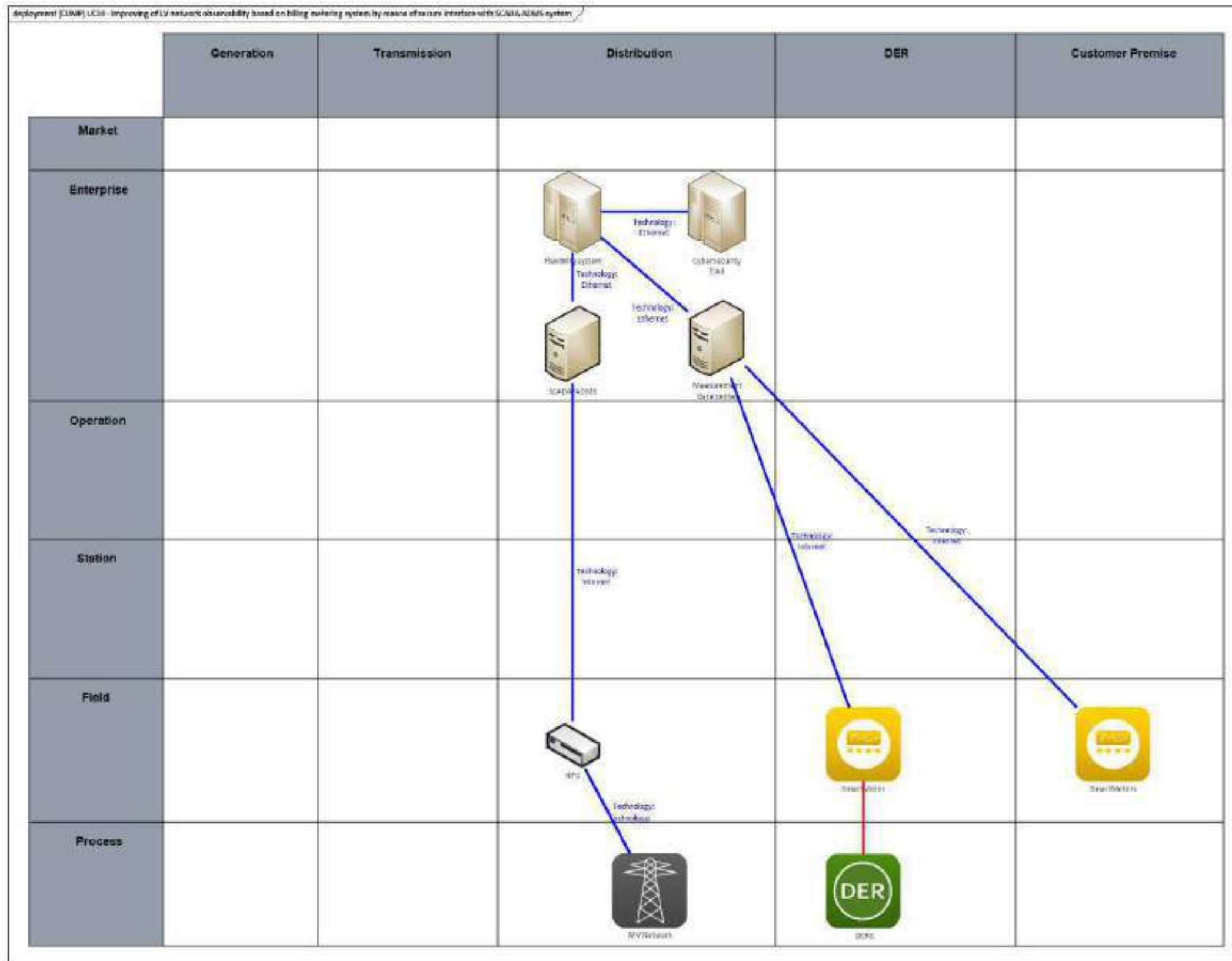


Figure 345 - UC10 Component Layer

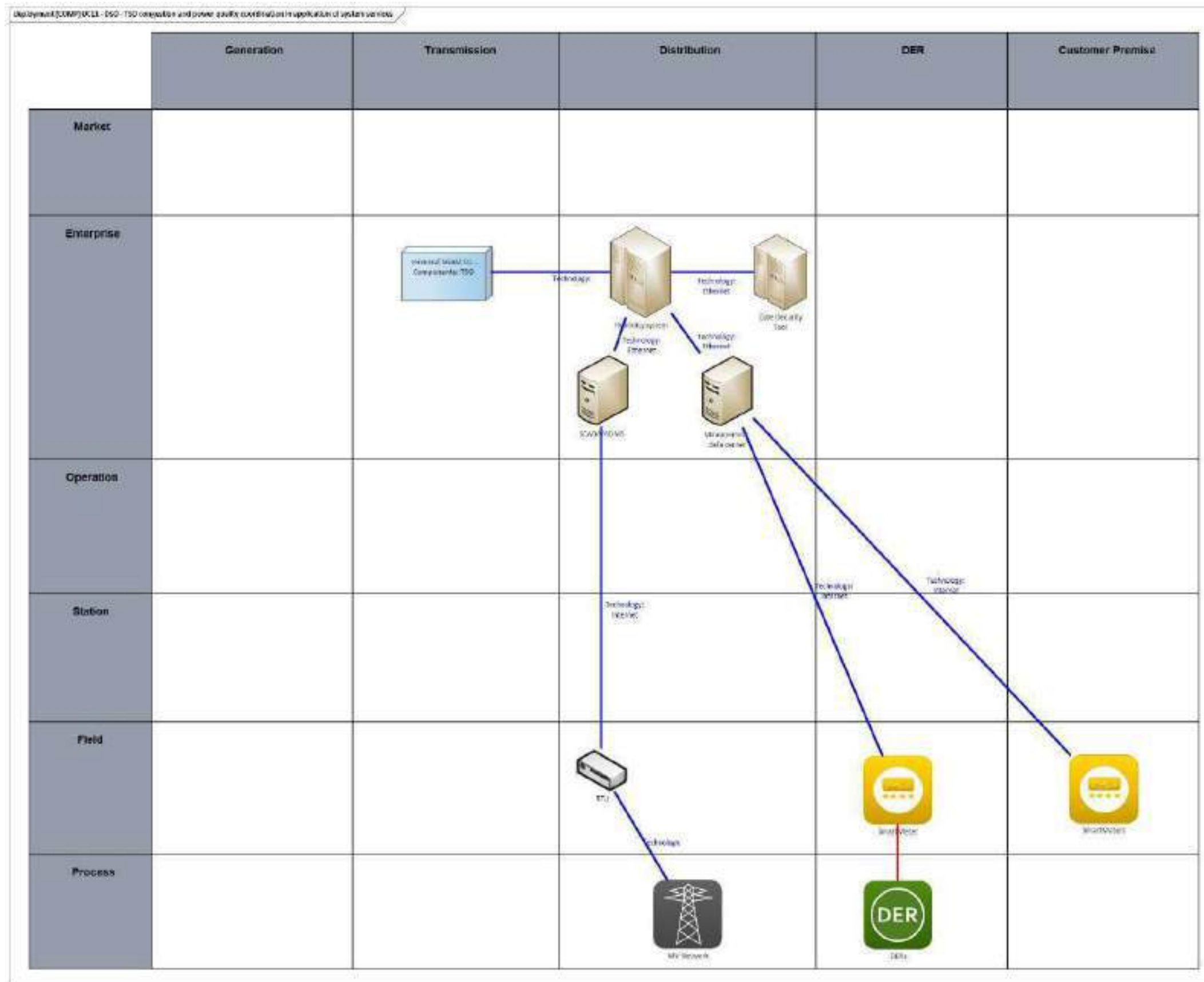


Figure 346 - UC11 Component Layer

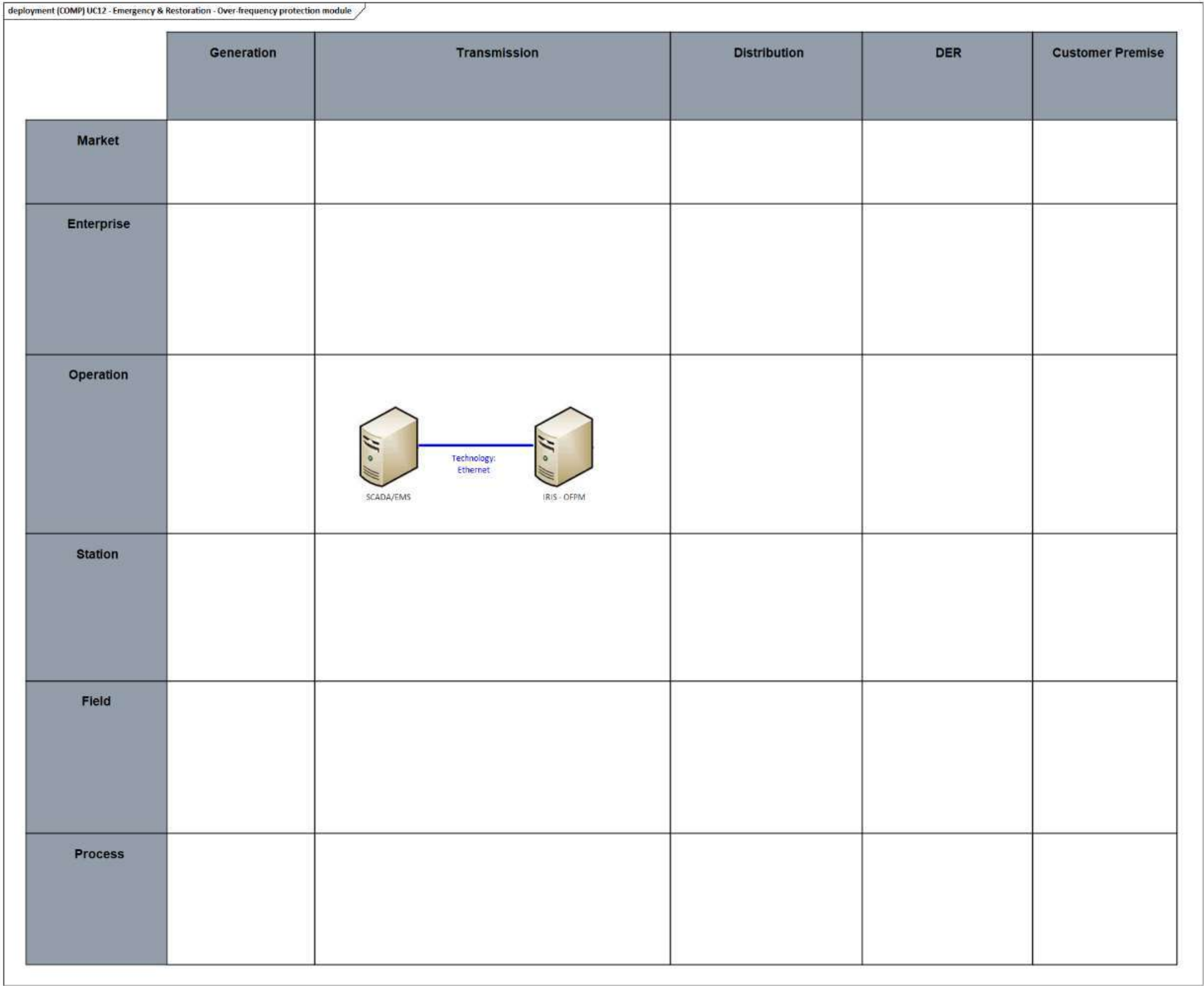


Figure 347 – UC12 Component Layer

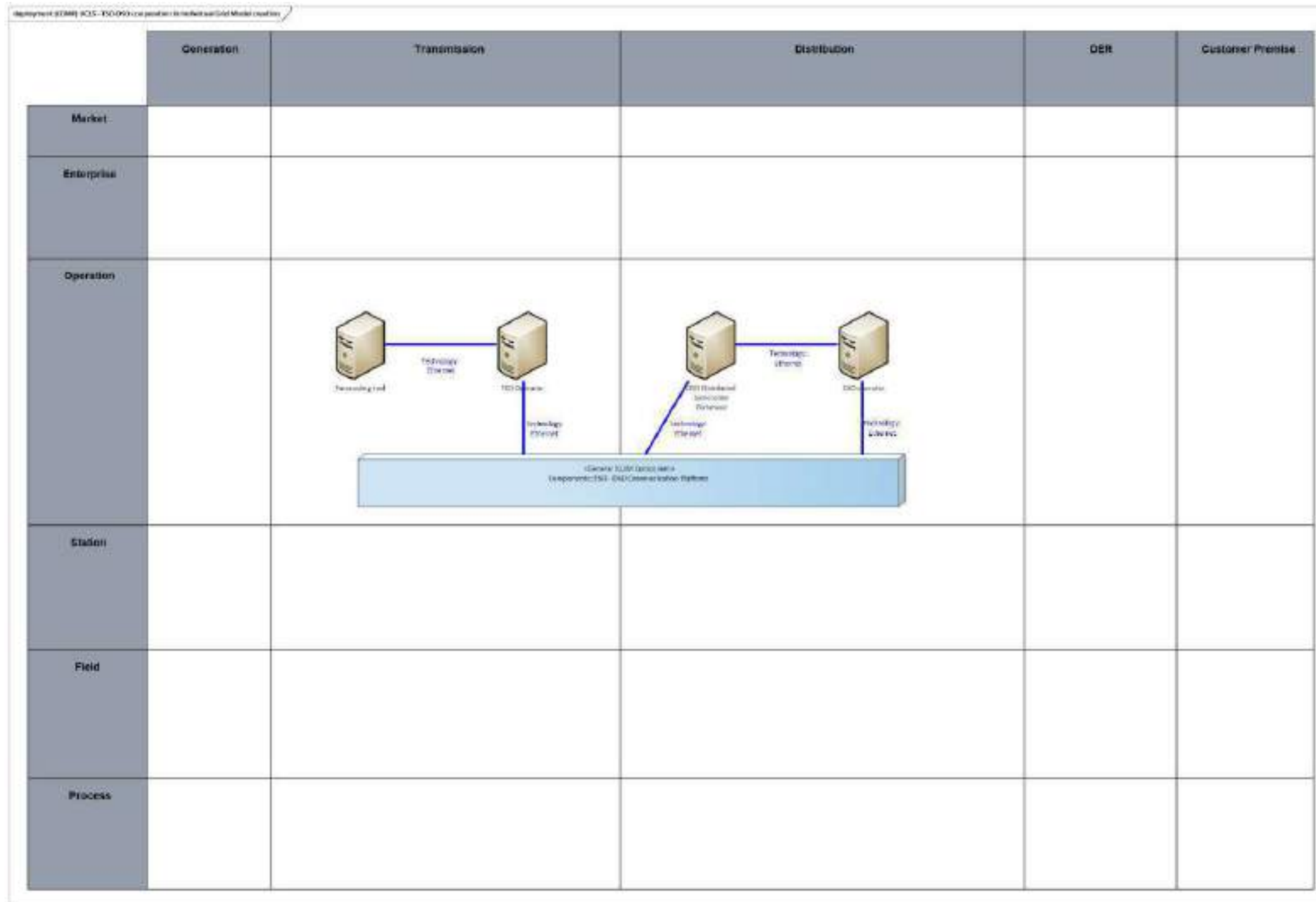


Figure 348 - UC15 Component Layer

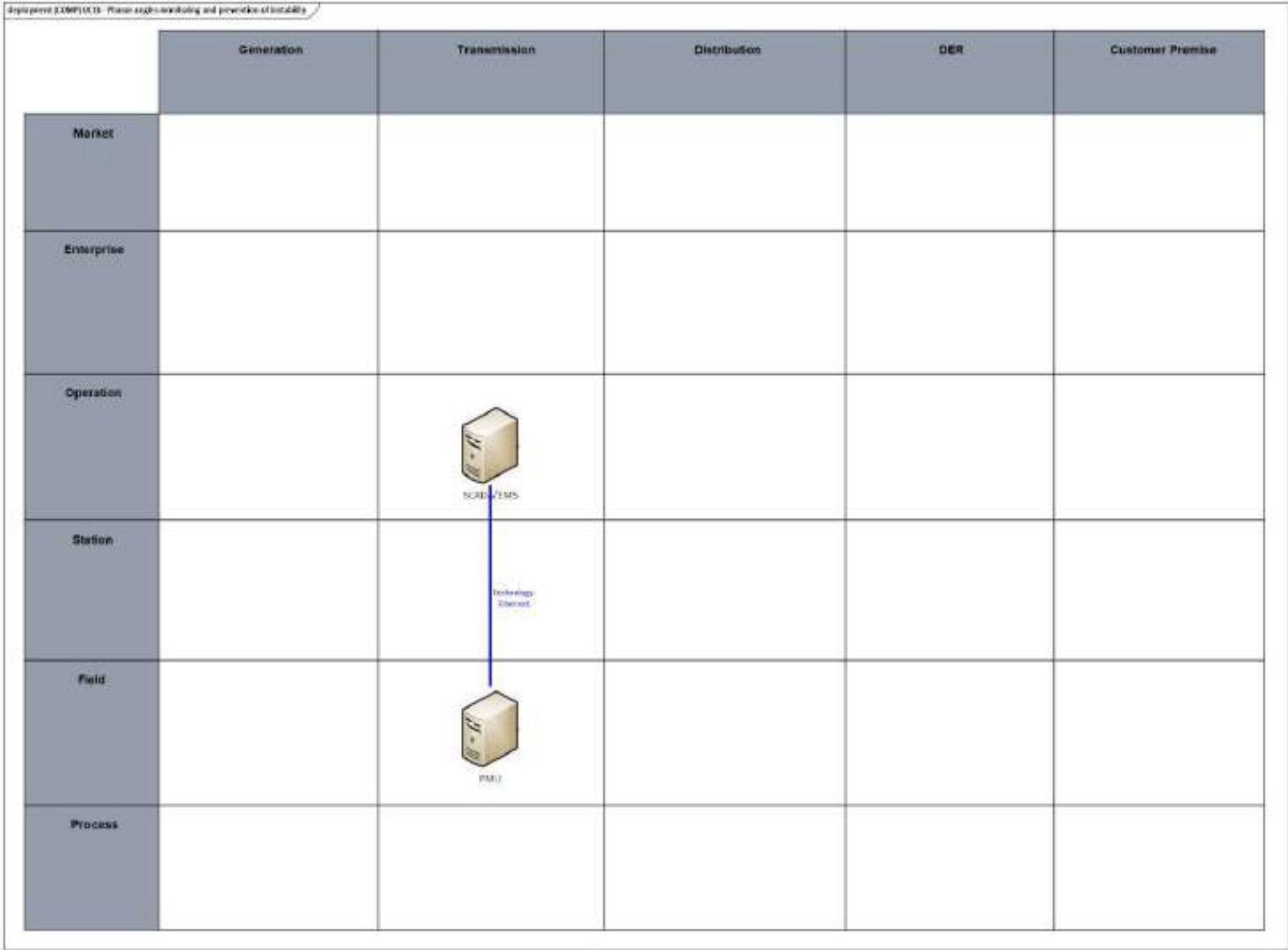


Figure 349 - UC16 Component Layer

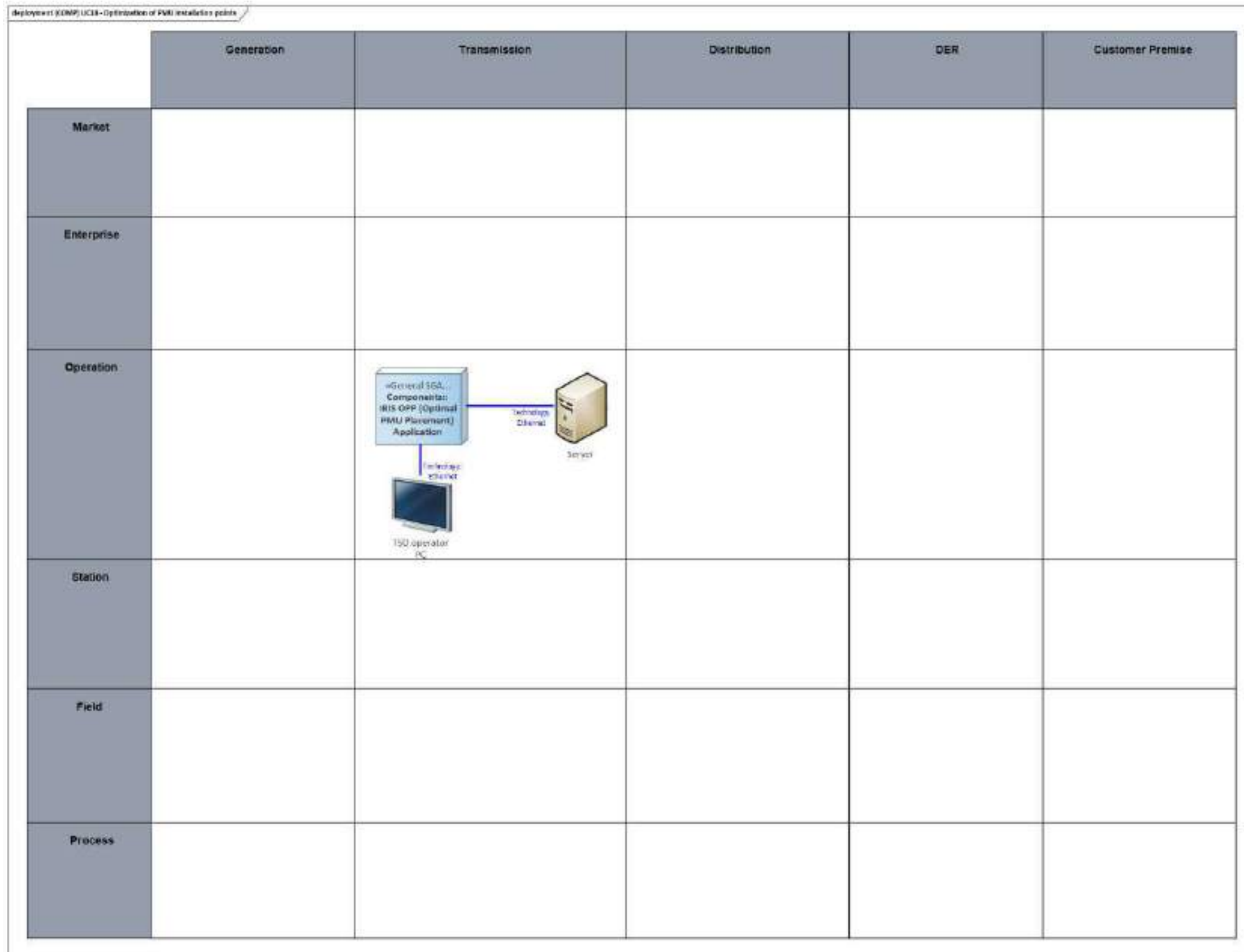


Figure 350 - UC18 Component Layer

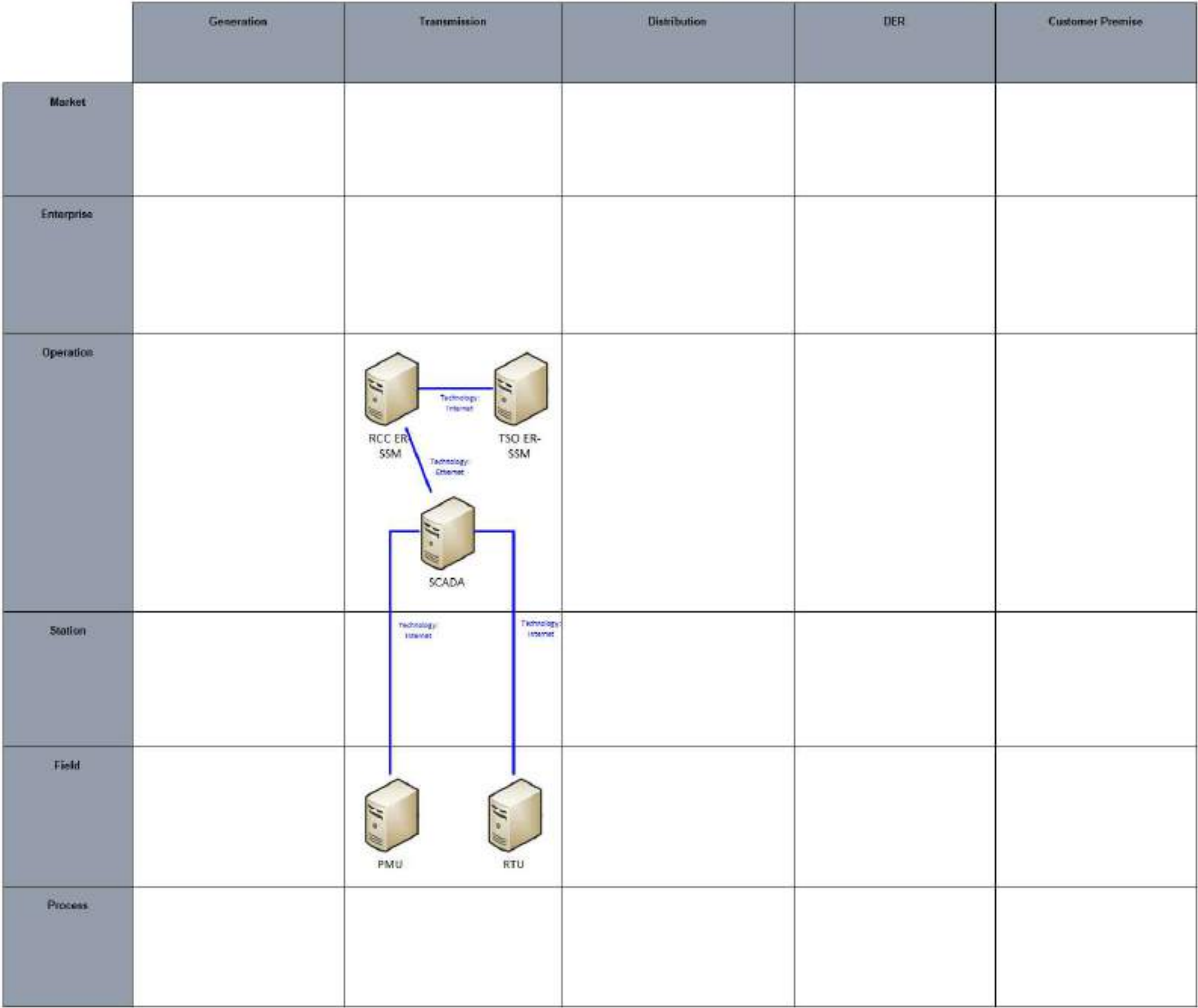


Figure 351 – UC19 Component Layer

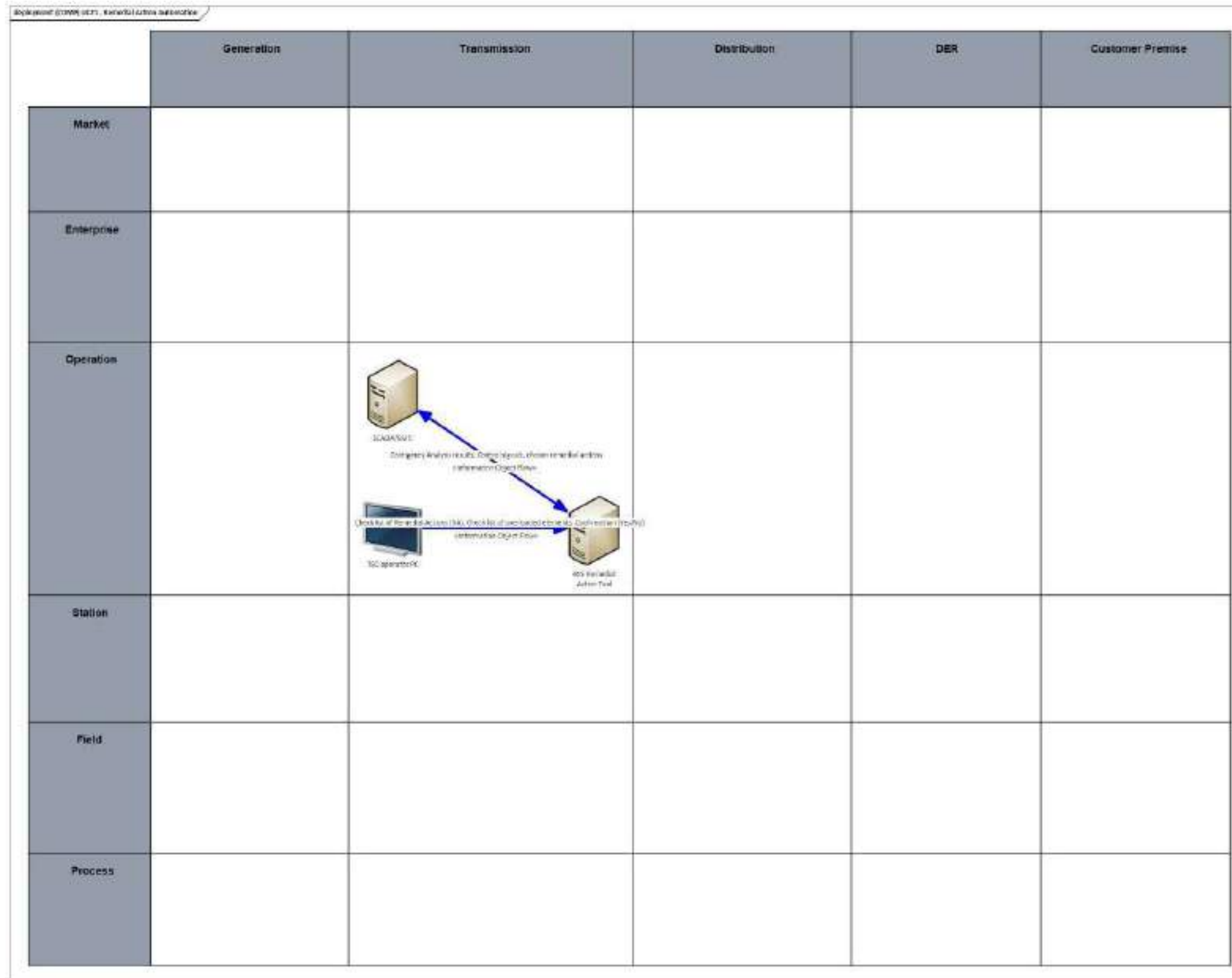
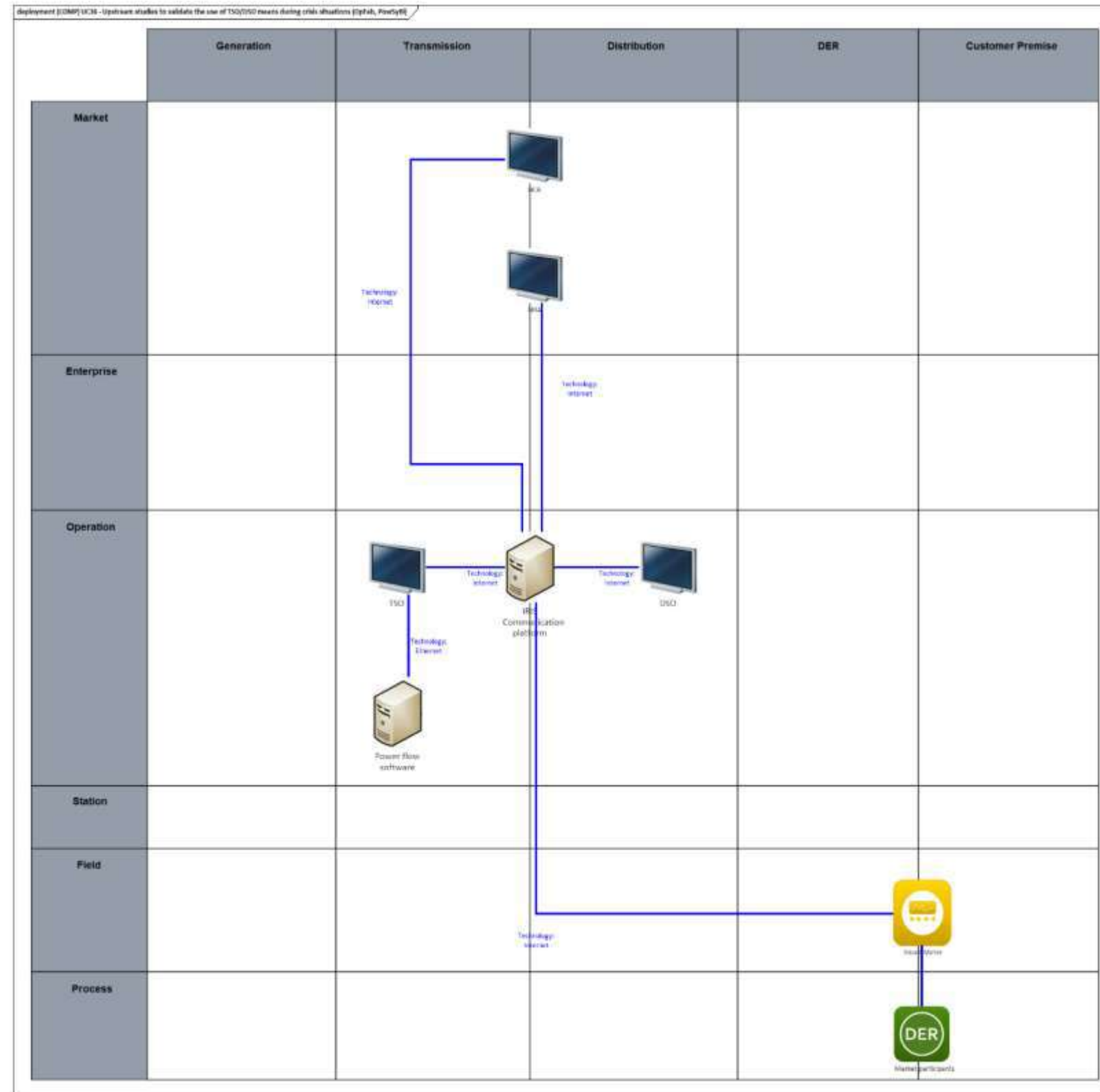


Figure 352 - UC21 Component Layer





13.4.3 WP5-PRECOG

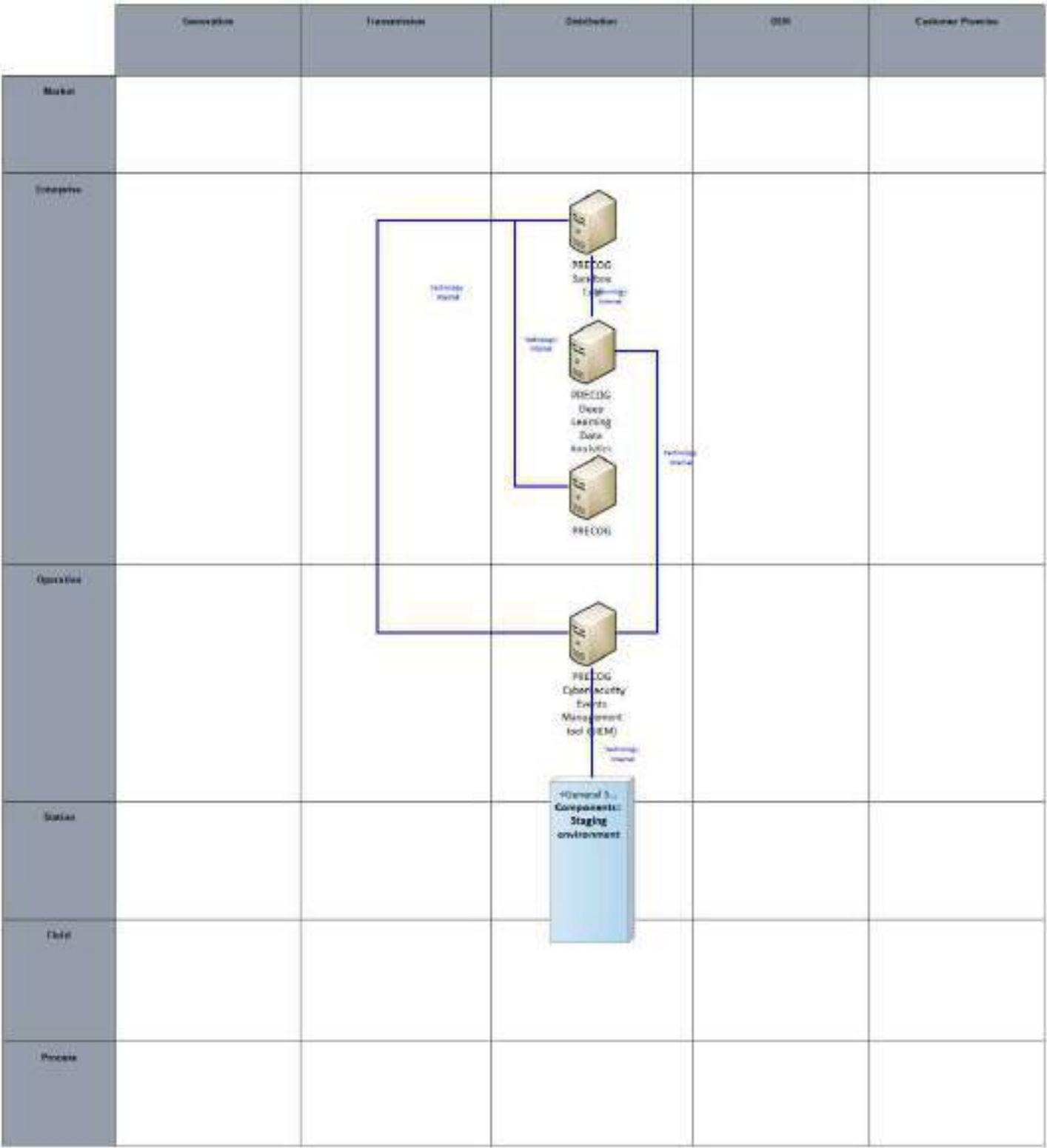


Figure 354 - UC27 Component Layer

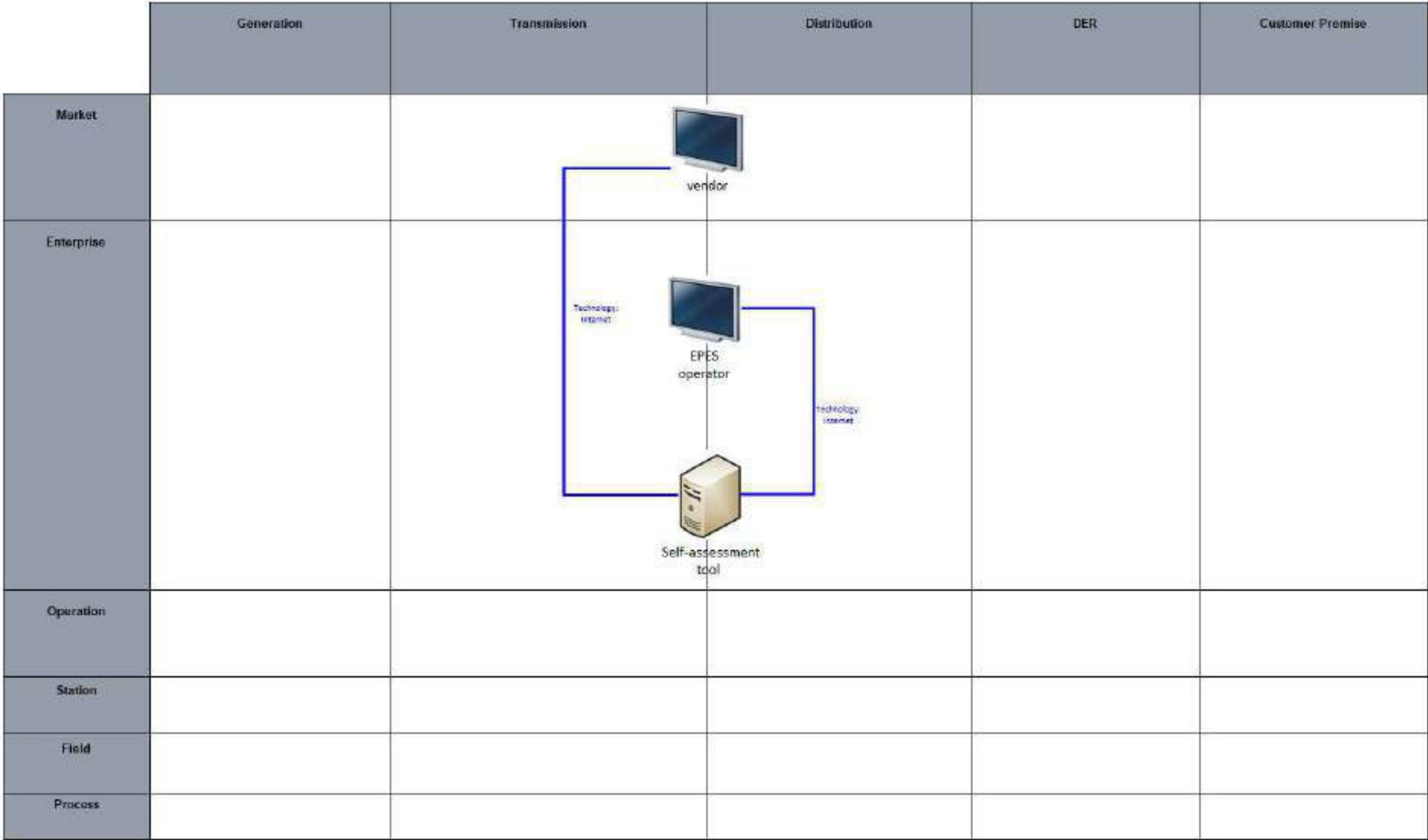


Figure 355 - UC36 Component Layer

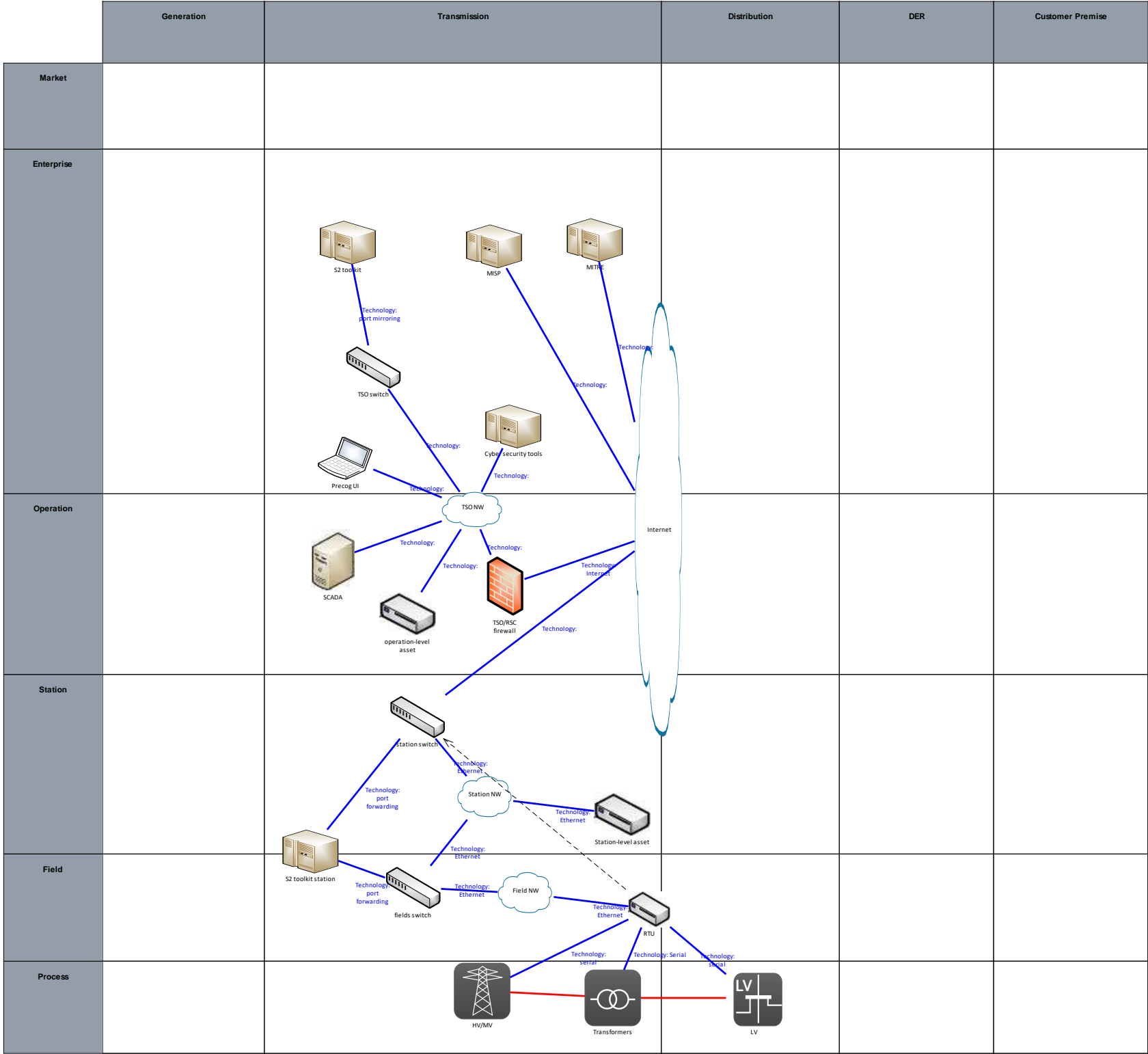


Figure 356 - UC33 Component Layer

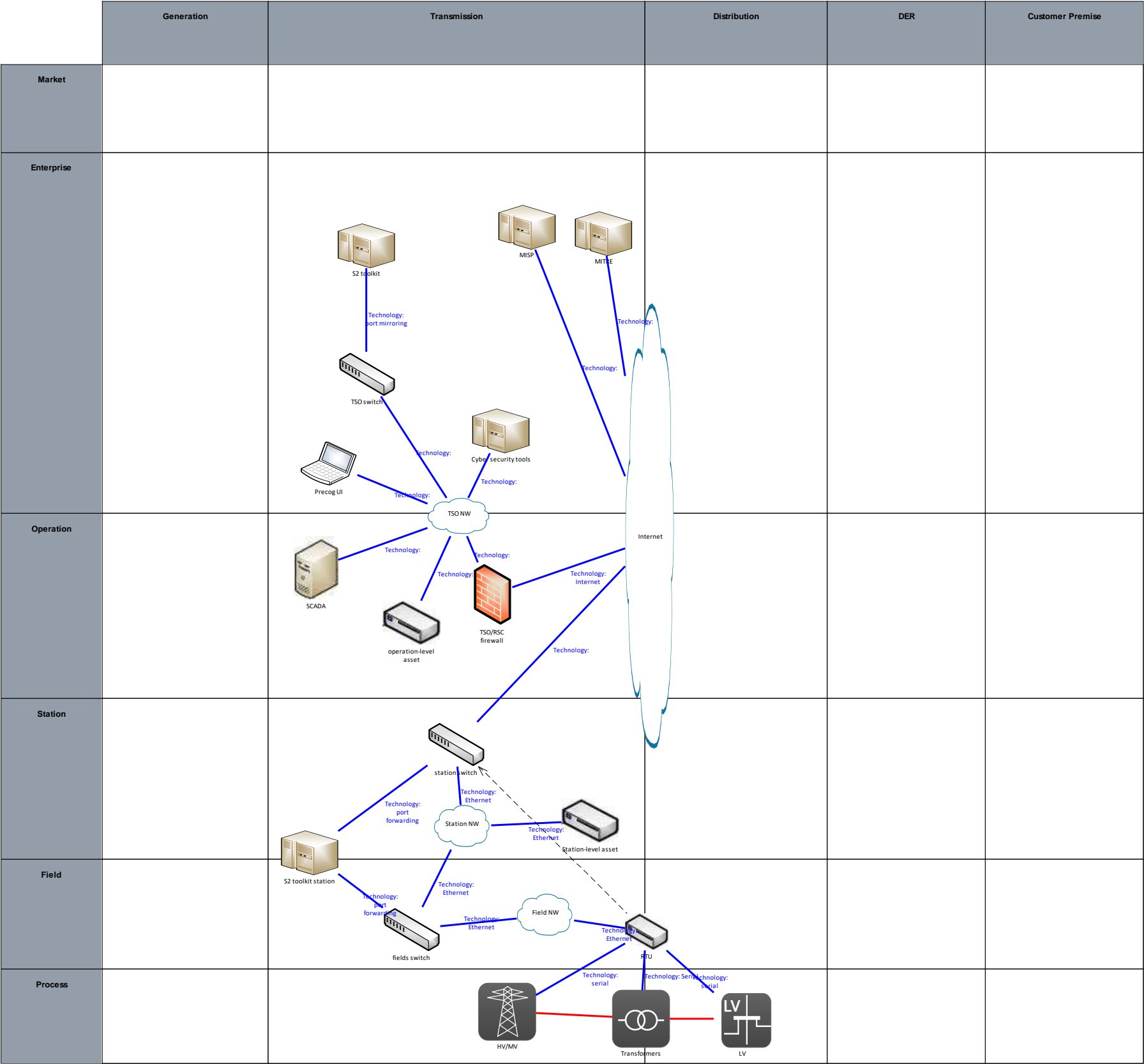


Figure 357 – UC34 Component Layer



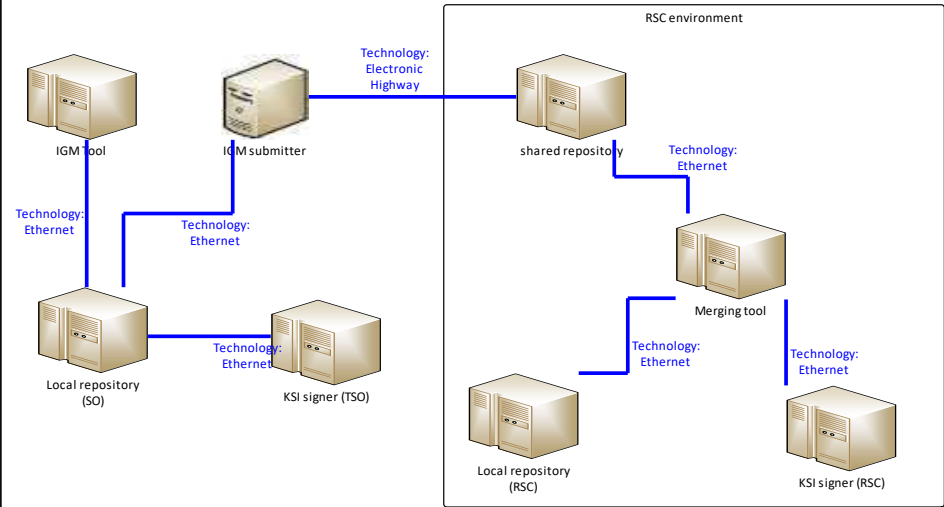
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 358 - UC36 Component Layer

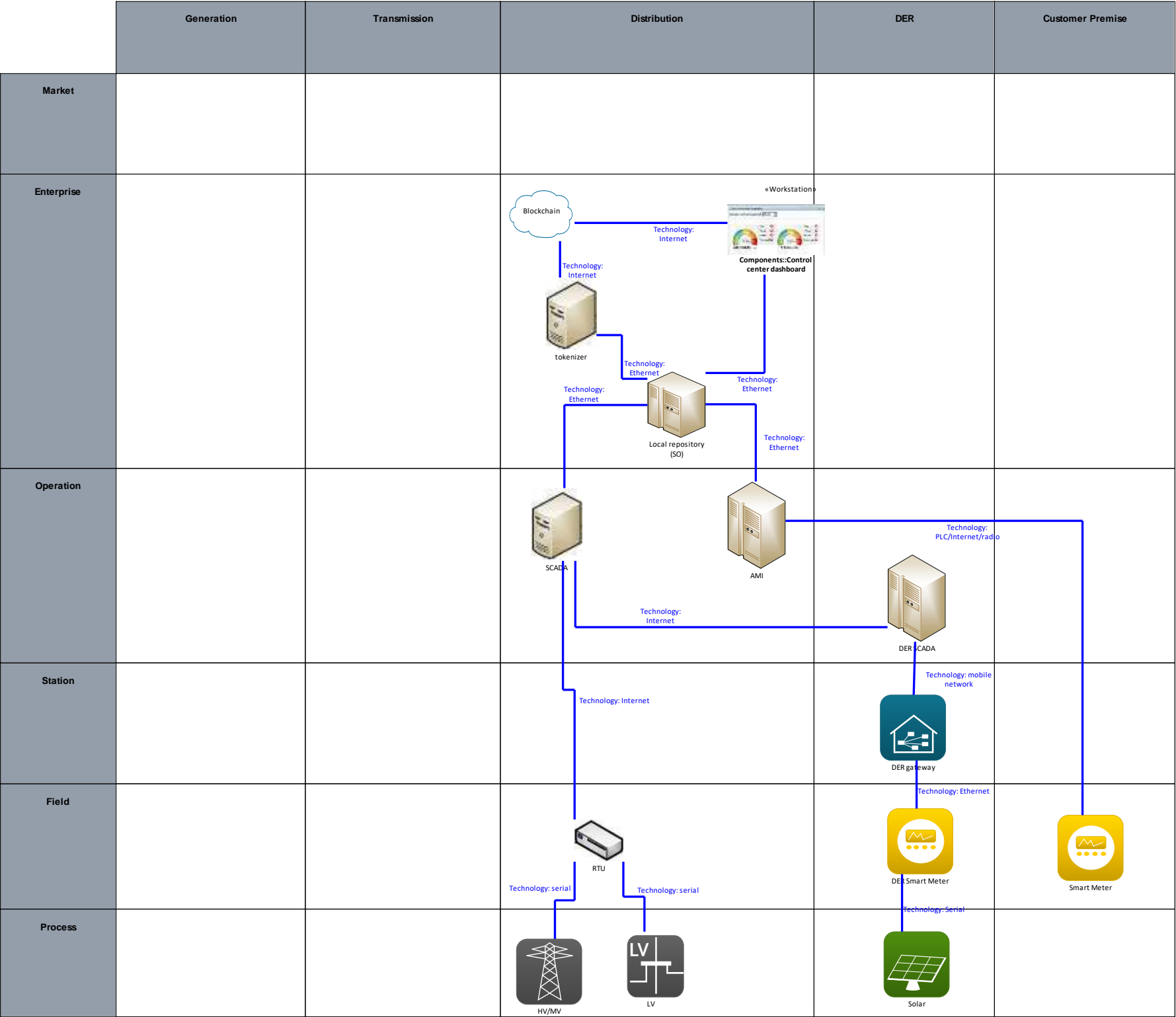


Figure 359 - UC37 Component Layer

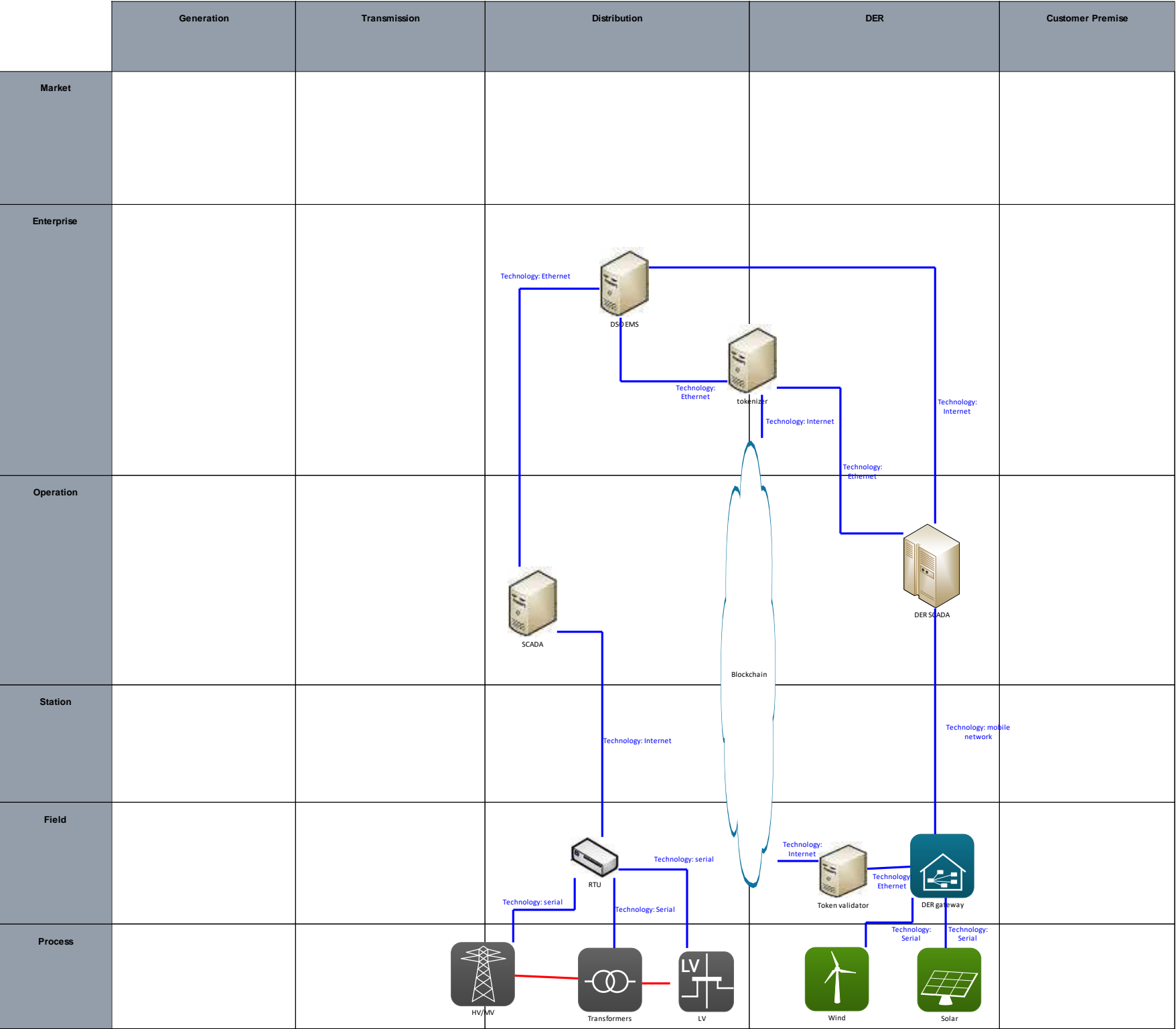


Figure 360 - UC38 Component Layer

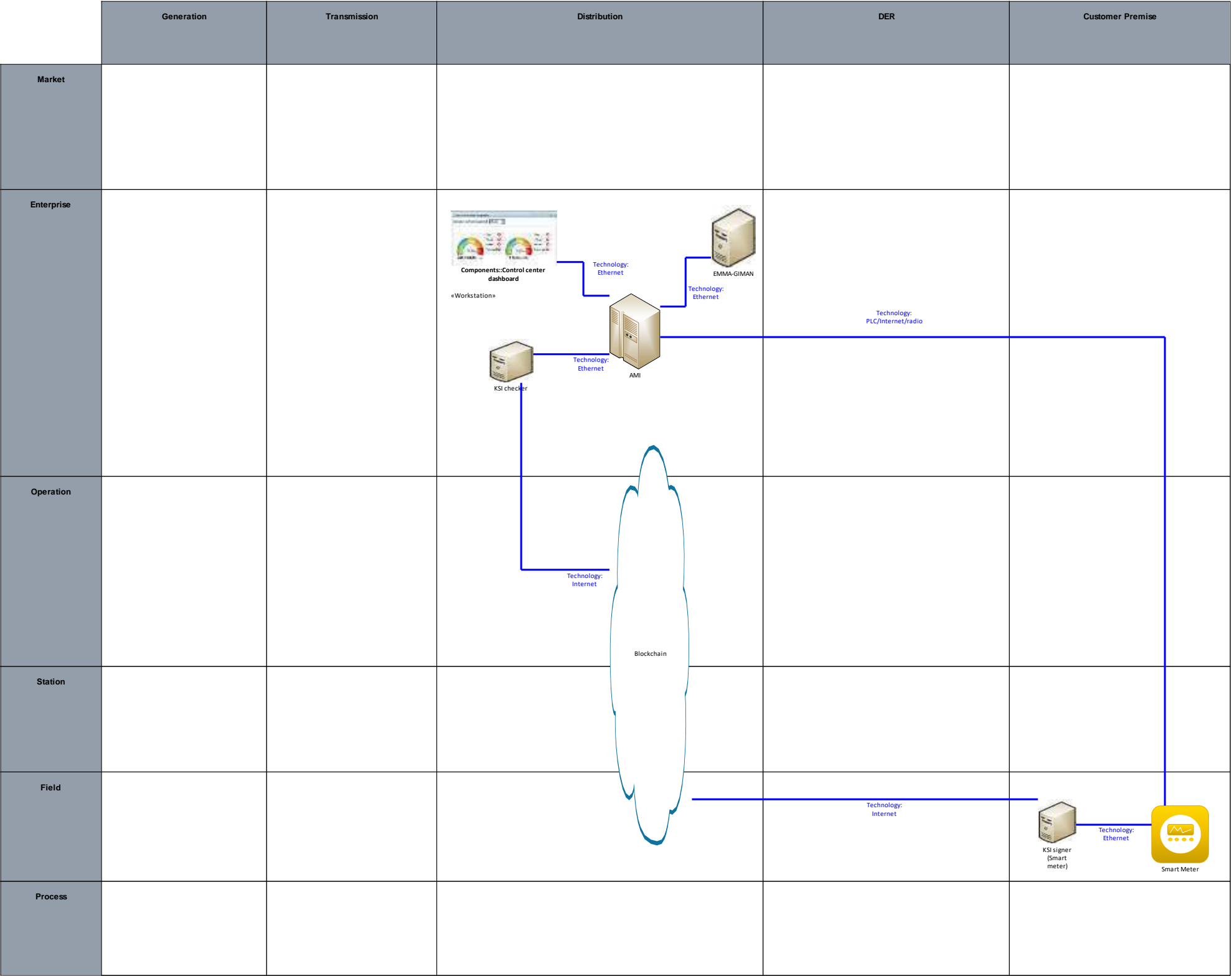


Figure 361 - UC40 Component Layer



13.4.4 WP6-EMMA

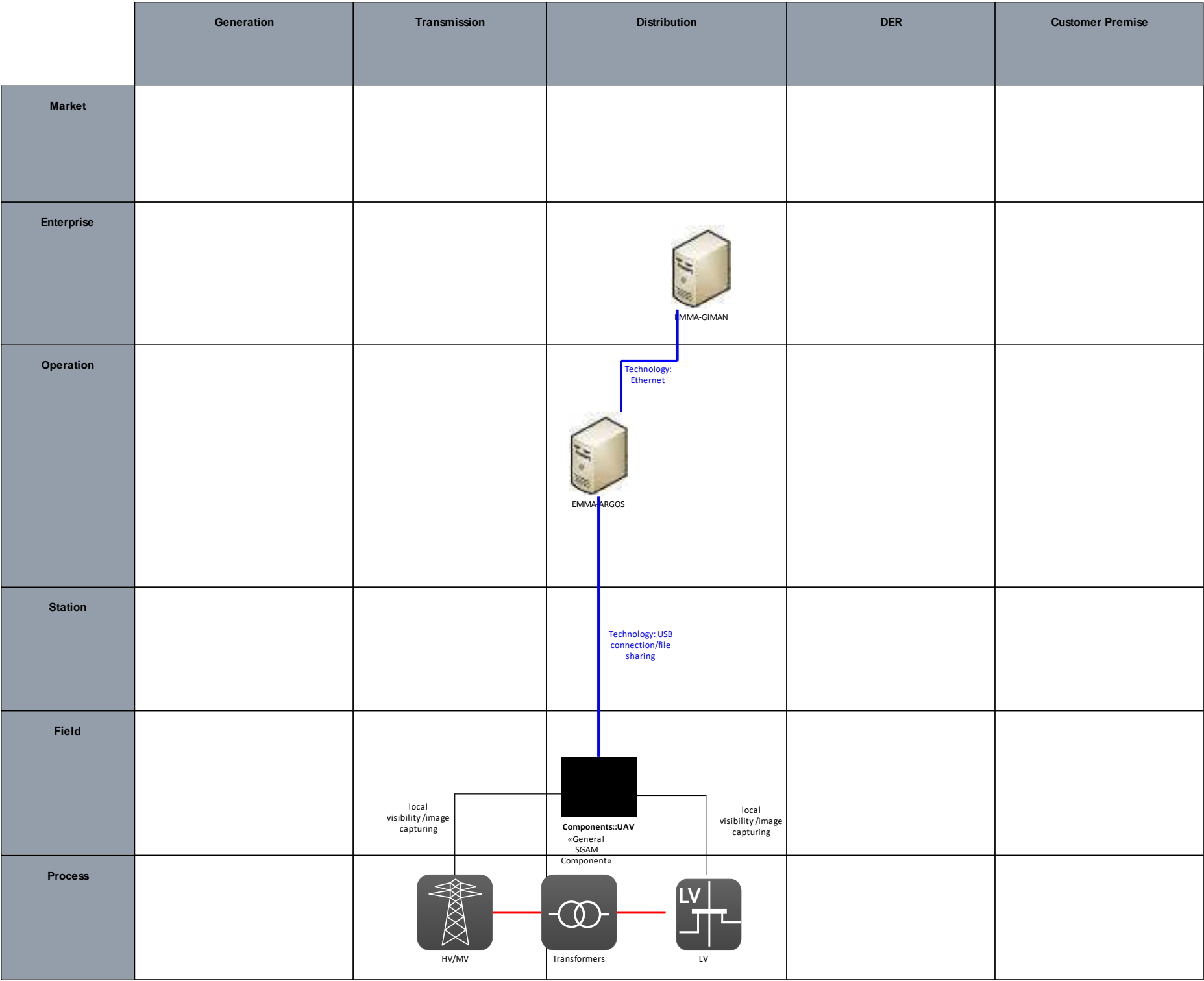


Figure 362 - UC01 Component Layer

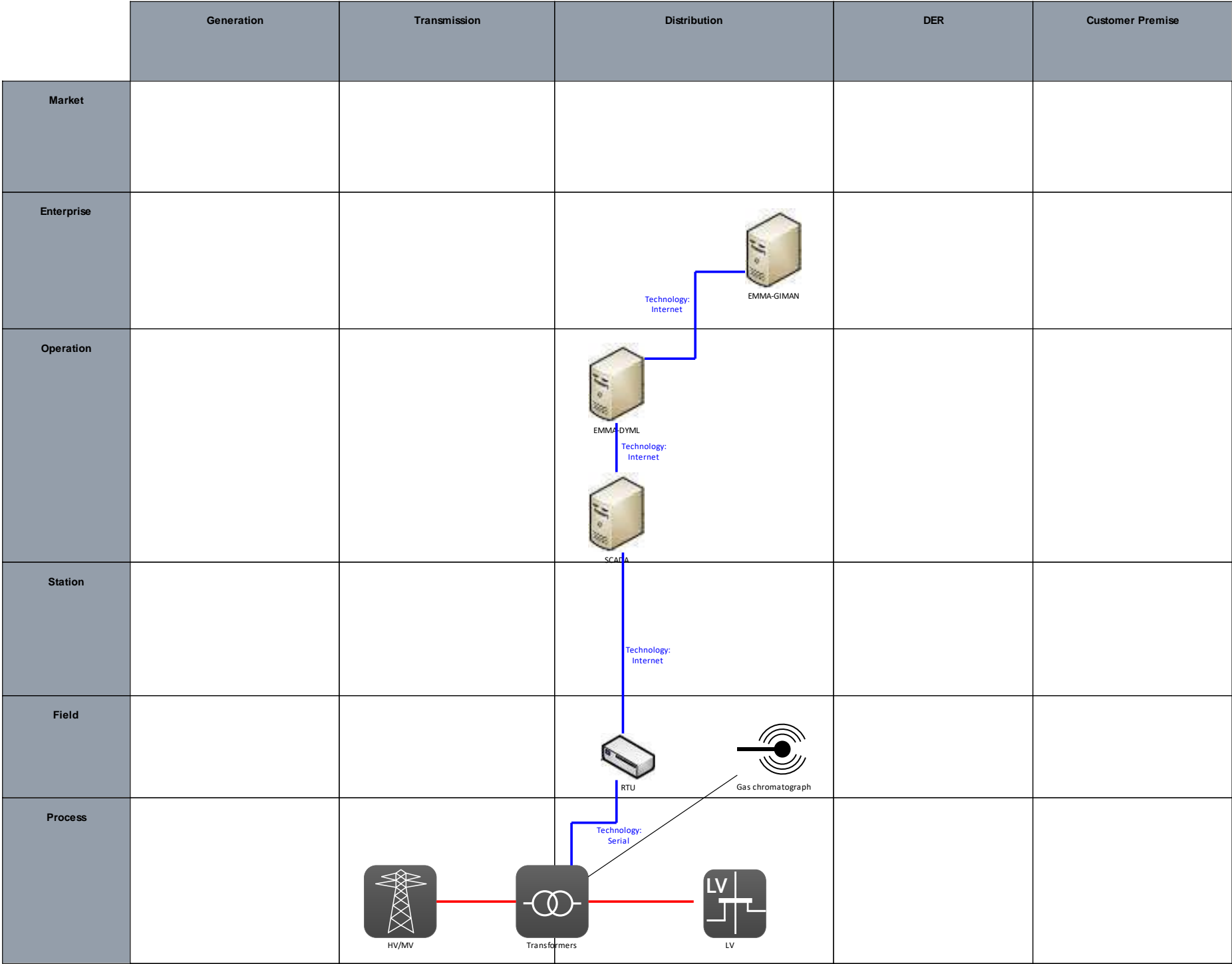


Figure 363 - UC02 Component Layer

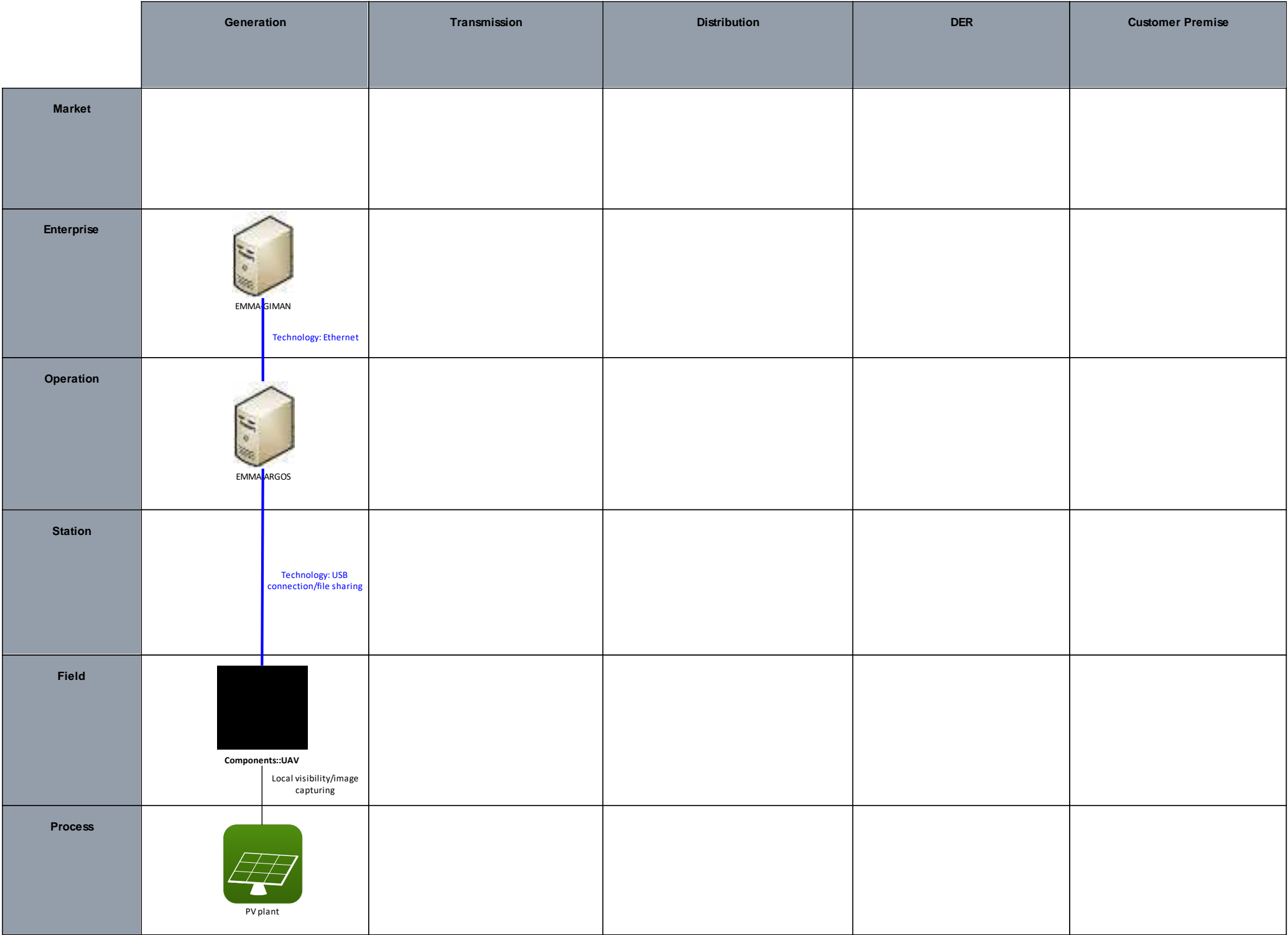


Figure 364 – UC03 Component Layer

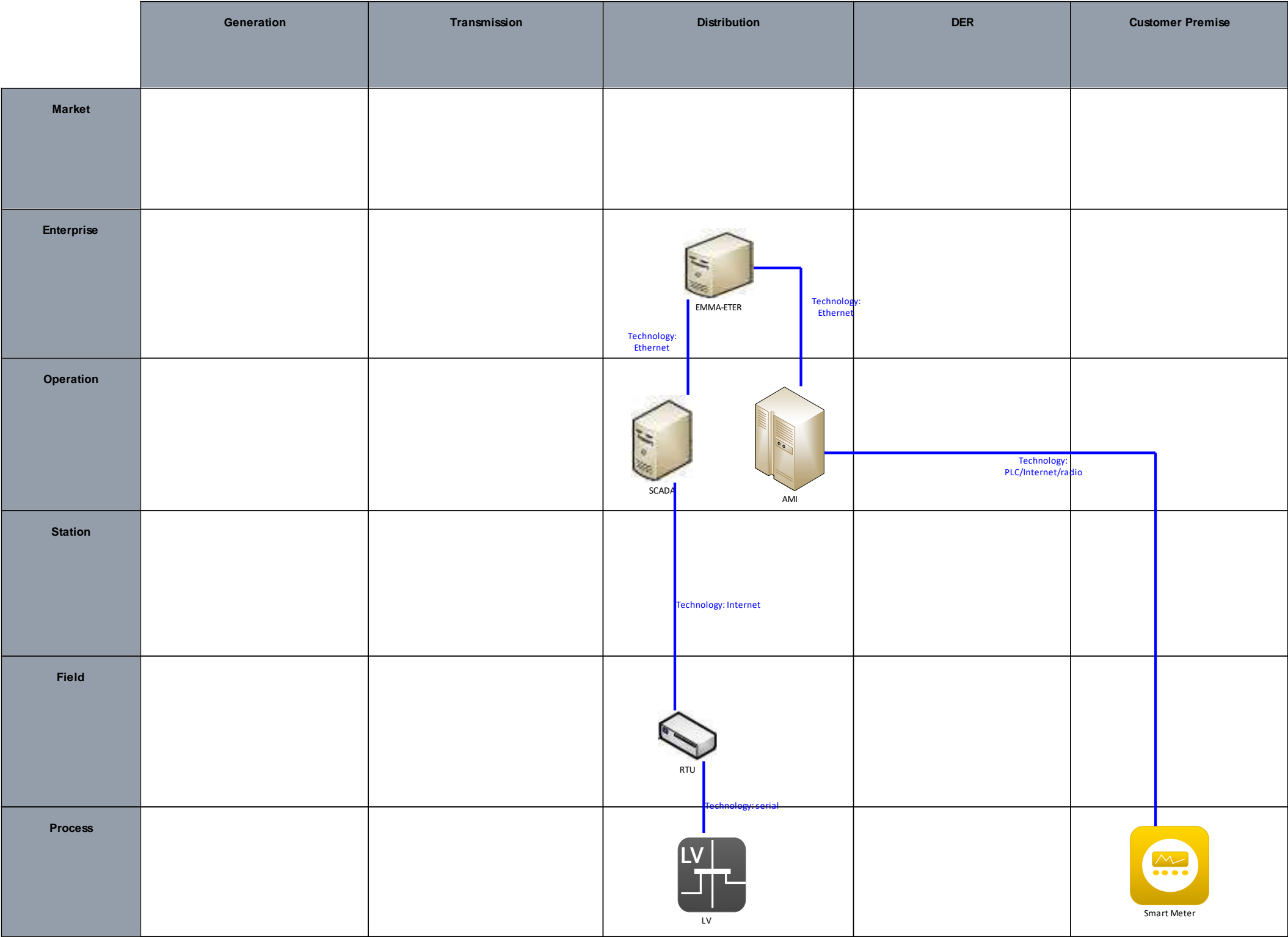


Figure 365 - UC04 Component Layer

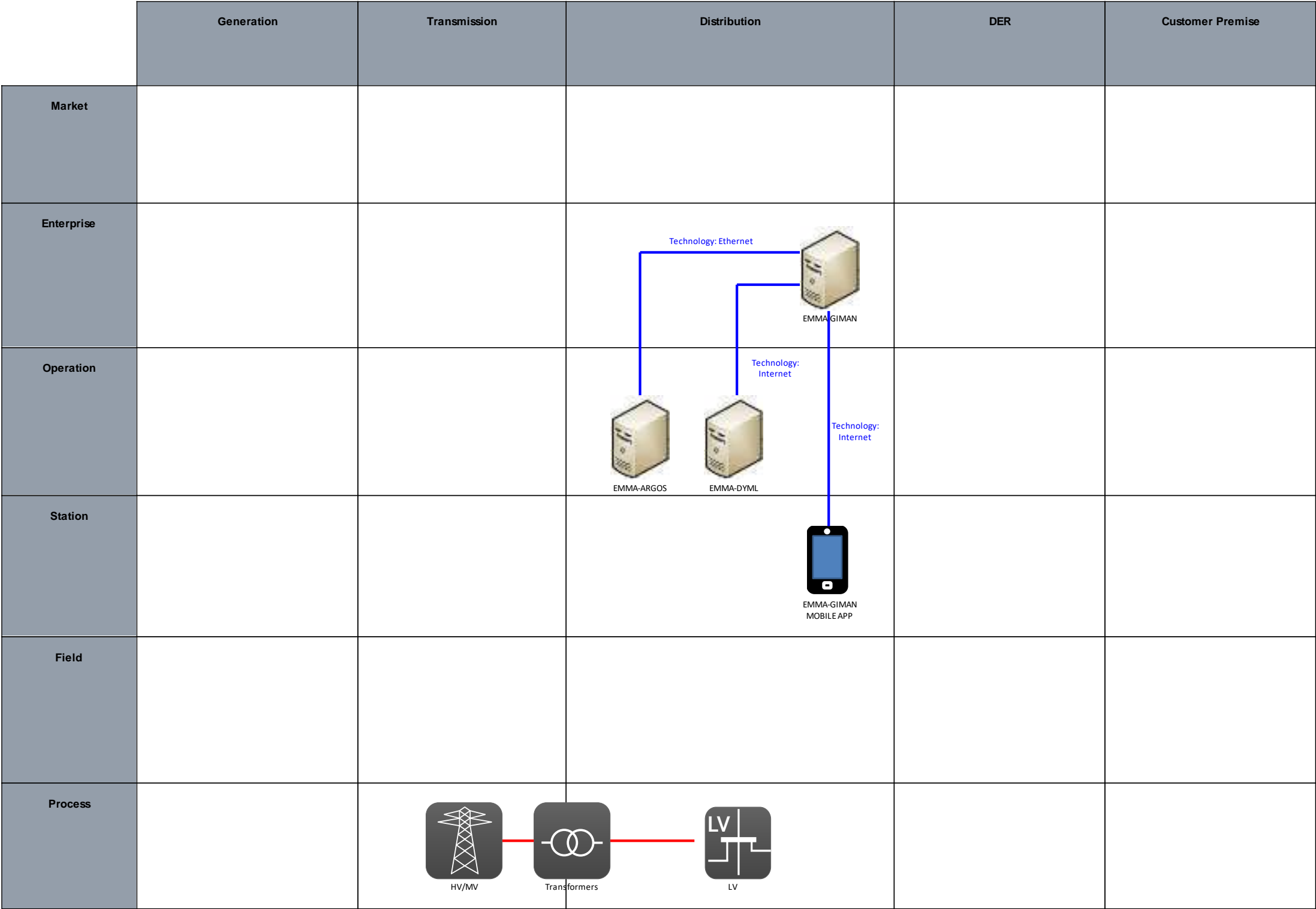


Figure 366 - UC05 Component Layer

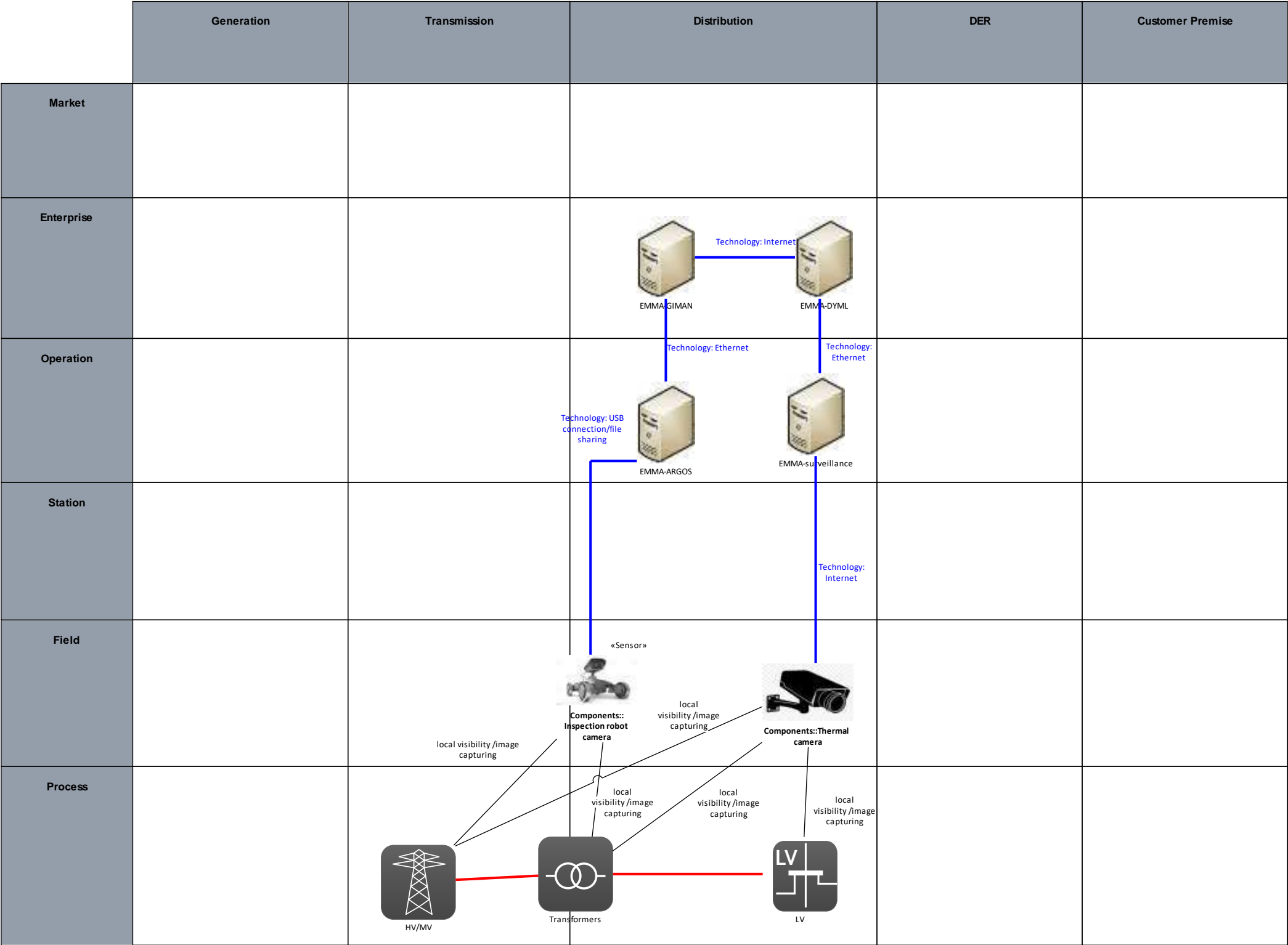


Figure 367 - UC06 Component Layer

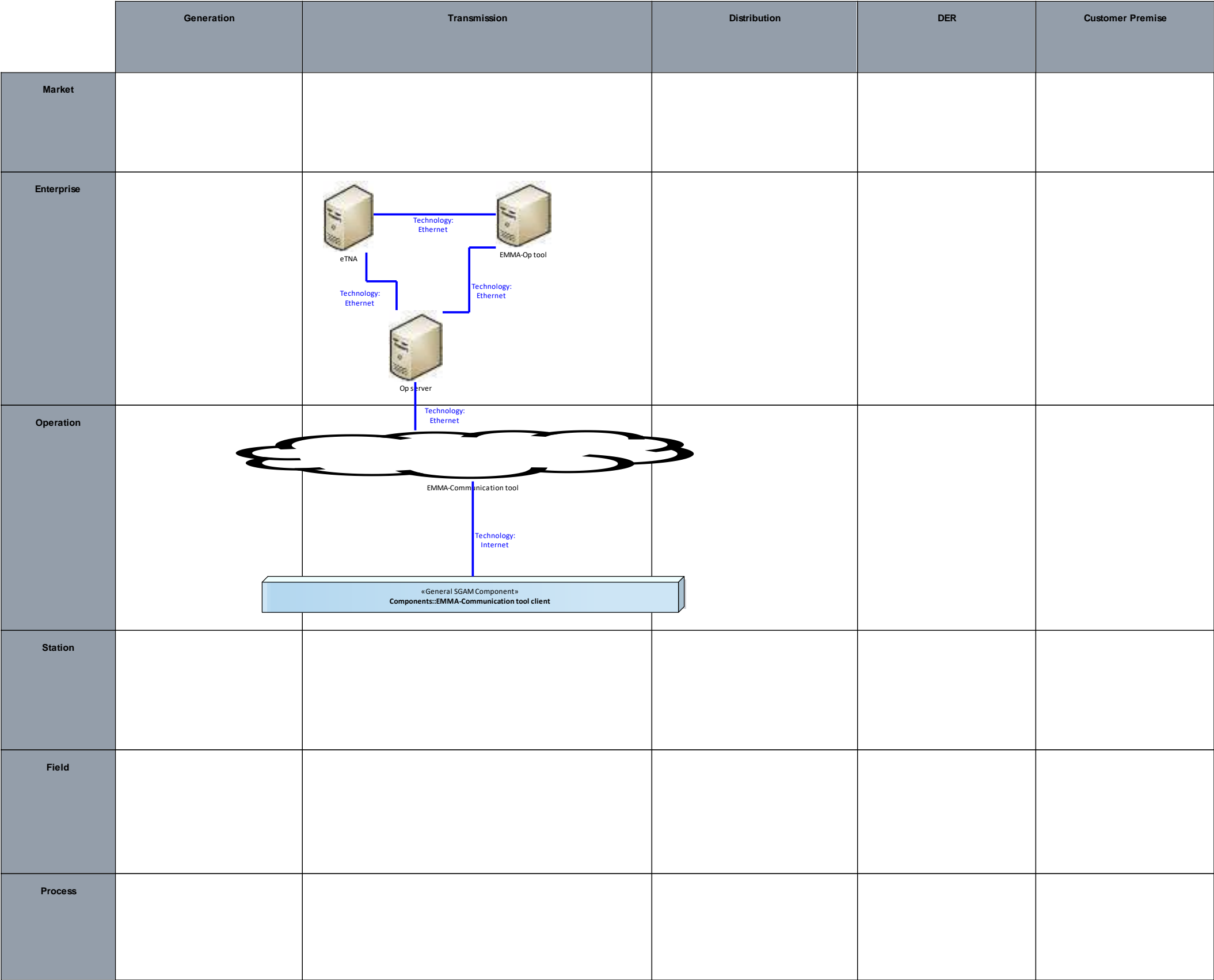


Figure 368 - UC08 Component Layer



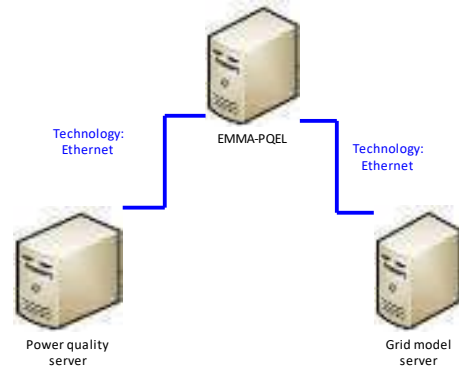
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise		<div></div>			
Operation					
Station					
Field					
Process					

Figure 369 - UC09 Component Layer

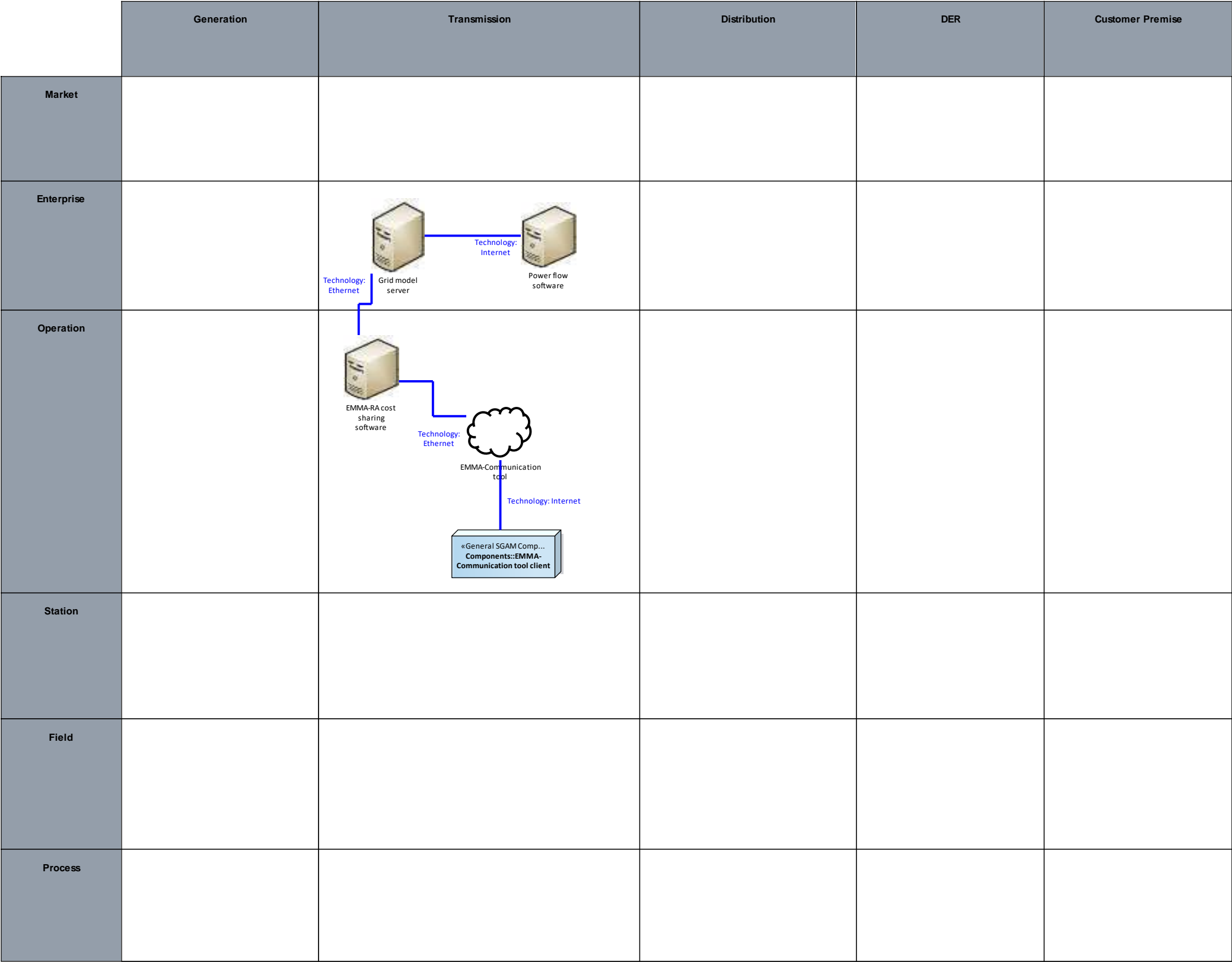


Figure 370 - UC13 Component Layer



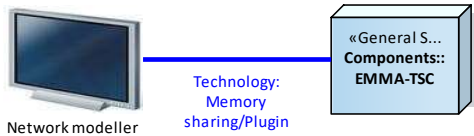
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 371 - UC14 Component Layer



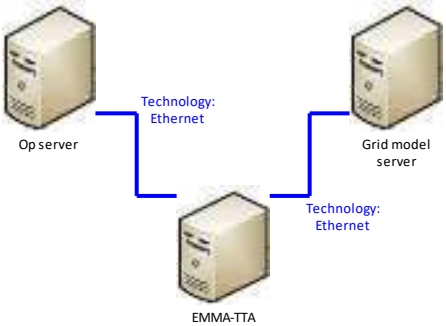
	Generation	Transmission	Distribution	DER	Customer Premise
Market					
Enterprise					
Operation					
Station					
Field					
Process					

Figure 372 - UC17 Component Layer

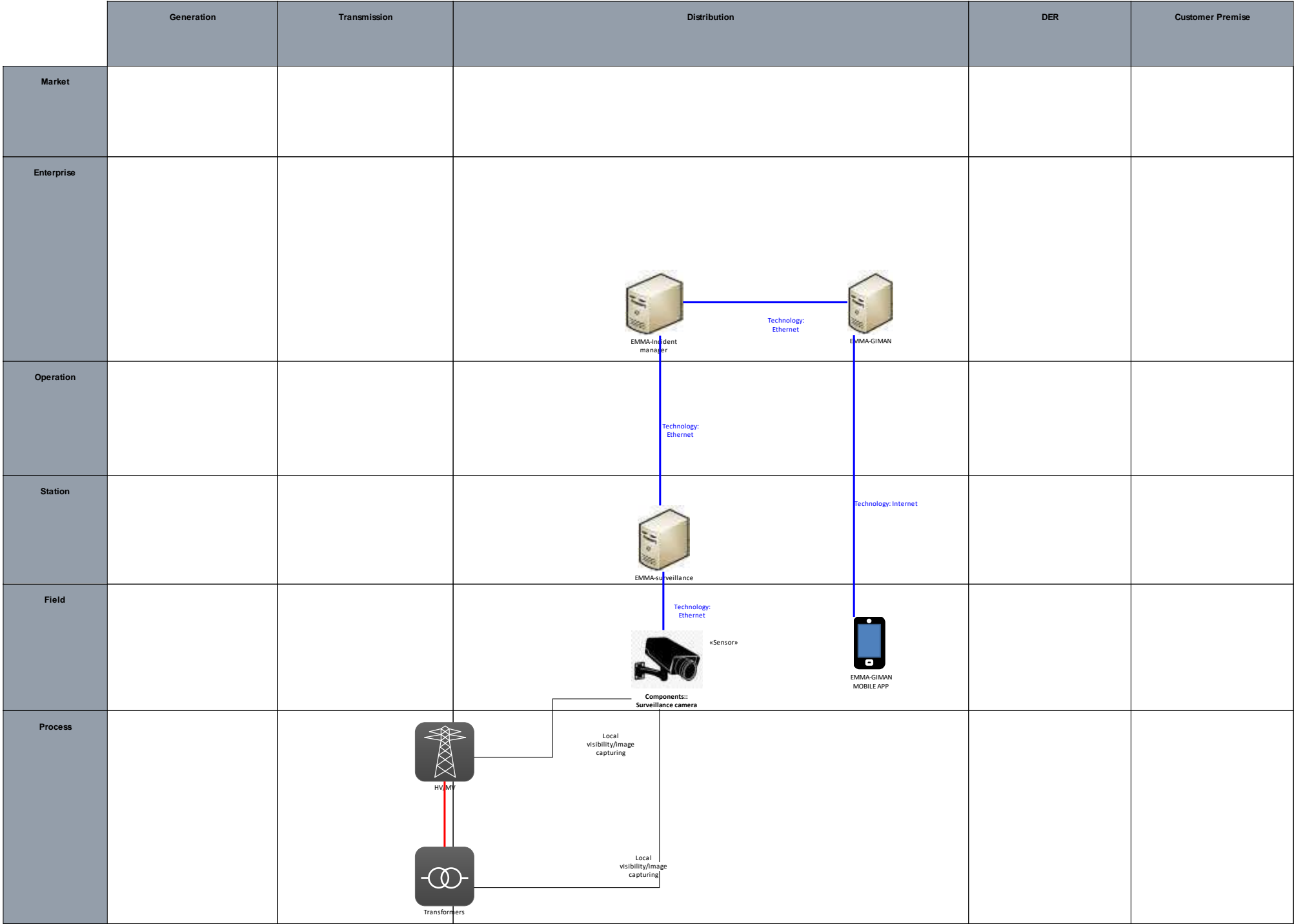


Figure 373 - UC20 Component Layer

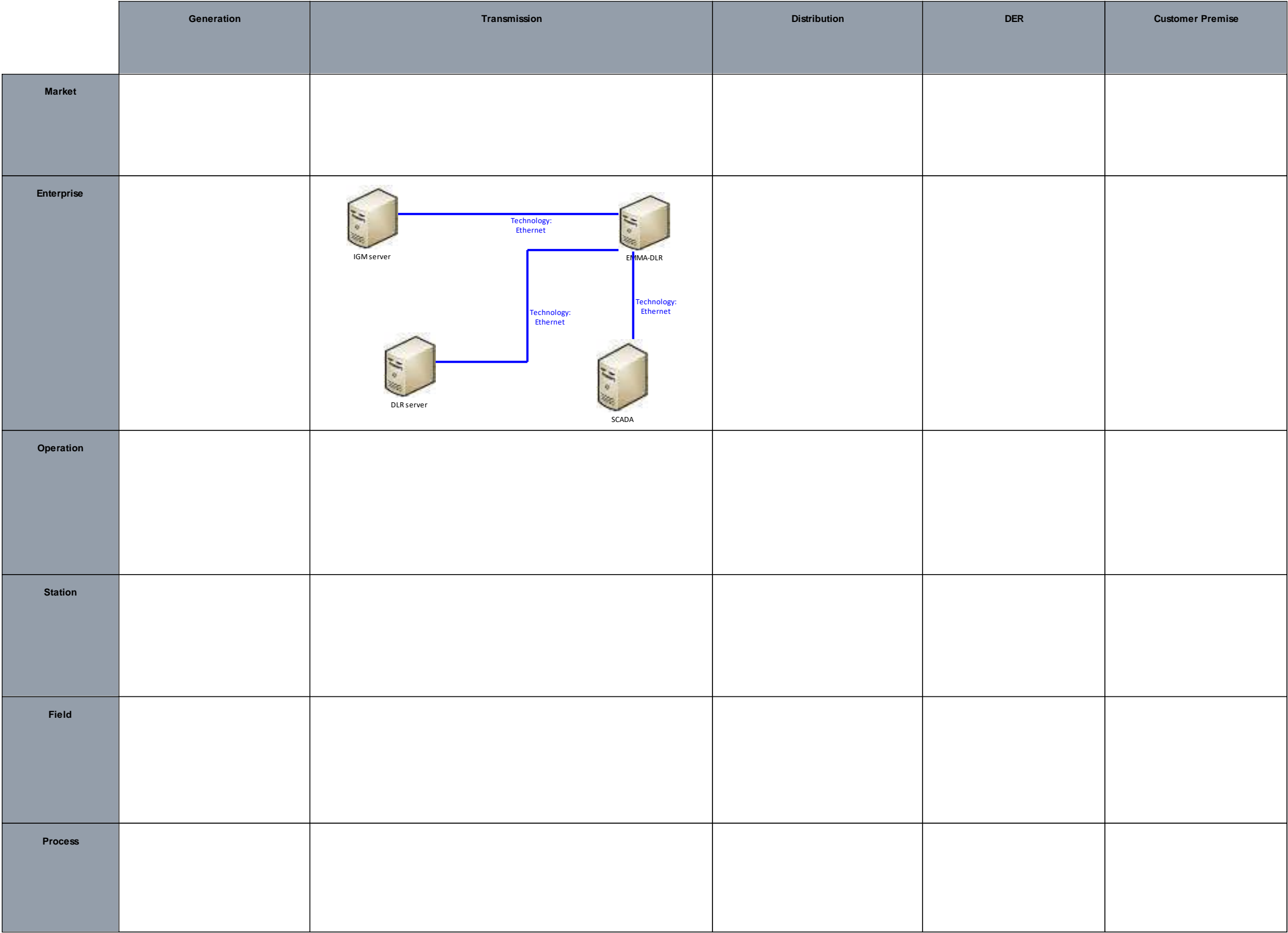


Figure 374 - UC31 Component Layer



14. ANNEX V: KPI TEMPLATES

BASIC KPI INFORMATION			
KPI Name		KPI ID	
R2D2 Strategic Objective(s)			
R2D2 DEMO(s)/product(s) where KPI applies			
R2D2 Use Case where KPI applies			
Owner			
KPI Description			
KPI Formula			
Unit of measurement			
Target / Thresholds			
Reporting Period			
Reporting Audience and Access Rights			
OTHER (please specify)			

KPI CALCULATION METHODOLOGY

KPI Step Methodology ID [KPI ID #]	Step	Responsible
[KPI ID] 1	Step by step methodology on how to calculate defined KPI	Person and Company responsible for specific step in KPI calculation methodology
[KPI ID] 2		
[KPI ID] 3		
[KPI ID] 4		

KPI DATA COLLECTION

Data	Data ID	Methodology for data collection	Source/Tools/Instruments for Data collection	Location of Data collection	Frequency of data collection	Data collection responsible
Data to collect	Identification of data requiring collecting, that is later used in formulas for calculating KPI	Describe method by which data is collected	Instruments / Tools used to collect data	Where is data measured / located ?	Indicate how often, when and for how long data is collected for	Name of person & Company responsible for collecting data



D2.3 - Requirements and Detailed Architecture Design

KPI BASELINE			
Source of Baseline Condition	LITERATURE VALUES	COMPANY HISTORICAL VALUES	VALUES MEASURED AT START OF PROJECT
Details of Baseline			
Responsible (Name, Company) for Baseline			

15. ANNEX VI: QUANTIFICATION INFORMATION OF KPIS

PROJECT KEY PERFORMANCE INDICES							
U C ID	Partner	UC Description	KPI Name	Demo Site	KPI Description	KPI Formula	Measurement Unit
1	ETRA	Improvement in overhead power lines inspection and maintenance using IA applied to UAV-captured images and data.	SAIDI	Spain, Greece	Average outage duration for each customer served	$SAIDI = \frac{\sum_{i=1}^k (N_i * D_i)}{N_T}$ <p>Ni : number of interruptions in the network suffered by customers, during k event, Di: duration of k event NT: total number of customers of the network</p>	Minutes
			Average Service Availability Index	Spain, Greece	Average Service Availability Index (ASAI) is the ratio of the total number of customer hours that service was available during a given time period to the total		Percentage

D2.3 - Requirements

ire Design

$$ASAI = \left(1 - \frac{\sum r_i * N_i}{N_T * T} \right) * 100$$

					customer hours demanded.	<p>Where</p> <p>T = Time period under study, hours.</p> <p>ri = Restoration time, hours.</p> <p>Ni = Total number of customers interrupted.</p> <p>NT = Total number of customers served.</p>	
			Average response time for customer re-electrification under extreme weather event	Spain, Greece	The average response time for mobile sources to provide resilience services between the fault occurrence and the load restorations.	Count (time).	Percentage.
			Increase of distributed RES capacity	Spain, Greece	Increase the amount (MW/GW) of RES/DER integration, using advance power technologies or better coordination of system operation	Count (time).	Percentage (MW).
			Number of assets analysed through R2D2	Spain, Greece	Number and categories of assets (devices, equipment, apparatus in general) to be potentially	Count (unit).	Percentage.



D2.3 - Requirements and Detailed Architecture Design

					inspected through R2D2 technologies		
			Assets Down-time Reduction	Spain, Greece	asset is not working due to unplanned conditions	Count (time).	Percentage.
			Cost of the activities related to equipment maintenance	Spain, Greece	Reduction of the average cost related to the maintenance of the equipment considered in this UC	Count (cost).	Percentage
			Creation of new jobs (contractors, equipment manufacturers)	Spain, Greece	Estimation of the new jobs potentially created through the introduction of R2D2 technologies in the considered pilots	Count (unit).	Percentage
			OPEX Reduction	Spain, Greece	the process of eliminating or reducing operational expenses, such as operations costs, telecommunications technology, and maintenance costs, in order to maximize profits	Count (cost).	Percentage

D2.3 - Requirements and Detailed Architecture Design

2	ETRA	Substation component status of health calculation based on SCADA measurements and DGA data	SAIDI	Spain, Greece	average outage duration for each customer served	$SAIDI = \frac{\sum_{i=1}^k (N_i * D_i)}{N_T}$ <p>Ni : number of interruptions in the network suffered by customers, during k event, Di: duration of k event NT: total number of customers of the network</p>	Minutes
			SAIFI	Spain, Greece	Average frequency at which users are affected by network fault or extreme weather event (EWE).	$SAIFI = \frac{\sum_{i=1}^k N_i}{N_T}$ <p>Ni : number of interruptions in the network suffered by customers, during k event NT: total number of customers of the network</p>	Percentage reduction (unit).
			CAIDI	Spain, Greece	CAIDI gives the average outage duration that any given customer would experience	$CAIDI = \frac{\text{sum of all customer interruption durations}}{\text{total number of customer interruptions}} = \frac{SAIDI}{SAIFI}$	Percentage reduction (time).

D2.3 - Requirements and Detailed Architecture Design

			Average Service Availability Index	Spain, Greece	Average Service Availability Index (ASAI) is the ratio of the total number of customer hours that service was available during a given time period to the total customer hours demanded.	$ASAI = \left(1 - \frac{\sum r_i * N_i}{N_T * T}\right) * 100$ <p>T = Time period under study, hours. ri = Restoration time, hours. Ni = Total number of customers interrupted. NT = Total number of customers served.</p>	Percentage
			Customers Experiencing Multiple Interruptions	Spain, Greece	Customers Experiencing Multiple Interruptions or "CEMI" means the percent of customers who have experienced a given number or more sustained Interruptions during the reporting period.	Count (unit).	Percentage reduction
			Restoration time of a damaged component under extreme weather events	Spain, Greece	Reduction of the average time for repairing and re-negising critical damaged assets	Count (time).	Percentage reduction (time).
			Number of assets analysed through R2D2	Spain, Greece	Number and categories of assets (devices, equipment,	Count (unit).	Percentage



D2.3 - Requirements and Detailed Architecture Design

					apparatus in general) to be potentially inspected through R2D2 technologies		
			Cost of the activities related to equipment maintenance	Spain, Greece	Reduction of the average cost related to the maintenance of the equipment considered in this UC	Count (cost).	Percentage
			Creation of new jobs (contractors, equipment manufacturers)	Spain, Greece	Estimation of the new jobs potentially created through the introduction of R2D2 technologies in the considered pilots	Count (unit).	Percentage
			OPEX Reduction	Spain, Greece	the process of eliminating or reducing operational expenses, such as operations costs, telecommunications technology, and maintenance costs, in order to maximize profits	Count (cost).	Percentage

D2.3 - Requirements and Detailed Architecture Design

			Number of new commercial opportunities and cooperation among stakeholders analysed	Spain, Greece	Number of new potential opportunities (customers, calls, tenders, etc.) that can be added to the traditional portfolio of the partners involved	Count (unit).	Percentage
3	ETRA	Malfunctioning detection of PV panels through autonomous UAV image acquisition	Increase of distributed RES capacity	Greece	Increase the amount (MW/GW) of RES/DER integration, using advance power technologies or better coordination of system operation	Count (time).	Percentage (MW).
			Number of assets analysed through R2D2	Greece	Number and categories of assets (devices, equipment, apparatus in general) to be potentially inspected through R2D2 technologies	Count (unit).	Percentage
4	ETRA	Detection of NTL through SCADA and AMI data, from a selected portion of the	Number of internet-connected devices to be protected by R2D2s solutions	Greece, Spain	Number of devices that can be remotely protected through R2D2 solutions compared with the traditional approach (previous existing solutions)	Count (unit).	Percentage

D2.3 - Requirements and Detailed Architecture Design

		distribution grid	Number of smart meters and edge devices that will be made cyber secure with R2D2	Greece, Spain	Number of smart meters and edge devices that will be made cyber secure with R2D2	Count (unit).	Percentage
			Number of assets analysed through R2D2	Greece, Spain	Number and categories of assets (devices, equipment, apparatus in general) to be potentially inspected through R2D2 technologies	Count (unit).	Percentage
			Detection of NTL patterns	Greece, Spain	Number of new suspicious and malicious events that can be possibly detected with R2D2, compared with existing solutions	Count (unit).	Percentage
			CAPEX Reduction or deferral in upgrading grid infrastructures	Greece, Spain	Economic quantification of the reduction of CAPEX for investment deferral only, by adopting R2D2 solutions	Count (cost).	Percentage

D2.3 - Requirements and Detailed Architecture Design

			OPEX Reduction	Greece, Spain	the process of eliminating or reducing operational expenses, such as operations costs, telecommunications technology, and maintenance costs, in order to maximize profits	Count (cost).	Percentage
			Number of potential customers of the R2D2 products	Greece, Spain	New customers potentially acquired through the development of R2D2 solutions	Count (unit).	Percentage
5	ETRA	Automated ranking intervention of assets and optimal scheduling (including routing) of intervention workforce to perform maintenance task.	Restoration time of a damaged component under extreme weather events	Greece	Reduction of the average time for repairing and re-negising critical damaged assets	Count (time).	Percentage reduction (time).
6	ETRA	Substation components	Customers Experiencing	Greece, Spain	Customers Experiencing Multiple	Count (unit).	Percentage reduction

D2.3 - Requirements and Detailed Architecture Design

		degradation detection by analysing images (Conventional & thermal)	Multiple Interruptions		Interruptions or “CEMI” means the percent of customers who have experienced a given number or more sustained Interruptions during the reporting period.		
			Restoration time of a damaged component under extreme weather events	Greece, Spain	Reduction of the restoration time of the affected component / Infrastructure after critical event, by adopting R2D2 solutions	Count (time).	Percentage reduction (time).
			Number of assets analysed through R2D2	Greece, Spain	Number and categories of assets (devices, equipment, apparatus in general) to be potentially inspected through R2D2 technologies	Count (unit).	Percentage
			Assets Down-time Reduction	Greece, Spain	asset is not working due to unplanned conditions	Count (time).	Percentage.



D2.3 - Requirements and Detailed Architecture Design

			Cost of the activities related to equipment maintenance	Greece, Spain	Reduction of the average cost related to the maintenance of the equipment considered in this UC	Count (cost).	Percentage
			CAPEX Reduction or deferral in upgrading grid infrastructures	Greece, Spain	Economic quantification of the reduction of CAPEX for investment deferral only, by adopting R2D2 solutions	Count (cost).	Percentage
			OPEX Reduction	Greece, Spain	the process of eliminating or reducing operational expenses, such as operations costs, telecommunications technology, and maintenance costs, in order to maximize profits	Count (cost).	Percentage
			Number of potential customers of the R2D2 products	Greece, Spain	New customers potentially acquired through the development of R2D2 solutions	Count (unit).	Percentage

D2.3 - Requirements and Detailed Architecture Design

7	ELEK	Enhancement in DER control and management systems to participate in flexibility procurement schemes for DSO and TSO to improve network operation security	Increase of the data availability and easier data exchange among system operators during emergencies	Slovenia	Increase of the data availability and easier data exchange among system operators during emergencies	Count (unit).	
			Number of smart meters and edge devices that will be made cyber secure with R2D2	Slovenia	Number of smart meters and edge devices that will be made cyber secure with R2D2	Count (unit).	
			Number of notifications exchanged with flexibility providers (RES producers and dispatchable loads)	Slovenia		Count (unit).	
			Increase of distributed RES capacity	Slovenia	Increase of distributed RES capacity	Count (unit).	

D2.3 - Requirements and Detailed Architecture Design

			Number of new commercial opportunities and cooperation among stakeholders analysed	Slovenia	Number of new commercial opportunities and cooperation among stakeholders analysed	Count (unit).	
			Number of regulatory barriers and gaps in standards identified and analysed in project	Slovenia	Number of regulatory barriers and gaps in standards identified and analysed in project	Count (unit).	
			KPI from proposal: ID 42 Number of policy recommendations provided at pilot sites project level	Slovenia	Number of policy recommendations provided at pilot sites project level	Count (unit).	
8	EMSS, SCC	Outage planning optimization	Efficiency improvement (Effl)	Serbia	This KPIs address to the use case basic intention to improve efficiency of outage planning.	$=100\% \cdot (\text{DataID1}) / \text{DataID2}$; DataID1 - Average time for manual outage optimization; DataID2 - Average time for automated outage optimization	%

D2.3 - Requirements and Detailed Architecture Design

9	EMSS	Automation of power quality parameters emission levels calculation	Efficiency improvement (Effl)	Serbia	This KPIs address the basic intention to improve efficiency of power quality parameters evaluation (planned and emission levels)	$=100\% \cdot (\text{DataID1}) / \text{DataID2};$ DataID1 - Average time for manual power quality parameters calculation; DataID2 - Average time for automated power quality parameters calculation	%
10	ELPROS	Setting up secure interface between SCADA-ADMS and billing metering system to improve LV network observability and consequently to improve system security and	Average Service Availability Index	Slovenia	Average Service Availability Index (ASAI) is the ratio of the total number of customer hours that service was available during a given time period to the total customer hours demanded.	$ASAI = \left(1 - \frac{\sum r_i * N_i}{N_T * T} \right) * 100$ <p>Where T = Time period under study, hours. ri = Restoration time, hours. Ni = Total number of customers interrupted. NT = Total number of customers served.</p>	Percentage

D2.3 - Requirements and Detailed Architecture Design

		quality of supply	Number of smart meters and edge devices that will be made cyber secure with R2D2	Slovenia	Number of smart meters and edge devices that will be made cyber secure with R2D2	Count	-
11	ELEK	DSO - TSO congestion and power quality coordination in application of system services	Average Service Availability	Slovenia	Average Service Availability Index (ASAI) is the ratio of the total number of customer hours that service was available during a given time period to the total customer hours demanded.	$ASAI = \left(1 - \frac{\sum r_i * N_i}{N_T * T} \right) * 100$ <p>Where T = Time period under study, hours ri = Restoration time, hours. Ni = Total number of customers interrupted. NT = Total number of customers served.</p>	
			Increase of the data availability and easier data exchange among system operators during emergencies	Slovenia	Increase of the data availability and easier data exchange among system operators during emergencies.	Count	Percentage



D2.3 - Requirements and Detailed Architecture Design

			Number of notifications exchanged with flexibility providers (RES producers and dispatchable loads)	Slovenia	Number of notifications exchanged with flexibility providers (RES producers and dispatchable loads)	Count	Percentage
			Number of regulatory barriers and gaps in standards identified and analysed in project	Slovenia	Number of regulatory barriers and gaps in standards identified and analysed in project	Count	Percentage
			Number of policy recommendations provided at pilot sites project level	Slovenia	Number of policy recommendations provided at pilot sites project level	Count	Percentage

D2.3 - Requirements and Detailed Architecture Design

12	EMSS, IMP	Emergency & Restoration – Over-Frequency Protection module	Over-Frequency Protection Module (OFPM) rate of inclusion	Serbia	% of the installed capacity of generators that are included in the OFPM at the national level	=100%·DataID2/DataID1; DataID1 - Sum of the installed capacity of generators ; ·DataID2 - Sum of the installed capacity of generators that are included in the OFPM at the national level	%
13	EMSS, SCC	Cost sharing of remedial actions with cross-border impact	Average user satisfaction rating	Serbia	User satisfaction refers to the user's comfort and acceptability of the Methodology on cost-sharing of remedial actions with cross-border impact. Each potential user (West Balkan TSO) will rate the methodology (e.g. in the range of 1 to 10).	=AVERAGE(DataID1); DataID1 - User satisfaction rating	-
14	EMSS	Automation of transient stability calculations for operation planning purposes	Efficiency improvement (EffI)	Serbia	This KPI address to the use case basic intention to improve efficiency of Critical Fault Clearing Time Calculation (CFCTC).	=100%·(DataID1)/DataID2; DataID1 - Average time for manual CFCTC; DataID2 - Average time for automatedCFCTC	%

D2.3 – Requirements and Detailed Architecture Design

15	EMSS	TSO-DSO cooperation in Individual Grid Model creation	IGM accuracy	Serbia	KPI refers to the average absolute deviation of the aggregated production and consumption plans (i.e. power exchange plans between the transmission and distribution system) in the nodes of interest (nodes with significant DER share) from the metered/measured values.	$= 100\% \cdot \text{AVERAGE (ABSOLUTE (Data ID1 - Data ID2)/ Data ID2));}$ <p>Data ID1 -Forecasted power exchange in nodes of interest DataID2 - Metered/measured power exchange in nodes of interest</p>	%
16	EMSS, IMP	Phasor angles monitoring and prevention of instability	Number of detected instabilities on an annual level	Serbia	This KPI counts the number of alarm activations for detected instability due to exceeding the critical angle between two observed points in the system (where PMUs are installed), which means that corrective measures need to be activated to avoid disturbance due to instability.	$= \text{DataID1};$ <p>DataID1 - Number of detected instabilities on an annual level</p>	-

D2.3 - Requirements and Detailed Architecture Design

17	EMSS	Outage coordination and automated creation of topology files for Individual Grid Models	Mean value of the topology accuracy	Serbia	Mean value of the topology accuracy in day-ahead Individual Grid Model	$=100\% \cdot \text{DataID1} / (24 \cdot \text{DataID2})$; DataID1 - Total number of topology inconsistencies; DataID2 - Number of monitored network elements	
18	EMSS	Optimization of PMU installation points	Efficiency improvement (Effl)	Serbia	This KPIs address to the use case intention to improve efficiency of optimal PMU installation points.	$=100\% \cdot (\text{DataID1}) / \text{DataID2}$; DataID1 - Average time for manual optimisation of PMU installation points; DataID2 - Average time for automated optimisation of PMU installation points	%
19	EMSS, IMP, SCC	Emergency & Restoration - System Split module upgrade	Average user satisfaction rating	Serbia	User satisfaction refers to the user's comfort and acceptability of the Emergency & Restoration module - System Split tool. Each potential user (West Balkan TSO) will rate this tool (e.g. in the range of 1 to 10).	AVERAGE (Data ID1) ; Data ID1 - User satisfaction rating	-

D2.3 - Requirements and Detailed Architecture Design

20	HEDNO	Physical security enhancement in core network components (Primary Substations)	Customers Experiencing Multiple Interruptions	Greece		Ni : number of interruptions in the network suffered by customers	
			Attack detection rate for new assets to be integrated into the EPES	Greece			
			Number of security constraints treated with R2D2	Greece			
21	EMSS, IMP	Remedial Action Automation	Efficiency of remedial action verification and activation	Serbia	This KPI address to the use case basic intention to improve efficiency of remedial action verification and activation.	$=100\% \cdot (\text{DataID1}) / \text{DataID2}$; DataID1 - Average time for manual Remedial Action activation; DataID2 - Average time for automated Remedial Action activation	%

D2.3 - Requirements and Detailed Architecture Design

22	HEDNO	Prevention and mitigation of cascading effects in case of extreme weather events	SAIDI	Greece		$SAIDI = \frac{\sum_{i=1}^k (N_i * D_i)}{N_T}$ <p>Ni : number of interruptions in the network suffered by customers, during k event, Di: duration of k event NT: total number of customers of the network</p>	Minutes
			SAIFI	Greece	Average frequency at which users are affected by network fault or extreme weather event (EWE).	$SAIFI = \frac{\sum_{i=1}^k N_i}{N_T}$ <p>Ni : number of interruptions in the network suffered by customers, during k event NT: total number of customers of the network</p>	
			CAIDI	Greece			

D2.3 - Requirements and Detailed Architecture Design

			Customers Experiencing Multiple Interruptions	Greece		Ni : number of interruptions in the network suffered by customers	
			Average response time for customer re-electrification under extreme weather event	Greece	In the event of fault or extreme weather event (EWE), this KPI measures the average time needed until the affected users re-electrification.	$AverageFaultMitigationTime = \frac{\sum_{i=1}^n T_{mitigation,i}}{n}$ $T_{mitigation} = UTC_{reelectrification} - UTC_{fault}$ <p>n: number of faults, UTCreelectrification: UTC time when even the last affected customer was re-electrified, UTCfault: UTC time when the fault was detected</p>	min
			ENS (MWh/year)	Greece		$EnergyNotSupplied = \frac{ENS_{aft} - ENS_{bef}}{ENS_{bef}} \times 100$ <p>ENSbef: is the estimated curtailed energy loss (kWh) of the network due to curtailment before the use of R2D2 tools ENSaft: is the estimated curtailed energy loss (kWh) of the network due to curtailment after the use of R2D2 tools</p>	%

D2.3 - Requirements and Detailed Architecture Design

					Estimation of the reduction in curtailed energy after implementation of R2D2 products.		
			Restoration time of a damaged component under extreme weather events	Greece		$T_{mitigation} = UTC_{reelectrification} - UTC_{fault}$ <p>UTCreelectrification: UTC time when damaged component was re-electrified, UTCfault: UTC time when the damage was detected</p>	min

D2.3 - Requirements and Detailed Architecture Design

23	HEDNO	Cooperative crisis handling in case of cascading effects	Number of notifications exchanged with R2D2	Greece	Percentage of scheduled or expected messages successfully delivered to targeted system operator (DSO or TSO) by DSO or TSO when an event requiring notification is detected.	$NDR(\%) = \frac{N_d}{N_e} \times 100$ <p>NDR: Notification Delivery Ratio, Nd: number of notifications successfully delivered to the targeted system operator in the considered period, Ne: number of expected messages to be delivered in the considered period</p>	%
24	ICCS, CYBER, SCC	Cyber Security Risk assessment on EPES infrastructure	Assessed cyber security risk/attack scenarios	Greece	Number of Cyber Security risk scenarios that the chosen pilot has been assessed against to evaluate associated cybersecurity risk levels	Count (risk_scenarios)	Natural Number

D2.3 - Requirements and Detailed Architecture Design

			Number of EPES infrastructure components to be assessed against cyber security risk/attack scenarios	Greece	Count the number of EPES infrastructure components to be assessed against cyber security risk/attack scenarios by the Static Cyber Risk Assessment tool.	Count (EPES infrastructure components)	Natural Number
			Participation in events/workshops/conferences at local/national/international level	Greece	Count the number of participations in events/workshops/conferences at local/national/international level	Count (participations)	Natural Number
			Number of new commercial opportunities and cooperation among stakeholders analysed	Greece	Count the number of new commercial opportunities and cooperation among stakeholders analysed	Count (opportunities)	Natural Number
25	ICCS, CYBER	Dynamic Cyber-Risk Status Evaluation considering existing	Number of internet-connected devices to be protected by R2D2s solutions	Greece	Count the number of internet-connected devices to be protected by the Dynamic Cyber-Risk Evaluation system	Count (devices)	Natural Number

D2.3 - Requirements and Detailed Architecture Design

		technical vulnerabilities	Number of scientific publications	Greece	Number of papers/manuscripts published in international scientific journals and in conference proceedings	Count(publications)	Natural Number
			Participation in events/workshops/conferences at local/national/international level	Greece	Count the number of participations in events/workshops/conferences at local/national/international level	Count(participations)	Natural Number
			Mean Time to Detect cyber-security issue (MTTD)	Greece	Calculate the improvement in the mean time to detect cyber-security Critical technical Vulnerabilities	(Previous Time to Detect Cyber-Security Critical Vulnerabilities - Current Time to Detect Cyber-Security Critical Vulnerabilities)/ Previous Time to Detect Cyber-Security Critical Vulnerabilities	Percentage

D2.3 - Requirements and Detailed Architecture Design

26	ICCS, CYBER	Cyber Threat Intelligence knowledge collection/sharing with external sources	CTI Collaboration and Sharing	Greece	Assess the extent to which the CTI tool facilitates collaboration and information sharing among security teams, both internally and externally. This KPI measures the tool's effectiveness in promoting threat intelligence sharing and coordination.	Count(internal & external sources)	Natural Number
27	CYBER	Monitor communications behavior of newly deployed components in an EPES staging environment	Number of NEW EPES infrastructure components to be assessed in the staging environment	Greece	Count the number of NEW EPES infrastructure components to be protected by assessing them in the staging environment.	Count(NEW EPES infrastructure components)	Natural Number
			The number of new components tested and failed to be evaluated as secure due to suspicious communication attempts.	Greece	Count the number of NEW EPES infrastructure components evaluated as suspicious by assessing them in the staging environment.	Count(suspicious NEW EPES infrastructure components)	Natural Number

D2.3 - Requirements and Detailed Architecture Design

29	ICCS	Event simulator of a progressing wildfire and assessment of its impact on distribution system (evaluation of line outages, quantification of spatiotemporal load shedding)	Customers experiencing multiple interruptions	Greece	$100\% * (X_baseline - X_result) / X_baseline$	MWh shedded during a certain time horizon	10% reduction compared to a standard baseline value
			Number of scientific publications ¹¹	Greece	Number of publications	Number of publications	(to be considered)
30	ICCS	Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling	Customers experiencing multiple interruptions	Greece	$100\% * (X_baseline - X_result) / X_baseline$	MWh shedded during a certain time horizon	10% reduction compared to a standard baseline value
			Average response time for customer re-electrification under extreme weather event	Greece	$100\% * (X_baseline - X_result) / X_baseline$	Hours	15% reduction compared to a standard baseline value

D2.3 - Requirements and Detailed Architecture Design

			Restoration time of a damaged component under extreme weather events	Greece	$100\% * (X_baseline - X_result) / X_baseline$	Hours	15% reduction compared to a standard baseline value
			Assets Down-time Reduction	Greece	$100\% * (X_baseline - X_result) / X_baseline$	Hours	15% reduction compared to a standard baseline value
31	EMSS, IMP	DLR integration with IGMs and SCADA/EMS	Average Additional Transmission Capacity	Serbia	Average additional transmission capacity in percentage for all lines on which DLR is implemented	$=AVERAGE(100\% \cdot (DataID1/DataID2));$ DataID1 - DLR Current Limit; DataID2 - Seasonal Current Limit	%

D2.3 - Requirements and Detailed Architecture Design

32	ICL	Planning and operation for a resilient multi-energy microgrid	<p>Average response time for customer re-electrification under extreme weather event.</p> <p>Restoration time of a damaged component under extreme weather events.</p> <p>Cost of the activities related to equipment maintenance.</p> <p>Number of scientific publications.</p>	Greece	<p>6. The average response time for mobile sources to provide resilience services between the fault occurrence and the load restorations.</p> <p>9. The average restoration time for mobile sources to provide resilience services when an outage occurs.</p> <p>30. The planning and operation costs of mobile sources to enhance system resilience.</p> <p>43. Academic papers published by IEEE, Applied Energy, and other publishers.</p>	<p>6. Count (time).</p> <p>9. Count (time)</p> <p>30. Count (cost).</p> <p>43. Count (publications).</p>	<p>6. Percentage.</p> <p>9. Percentage.</p> <p>30. Percentage.</p> <p>43. Natural number.</p>
33	S2	Detection of anomalies associated with cybersecurity through the characterization of traffic in	New threat detection rate	TBD	This KPI measures how many of the threats in the validation set which were not detectable without developments in R2D2 will be possible	$\frac{\text{(Number of non detectable threats after R2D2)}}{\text{(Number of non detectable threats before R2D2)}} \leq 0,90$	Rate / percentage

D2.3 - Requirements and Detailed Architecture Design

		the perimeter, levels of control and supervision, operation and in physical environments.			<p>to detect after the project developments are deployed in sites.</p> <p>In order to measure this KPI, a battery of tests will be designed, considering which attacks are relevant to each of the demo sites and considering also which data sources can be monitored before and after R2D2 developments.</p>		
34	S2	Detection of anomalies associated with extreme events through the characterization of traffic in the perimeter, levels of control and supervision, operation and	Threat detection time	TBD	<p>This KPI measures the improvement in threat detection time thanks to R2D2 developments. Detection time will be defined as the time elapsed from the moment an action part of the attack/threat takes place to the moment at which a cybersecurity alert is</p>	$\frac{((\text{Cybersecurity alert rising date time after R2D2}) - (\text{Threat action date time}))}{((\text{Cybersecurity alert rising date time before R2D2}) - (\text{Threat action date time}))} \leq 0,90$	Rate / percentage

D2.3 - Requirements and Detailed Architecture Design

		in physical environments.			rised. The improvement will be defined as the difference between this detection time before and after R2D2 developments.		
35	S2	Pattern detection and correlation with information from other cyberattacks in order to detect potential threats.	False positive reduction	TBD	This KPI measures the reduction in the number of cybersecurity alerts which do not correspond to any actual attack or threat (False Positives, FP). This improvement will be defined as the ratio between these FP and the total number of cybersecurity alerts.	((Number FP alerts rised before R2D2) / (Total number alerts rised before R2D2)) - ((Number FP alerts rised after R2D2) / (Total number alerts rised after R2D2)) >= 0.1	Rate / percentage
39	SCC	1) Enable entry form for risk submission and modification; 2) Display all submitted risks and their	Increased efficiency of OPDE risk review process	Serbia	This KPI will be focused on the reduction of communication time between current manual process and future centralized semi-automatic process.	$E = \frac{\sum_{i=1}^N (T_i^{old} - T_i^{new})}{N}$ <p>E – average time per risk that represents increased efficiency of OPDE risk review process; T_i^{old} – Effective time necessary to process risk using current ENTSO-E business process;</p>	Hours



D2.3 - Requirements and Detailed Architecture Design

		information based on the “need to know” principle on centralised place; 3) Enable fast, secure and simple communication between users on the specific risk; 4) Log all changes of data in the system.				T_i^{new} – Effective time necessary to process risk using OPDE Risk Register; N – Total number of risks that will be demonstrated.	
40	GUARD	IoT data security enforcement	Accuracy of Tokenization tool	Greece	Tokenization tool provides tokens, which must verify originality of tokenized data in 100% of cases	<i>Percentage of accurate verification</i>	Percentage (%)

16. ANNEX VII: CONTINUOUS SW QUALITY AND SECURITY DEPENDENCY

Purpose and objective of the document

This document aims at gathering the possible standards and methodologies when developing applications and services for power system operation, planning and maintenance. Considering R²D² is a Horizon Europe I&A project dealing with the improvement of the cyber resiliency and cyber security of EPES, several applications are going to be developed for RSC, TSO and DSO. The Consortium has identified the need to define guidelines to ensure quality and security development of such applications.

The R²D² project aiming at improving the resiliency of the EPES, especially regarding cyber security, it was proposed to define for the deliverables of the project (e.g. the Products in this case), to establish precise guidelines and procedures that guarantee a superior level of security and quality throughout the software development process. This involves defining coding standards, utilizing tools like SonarQube, MendBolt, Dependency checker, and Coverity for rule enforcement, and incorporating routine code reviews and testing protocols.

Minimum guideline is encouraged but each company should follow the practices that their internal standards dictate. This document provides generic guidelines under the overmentioned scope, and it does not take into account standards for specific domains, that shall be adapted when applicable.

The proposed guidance hereunder can be applied, if needed, to the extent these elements are relevant to the Products only (i.e. partners in charge of the applications development shall check case by case if the methodology is relevant and applicable). This guidance briefly identifies best practices on five major aspects while dealing with SSDLC such as: Threat modelling and risk assessment, SSDLC for development, Testing, Deployment and Methodology. To complete the guidance some criteria to comply with the SSDLC.

In the light of cooperation and sharing knowledge, when relevant the proposed methodology can be included in public deliverables and disseminated, in order to share R²D² best practices with the scientific community and other Horizon Europe projects in the power system domain.

Threat modelling and Risk Assessment

- Conduct threat modelling to identify potential security threats and vulnerabilities in the application's design and architecture.

- Perform a risk assessment to prioritize identified threats based on their potential impact and likelihood.

To this extent, the ENISA taxonomy for the threat modelling can be of use:

<https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view>

SSDLC for development

- Follow secure coding guidelines and best practices during the development phase.
- Regularly perform code reviews to identify and address security and quality issues. Hereunder are some examples of applications that can support this code reviews.
 - o SonarQube to automate static code analysis and identify code vulnerabilities and quality issues.
 - o MendBolt, Dependency checker, and Coverity to scan for security vulnerabilities and dependencies with potential weaknesses.
 - o Mend Renovate to regularly update the libraries used in the project to stay up to date.
 - o Evaluation of the CVSS scores of identified vulnerabilities and prioritize based on risk (using Mendbolt or Coverity)
- Address any findings promptly and ensure fixes are properly tested before integration.

Testing

- Conduct comprehensive testing, including unit testing, integration testing, and security testing.
- Use analysis tools to detect gaps during in the testing (SonarQube, possibly Cypress or others)

Deployment

- Implement security measures specific to the chosen deployment environment, such as Docker.
- Integrate vulnerability scanning for Docker images using tools like Docker Hub's vulnerability scanning feature.
- Ensure proper configuration and hardening of the deployment environment.

Methodology

- Quality checks to be implemented before deployment



D2.3 - Requirements and Detailed Architecture Design

- Dependencies to be checked on a regular basis
- Testing and deployment to be tested

The project's partners can define the criteria to be reached, possibly by applying the checks for the first time and establishing a gap analysis from there.

Proposed criteria

- Coverage: Aim for a coverage rate of 50% to 60% across the codebase.
- Code Smells: Measure code smells by the number of instances per 1000 lines of code. A tolerance of up to 20 code smells per 1000 lines of code is acceptable.
- Bugs
 - Major Bugs: Strive for zero major bugs.
 - Minor Bugs: Allow up to 5 minor bugs per 1000 lines of code.
- Vulnerabilities:
 - Critical Vulnerabilities: Aim for zero critical vulnerabilities.
 - Minor Vulnerabilities: Tolerance of around 3 minor vulnerabilities for the entire project.
- Hotspots Reviewed: Ensure that 80% of identified code hotspots are thoroughly reviewed and addressed.
- Duplications: Keep code duplications under 10% across the project.

By following this methodology, it is possible to systematically integrate security and quality measures into software development process, reducing the likelihood of vulnerabilities and ensuring a higher level of security for the applications.



**Funded by
the European Union**

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Horizon Europe Grant agreement N° 101075714.