R2D2

Reliability, Resilience and Defense technology for the griD

D7.1 - Preliminary Report on Integration, Demonstration and Validation

Date: 30/09/2024

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.

Deliverable details

Title	Responsible Partner	WP	Version
Preliminary Report on Integration, Demonstration and Validation	ELPROS	7	1

Contractual delivery date	Actual delivery date	Delivery type*
30/09/2024		Report

*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
Tadeja Babnik, Bojan Mahkovec	ELPROS
Marija Popović, Goran Jakupović, Milan Josifović	IMP
Ugo Stecchi, Lucas Pons, Pablo Bort	ETRA I+D
Lucia Revert, Luis Burdalo	S2
Mihkel Väljaots, Margo Raja, Priit Anton	GUARD
Kostas Papadatos, Kostas Rantos, George Aslanidis, Eleni Klaoudatou, Konstantinos Koulouris, Angeliki Zapalidi, Evangelos Georgakoudis, Christos Paraskevopoulos	CYBER
Ektor Stasinos, Aris Dimeas, Andrew Syrmakesis	ICCS
Petar Krstevski, Aleksandra Krkoleva	UKIM
Marta Gačić, Kristina Janošević, Predrag Simić, Dušan Prešić, Ismar Sinanović	SCC
Srđan Subotić	EMSS
Dimitrios Stratogiannis, Dimitrios Selimis, Victoras Papadimas, Greg Kanellos, Theofanis Kontopoulos	HEDNO
Anja Korošec, Jurij Curk, Boris Turha	ELEK
Suzana Wallner, Božana Govednik, Urban Pišljar, Anton Žagar	ELOVE
Joao Mateus, Motaz Ayiad	EDP
Mathaios Panteli, Georgios Paphitis, Marios Shimillas	UCY
Anouar Guesrami, Olivier Voron	RTE-i
Dawei Qiu, Danny Pudjianto, Yi Wang, Goran Strbac	ICL

Version	Date	Person	Action	Status*	Dissemination**
V0.1	17/05/2024	Tadeja Babnik	Table of Content	Draft	CO
V0.2	05/06/2024	Marija Popović	Added part related to Sandboxing and digital twins	Draft	CO
V03	02/09/2024	Tadeja Babnik Marija Popović	Document improvements	Draft	CO
V0.4	19/09/2024	Tadeja Babnik Marija Popović	Final improvements before peer review	Version ready for peer review	CO
V0.5	20/09/2024	Mihkel Väljaots Anja Korošec	Peer review	Reviewed version	CO

		Boris Turha Ugo Stecchi			
V0.6	25/09/2024	WP7 Partners	Final contributions	Version interating reviewers comments	CO
V0.7	27/09/2024	Tadeja Babnik, Marija Popović	Finalization	Final version	CO
V1.0	30/09/2024	Ugo Stecchi	Submission	Submitted	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

Deliverable 7.1 describes and compiles the results of the first two tasks of WP7, Task 7.1 "Integration, demonstration and validation coordination" and Task 7.2 "Sandboxing and digital twins" of R^2D^2 project from M19 to M24.

Task 7.1 gathers technical data related to the assets (devices, systems and communications) for each scenario and pilot site. This task also deals with

- description of demo and identified constraints,
- preliminary integration, deployment and demonstration schedule,
- constraints and dependencies and risks,
- deployed software and hardware,
- preliminary demonstration activities.

Task 7.2 implements the controlled environments used for testing purposes in the cases where the demonstration of the R^2D^2 products could disrupt the normal operations of the EPES. For this purpose, are used sandboxing and digital twins.

Based on previous analysis developed in T2.1 "Definition of Business scenarios, use cases and requirements", T2.2 System architecture definition, T2.3 KPI identification and monitoring preparation and T2.4 Pilot sites survey recognition, this deliverable provides an extended and updated description of the demos to be performed under each use case, as well as the definition of the systems, assets and activities necessary to begin running the demos. Following the project iterative approach, two different phases are considered to integrate the project results in the pilot sites: preliminary deployment with preliminary demonstrations, and final deployment with final demonstrations. For each one of the UCs previously defined, useful information about description of testing, targets, scope and approach (with the criteria for the definition, execution and evaluation phases). The two stages have been planned with a monthly pace, according to the scheduling and deadline of the project. Technical and pilot Partners worked in a coordinated way to provide possible constraints and risks, along with the identification of HW and SW components to be deployed. Feedback gathered from the first phase will be used to refine the integrated solutions and introduce improvements in the following phase.

After analysis of the sandboxes and digital twins in the power systems and collected information from R^2D^2 involved partners, the results of T7.2 are presented in this deliverable

as the systematic overview of sandboxes and digital twins per pilots, with the focus on their architecture and the infrastructure which will be provided for enabling secure and controlled environments for testing R²D² tools.

Finally, this deliverable takes in consideration the pilot change suffered by the beneficiary EDP. Considering EDP Spain will leave the Project and it will be replaced by E-Redes (another DSO in Portugal belonging to the same EDP group) a Grant Agreement amendment is under preparation meanwhile this deliverable is completed and submitted. This change has been already discussed with Project Officer and the request for the GA Amendment is included in the interim review result.

Keywords

Integration, Deployment, Planning, Demonstration, Schedule, Sandboxing, Digital twins.

1 Table of contents

1.1 LIST OF TABLES

1.2 LIST OF FIGURES

1.3 ABBREVIATIONS / ACRONYMS

Abbreviation / Acronym	Description
AC-CFM	AC Cascading Failure Model
ADR	Automated Detection and Response
AMI	Advanced Metering Infrastructure
APT	Advanced Persistent Threat
C3PO	R^2D^2 product: Multi-risk assessment framework for power systems
CARMEN	S2 tool for anomaly detection and threat hunting.
CCTV	Closed Circuit Television
CGM	Common Grid Model
CIM	Common Information Model
CMD	Command Prompt
CPU	Central Processing Unit
CROSA	Coordinated Regional Operational Security Assessment
CSm	Cost-Sharing methodology
CTI	Cyber Threat Intelligence
D	Deliverable
D1	Low-energy discharge
D2	High-energy discharge
DC OPF	DC Optimal Power Flow
DER	Distributed Energy Sources
DGA	Dissolved Gass Analysis
DL	Deep Learning
DLR	Dynamic Line Rating
DMS	Distribution Management System
DSO	Distribution System Operator
EMMA	R2D2 product: Enhanced maintenance and asset management tool
AC-CFM	AC Cascading Failure Model
EPES	Electric Power and Energy System
ER	Emergency & Restoration
ER-SSM	Emergency & Restoration - System Split module
eTNA	Enterprise Transmission Network Analyser
FW	firmware
GCS	Ground Control Station
GIS	Geographic Information System
GUI	Graphical User Interface
HMI	Human Machine Interface
HV	High Voltage
IA	Artificial Intelligence
ICCP	Inter-Control Centre Communications Protocol
IGM	Individual Grid Model
IR	Infrared
IRIS	R^2D^2 product: Resilience suite for TSO and DSO
IT	Information Technology
KPI	Key Performance Indicator
KSI tool	Tool developed by GUARD providing data signing
Tokenization tool	Tool developed by GUARD providing data tokenization

LFSM-O	Limited Frequency Sensitivity Mode – Over-frequency
LTE	long term evolution
LV	Low Voltage
M	Month
MCDA	multi-Criteria Decision Making
MinIO	Open-source object storage solution designed for high-performance
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
MV	Medium Voltage
NTL	Non-Technical Losses
O&M	Operation and Maintenance
OF	Operator Fabric
OFGS	Over-Frequency Generation Shedding
OFP	Over-Frequency Protection
OFPM	Over-frequency protection module
OLP	Overcurrent Line Protection
OP	Outage planning
OPA	Outage Planning Application
OPC	Outage Planning Coordination
OPDB	Outage Planning Database
OPDE	Operational Planning Data Environment
OPF	Optimal Power Flow
OPO	Outage Planning Optimization
OPP	Optimal PMU Placement
OPR	Outage Planning Processor
OT	Operational Technology
OXL	Over Excitation Limiters
PCAPs	Packet Captures
PD	Partial Discharge
PDC	Phasor Data Concentrator
PMU	Phasor Measurement Unit
PowSyBl	Power System Blocks is an open-source library based on GitHub platform UC 35
PQEL	Power Quality Emission Levels
PRECOG	R2D2 product: Prevention Systems For Energy Infrastructures Security
PTDF	Power Transfer Distribution Factor
PV	Photovoltaics
R^2D^2	Reliability, Resilience and Defense technology for the griD
RA	Remedial Action
RACS	Remedial Actions Cost-Sharing
RCC	Regional Coordination Centre
RES	Renewable Energy Sources
RGB	Red Green Blue
RSC	Regional Security Coordinator
RACS	Remedial Action Cost Sharing
SCADA	Supervisory Control and Data Acquisition
SCADA-ADMS	Supervisory Control and Data Acquisition/Advanced Distribution Management System
SLAM	Advanced Smart Meter
SPD	Surge Protection Device
T	Task
TASE.2	Telecontrol Application Service Element
TSC	Transient Stability Calcul
TSC	Transient Stability Calculation
TSO	Transmission System Operator
TTA	Topology Transfer Application
UAV	Unmanned Aerial Vehicle
UC	Use Case

UFLS	Under Frequency Load Shedding
UI	User Interface
UniFusion	ELPROS Multifunctional system for telemetric applications
UVLS	Under Voltage Load Shedding
UXL	Under Excitation Limiters
VCLS	Voltage Collapse Load Shedding
VM	Virtual Machine
VPN	Virtual Private Network
CMD	Command Prompt

2 Introduction

2.1 PURPOSE OF THE DOCUMENT

Deliverable D7.1 describes the results of work performed within Task 7.1 "Integration, demonstration and validation coordination" and Task 7.2 "Sandboxing and digital twins" of R^2D^2 project from M19 to M24.

The methodology for providing the information presented in this document for Task 7.1 is based on the template "Description of demos, identified constraints and preliminary demonstration" which is used for each R^2D^2 use case. The purpose of this template was to identify the current situation of developed products for implementation and demonstration in pilot sites together with constrains, dependencies and identified risk(s). Additionally, the temple provides the time schedule of preliminary integration, deployment and demonstration activities. The template also includes information what functionalities will be demonstrated and tested in the preliminary stage of demonstration activities.

The approach for providing the information presented in this document for Task 7.2 is based on systematic overview of sandboxes and digital twins per pilot sites. The focus is on their architecture and the infrastructure which will be provided for enabling secure and controlled environments for testing developed R^2D^2 tools.

The first part related to the Task 7.1 reports the planning of the integration, deployment demonstration and validation activities to be performed in R^2D^2 project. Moreover, a description of demos with identified constraints, dependencies and risks, together with deployed software and hardware for each use case is included to update the information provided in D2.2 [3.] and D2.3 [4.].

The second part related to Task 7.2 reports planned sandboxing and digital twins' activities which will include setting up the real-time systems' equivalents on a smaller scale but keeping the full range of functionalities and interfaces between components.

2.2 SCOPE OF THE DOCUMENT

This deliverable comprises the planning of the integration, deployment and demonstration activities for the four R^2D^2 products in four demonstration sites following the use cases which were defined in previous WPs. This includes also identifying the existing systems and facilities to be integrated with R^2D^2 products, and the software and hardware needed to ensure a suitable deployment and commissioning.

Following the project iterative approach, two phases are considered to integrate the project results in the pilot sites: preliminary deployment with preliminary demonstrations, and final deployment with final demonstrations. Feedback from the first phase will be used to refine the integrated solution and introduce improvements in the second phase.

Sandboxing and digital twins will be utilized for testing various types of EPES risks before the tools are demonstrated in the real users' systems, as well as for providing a secure, controlled and isolated environment for the tools whose demonstrations could disrupt the normal operations of EPES and cannot be validated in real-world scenario.

2.3 STRUCTURE OF THE DOCUMENT

The document is organized into seven chapters, references and one annex.

Chapter 1 provides a table of contents.

Chapter 2 presents a brief description of the purpose, scope and structure of the document.

Chapter 3 summarises the R^2D^2 products and their use cases together with pilot sites.

Chapter 4 provides for each use case demo sites, identified constrains and preliminary demonstration. Additionally, is provided with the time schedule related to assets integration, product integration integrated ecosystem preliminary deployment and final deployment as well as a preliminary and final demonstration.

Chapter 5 presents the template which will be used for reporting preliminary and final demonstration results.

Chapter 6 presents the digital twins and sandboxing which will be used to demonstrate use cases which cannot be tested and demonstrated in a real environment due to security reasons. Digital twins and sandboxes are represented by each Pilot site, providing the list of tools belonging to different R^2D^2 products.

Chapter 7 provides the conclusions and next steps.

The final two chapters contain references and an annex.

3 Summary of products and their use cases

3.1 R^2D^2 PRODUCTS

This chapter summarises R^2D^2 products and their use cases.

3.1.1 Multi-risk assessment framework for power systems (C3PO)

The enhancement of resilience in Electrical Power and Energy Systems (EPES) is becoming increasingly critical due to the increasing frequency of extreme weather events and cyberattacks. These events can jeopardize the reliable operation of the system, compromise its infrastructure integrity and have damaging effects on various stakeholders and end customers.

C3PO comprises an advanced toolkit to encompass both physical resilience and cybersecurity assessment and enhancement tools.

C3PO product contains the following tasks and tools:

1. Security assessment through advanced IT technologies – Cyber Risk Assessment Tool.
    a. Cyber Risk Assessment
    b. OPDE Risk Register
2. Dynamic Cyber-Risk Status Evaluation.
3. Spatial and Temporal Modelling and Quantification of Cascading Physical Events.
    a. Spatial and temporal event and fragility modelling
    b. Cascading modelling and quantification
    c. Event simulator of a progressing wildfire and assessment of its impact on the distribution system
4. Resilience-driven investment and operational planning to mitigate or prevent cascading effects.
    a. Resilience-driven investment and operational planning to mitigate or prevent cascading effects.
    b. Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling
5. Operation and Planning of Advanced Multi-Energy micro-grids for Enhancement of Resilience.
6. Knowledge sharing – Cyber Threat Intelligence and cascading events.

3.1.2 Resilience suite for TSO and DSO (IRIS)

IRIS Resilience Suite is designed to enhance the resilience of Transmission System Operators (TSOs) and Distribution System Operators (DSOs) in the context of the evolving energy landscape. As the integration of Renewable Energy Sources (RES) increases and TSO and DSO operations become more interconnected, the need to enhance collaboration to manage crisis situations (disruptions such as cyberattacks and natural disasters, etc.) becomes crucial. IRIS addresses the challenges faced by TSOs, DSOs, and Regional Security Coordinators / Regional Coordination Centres (RSCs/RCCs) during crises, emergency & restoration processes, and multi-energy planning coordination.

IRIS product contains the following tools:

1. Optimal resources coordination for TSO and DSO
    - DSO-TSO congestion and power quality coordination in the application of system services
    - Crisis situation coordination tool
2. Emergency & Restoration
    - Enhancement in DER control and management systems to participate in flexibility procurement schemes
    - Improving LV network observability based on the billing metering system by means of a secure interface with SCADA/ADMS system
    - Over-Frequency Protection Module
    - Phasor angle monitoring tool
    - Optimal PMU Placement Application
    - Emergency & Restoration - System Split Module (ER-SSM)
    - OperatorFabric communication platform
    - Remedial Action tool
3. Multi Energy TSO-DSO planning coordination
    - OperatorFabric communication platform, IGM-DER tool
    - TSO-DSO planning coordination suites

3.1.3 Prevention Systems For Energy Infrastructures Security (PRECOG)

PRECOG product is a collection of cyber-security related tools.

Tools serve two specific objectives defined in the R^2D^2 project – contributing to the improvement of the overall security and resiliency in the power system (SO1) and increasing the cyber-security and cyber-resilience in OT and IT of the EPES (SO3) [2].

PRECOG product contains following tools:

1. Identification and authentication of energy IoT and edge devices
    - KSI tool – developed and implemented by GUARD, providing integrity validation
    - ETER tool – developed and implemented by ETRA, providing IoT management and secure data transfer
2. Energy tokens and trading certificates security

- Tokenization tool – developed and implemented by GUARD, providing data tokenization and data immutability verification

3. Cyber-security events management tools
   - CARMEN tool – developed and implemented by S2
   - Upgraded UniFusion platform developed and implemented by ELPROS
4. Deep learning data analytics for security
   - CARMEN tool
5. Device origin and supply chain
   - Sandbox tool – developed and implemented by CYBER
   - Self-assessment tool – composed by CYBER

3.1.4 Enhanced maintenance and asset management tool (EMMA)

EMMA product contains following tools:

1. Equipment inspection through autonomous image acquisition
   - EMMA ARGOS: tool is to assist in the predictive maintenance of the field assets.
   - EMMA SURVEILLANCE Tool aims to perform manual segmentation of photos captured at regular intervals (approximately every hour) by a fixed camera pointed at a substation, utilizing thermal imaging and identification of substation components hotspots.
2. Optimal Asset management
   - EMMA DYML Tool to perform predictive maintenance by generating alarms for possible malfunctions of the substation's components based on SCADA system and DGA.
   - EMMA ETER is an ETRA portfolio product for distribution system operators, aiming facilitating the monitoring and control of the modern grid effectively.
3. Resource management in case of critical events
   - EMMA GIMAN Tool
4. Maintenance coordination and planning
   - Outage planning (OP) Tool
   - Power Quality Emission Levels (PQEL) Tool
   - Remedial Actions Cost-Sharing (RACS)Tool
   - Transient Stability Calculation (TSC) Tool
   - Topology Transfer Application (TTA)
   - Dynamic Line Rating (DLR) Tool

3.2 PRODUCTS AND THEIR USE CASES

In the following sections are tables summarizing R^2D^2 tools verse use cases.

3.2.1 C3PO

C3PO Tools vs Use cases	UC22	UC23	UC24	UC25	UC26	UC29	UC30	UC32	UC39
Cyber risk assessment tool			✓						✓
Dynamic Cyber-Risk Status Evaluation				✓					
Quantification of Cascading Physical Events	✓					✓			
Resilience-driven investment and operational planning		✓					✓		
Operation and Planning of Advanced Multi-Energy micro-grids								✓	
Knowledge sharing					✓				

3.2.2 IRIS

IRIS Tools vs Use cases	UC7	UC10	UC11	UC12	UC15	UC16	UC18	UC19	UC21	UC35	UC32
DSO-TSO congestion and power quality coordination in application of system services			✓								
Crisis situation coordination tool										✓	
Enhancement in DER control and management systems	✓										
Improving of LV network observability based on billing metering system		✓									
Over-Frequency Protection Module				✓							
Phasor monitoring tool						✓					
Optimal PMU Placement Application							✓				
Emergency & Restoration - System Split module (ER-SSM)								✓			
Remedial Action tool									✓		
OperatorFabric Communication platform, IGM-DER tool					✓						
TSO-DSO planning coordination suites											✓

3.2.3 PRECOG

PRECOG Tools vs Use cases	UC10	UC27	UC28	UC33	UC34	UC36	UC37	UC38	UC40
KSI tool		✓				✓			
Tokenization tool							✓	✓	✓
CARMEN tool		✓		✓	✓				
UniFusion platform	✓								
Sandbox tool		✓							
Self-assessment tool			✓						
ETER tool									✓

3.2.4 EMMA

EMMA Tools vs Use cases	UC1	UC2	UC3	UC4	UC5	UC6	UC8	UC9	UC13	UC14	UC17	UC20	UC31
EMMA ARGOS	✓		✓										
EMMA SURVEILLANCE						✓						✓	
EMMA DYML		✓				✓							
EMMA ETER		✓		✓									
EMMA GIMAN		✓		✓	✓	✓						✓	
OP Tool							✓						
PQEL Tool								✓					
RACS Tool									✓				
TSC Tool										✓			
TTA											✓		
DLR Tool													✓

4 Description of demos, identified constraints and preliminary demonstration

4.1 INTRODUCTION

This chapter includes the table for each UC which presents the description of demo and identified constraints together with information regarding the schedule of preliminary integration, deployment and demonstration. It includes:

- Description of demo and identified constraints
  - Description
  - Targets
  - Scope
  - Approach
- Preliminary integration, deployment and demonstration schedule
- Constraints and dependences
- Risks identified at the beginning of testing and validation activities
- Pilot site(s)
- Deployed Software and hardware
- Preliminary demonstration
- Scenario demonstration

Existing assets at pilot sites are already described in D2.2.

4.2 C3PO

This chapter presents the description of demos, identified constraints and preliminary demonstration for R^2D^2 product C3PO.

4.2.1 Use case 24

UC number	24
UC title	Cyber Security Risk assessment on EPES infrastructure
Involved R^2D^2 product(s)	C3PO
Description of demo and identified constraints	
Description Through the UC the EPES operator will identify and assess cyber security risks, measure risks levels and assess the security posture of the target environment, propose risk mitigation measures. 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:	

1. Context Establishment: 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. Context Modelling: 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. Assessment, Evaluation and Treatment of Risks: 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 R^2D^2, to demonstrate their contribution towards risk reduction.

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 modelling 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.

Targets

- 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.

Scope

- One R^2D^2 product (C3PO)
- HEDNO test environments

Approach

1. Definition:
    1.1 Identify key partners and stakeholders and assign roles and responsibilities.
    1.2 Detailed definition of targets, scope and evaluation criteria.
    1.3 Determine a detailed schedule.
    1.4 Documentation to be delivered.
2. Execution:
    2.1 Perform use cases according to the defined scenarios.
    2.2 Keep key actors and stakeholders informed across the process.
    2.3 Examine the usability of the solution.
    2.4 Record results and document the process.
3. Evaluation:
    3.1 Review and analyse the results with relevant partners and stakeholders.

3.2 Assess KPIs 3.3 Report key findings and lessons learnt
Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences
• None
Risks
• Target environment information unavailability
Pilot site(s)
• Greece: HEDNO, Xanthi

Deployed Software and hardware	
Software	C3PO
Hardware	N/A
Preliminary demonstration	
• Tool, assets & assessment specifications established with Pilot • Pilot will use tool to run test assessments	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.2.2 Use case 39

UC number	39
UC title	OPDE Risk Register
Involved R^2D^2 product(s)	C3PO
Description of demo and identified constraints	
Description In order to protect operational planning data from cyber-attacks, ENTSO-E developed Operational Planning Data Environment (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 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 (OPDE Risk Register) that could support and improve monitoring and communication during risk treatment process that is currently established on the ENTSO-E level.

Targets

- 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

Scope

- One R^2D^2 product involved: C3PO;
- Connection between two C3PO modules: OPDE Risk Register and Cyber Risk Assessment tool;

Approach

1. Definition:
    - 1.1 Detailed definition of input data necessary for preliminary demonstration.
    - 1.2 Detailed definition of timeline.
    - 1.3 Definition of integration and preliminary demonstration test cases.
    - 1.4 Definition of expected results
2. Execution:
    - 2.1 Perform predefined test cases.
    - 2.2 Record results and document the process
3. Evaluation:
    - 3.1 Review and analyse the results with relevant partners.
    - 3.2 Compare expected results with real outcomes to see how they meet success criteria.
    - 3.3 Calculate predefined KPI.
    - 3.4 Remove detected bugs in the IT tool and related databases.
    - 3.5 Report key findings and lessons learnt

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences	
• OPDE Risk Register tool must be ready • Cyber Risk Assessment tool must be capable to export results that are needed for the OPDE Risk Register tool	
Risks	
• No significant risks	
Pilot site(s)	
• Serbia: SCC	
Deployed Software and hardware	
Software	Web application developed in ScriptCase, with PostgreSQL as database, and Dovecot mail server for communication. Operational system for Virtual machine is Linux Centos 7
Hardware	Virtual machine with following specifications: 4 vCPUs, processor type Intel Xeon E5620 2.40GHz, RAM 16 GB, storage 20 GB
Preliminary demonstration	
• Preliminary demonstration will cover all designed functionalities of OPDE Risk Register tool, except risk information import from .csv file (final demonstration will cover this). • Duration of preliminary demonstration will last 5 working days. • Communication between Information Security Body user and Party users will be demonstrated throughout the preliminary demonstration.	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.2.3 Use case 25

UC number	25
UC title	Dynamic Cyber-Risk Status Evaluation considering existing technical vulnerabilities
Involved R^2D^2 product(s)	C3PO
Description of demo and identified constraints	
Description UC25 will facilitate dynamic cybersecurity vulnerability management in the targeted IT/OT environment. The C3PO Dynamic Cyber Risk Evaluation Tool will integrate the asset inventory and their corresponding values provided by the Asset Management Toolkit (T6.2) and/or the C3PO Cyber Risk Assessment Tool (UC24), the technical Vulnerability	

Assessment tool, and the Deep Learning Data Analytics for Security Tool (UC 26, 34) to generate risk scoring for critical assets along with mitigation suggestions.

This Dynamic Risk Analysis will help organizations confront existing and emerging threats targeting vulnerabilities in their environment and propose appropriate mitigation measures to maintain an acceptable security posture. The developed tool will address the requirements of the converged IT-OT environment, considering threats and vulnerabilities specific to the OT environment.

Unlike the static risk assessment demonstrated by UC24 (C3PO Cyber Risk Assessment Tool), the dynamic risk assessment focuses on technical existing and emerging threats and newly identified technical vulnerabilities. It assesses the criticality of a vulnerability and the likelihood of a threat actor attacking an organization's asset to conduct malicious activity. Based on these parameters and the potential impact on the organization, the dynamic risk assessment tool will calculate associated risk levels and provide near real-time visibility into the organization's security posture.

Targets

- Dynamically assess cybersecurity risks by considering collected and analyzed cyberthreats and technical vulnerabilities reported about the environment.
- Suggest mitigation measures.
- To increase the cyber-security and cyber-resilience in OT and IT of the EPES.

Scope

- Two R^2D^2 products involved: Dynamic Risk assessment (T3.2), CARMEN
- Integration with CTI tool and CARMEN

Approach

1. Definition:
    - 1.1 Information about the target environment (assets, impact, infrastructure).
    - 1.2 Deployment of a Vulnerability Assessment tool in the target environment.
    - 1.3 R^2D^2 components that provide input to the Dynamic Risk Assessment tool (Deep learning data analytics, Asset management toolkit) should be deployed to the same environment
    - 1.4 Interfaces with the Asset Management Toolkit (T6.2) and the "Deep learning data analytics for security" tool (T5.4)
2. Execution:
    - 2.1 Identify the target environment
    - 2.2 Dynamic Risk Evaluation data feed provision
    - 2.3 System initialization
    - 2.4 Vulnerabilities Identification
    - 2.5 Dynamic Risk Assessment
3. Evaluation:
    - 3.1 Results from the technical vulnerability assessments
    - 3.2 Analytics from the T5.4 Deep Learning component – Threats likelihood, Vulnerabilities criticalities, Courses of action suggestion
    - 3.3 Asset Value is available from the Cybersecurity Risk Assessment Tool and/or via manual input

3.4 Risks are being calculated for cyber threats that aim to exploit identified vulnerabilities. 3.5 Based on the scoring and the data provided, courses of action are suggested
Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences
• CARMEN integration (T5.3) must be completed • Functional test environment and intercommunication • Data availability
Risks
• Target environment information unavailability • Issues with data derived from CARMEN tool
Pilot site(s)
• Greece: HEDNO, Xanthi

Deployed Software and hardware	
Software	Deep Learning Data Analytics Cyber Threat Intelligence Collection/Sharing System Vulnerability Assessment Tool
Hardware	N/A

Preliminary demonstration
• Establish CARMEN integration • Ensure produced results are correct.
Scenario demonstration

System operators/ distributed energy resources	System operators

4.2.4 Use case 22

UC number	22
UC title	Prevention and mitigation of cascading effects in case of extreme weather events
Involved R^2D^2 product(s)	C3PO, EMMA

Description of demo and identified constraints

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 that derive from a possible extreme weather event are necessary for the R^2D^2 tools to propose the optimal remedial actions for the minimization of potential major outages. 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.

Targets

- Minimization of extreme weather events' impact on the grid
- Mitigation of cascading effects
- Lessons learned for better performance in similar situations

Scope

The scope of this use case is to assess and enhance the resilience of the grid against potential cascading effects, which stem from an extreme weather event. Initially, an assessment of the current state grid resilience is performed, followed by an analysis of the impact of a potential cascading effect, triggered by an extreme weather event simulation. By exploiting R^2D^2 C3PO and EMMA tools, the optimal mitigation measures can be proposed to the network operator and then be investigated, in order to achieve a faster restoration of the network and minimize load shedding and power losses to customers. The available workforce can be optimally intervene to the most critical locations of the damaged infrastructure, so that a faster repair of infrastructure can be achieved.

Approach

1. Definition:
    - 1.1 Detailed definition of targets, scope and evaluation criteria.
    - 1.2 Detailed definition of data needs
    - 1.3 Determine a detailed schedule for tools integration.
    - 1.4 Define necessary documentation to be delivered upon UC finalization.
2. Execution:
    - 2.1 Integration of the tools developed
    - 2.2 Acquisition of necessary data
    - 2.3 Perform simulation test cases and examine the usability of the solution.
    - 2.4 Record results and document the process.
3. Evaluation:
    - 3.1 Investigate extreme weather events mitigation strategies over existing ones
    - 3.2 Calculate KPI(s)
    - 3.3 Report key findings and lessons learned.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

• Data must be available • Tools must be developed • An accurate weather forecast for the area of the grid is available and periodically updated
Risks
• Temporary communication failure between systems • Inefficient communication between C3PO and Weather Service Provider
Pilot site(s)
• Greece: HEDNO
Deployed Software and hardware

Software	R^2D^2 Products: C3PO, EMMA
Hardware	SCADA / DMS, AMI (Isolated environment for the purposes of R^2D^2 project)
Preliminary demonstration	
• Initial assessment of tools functionalities under testing scenarios • Assessment and mitigation of extreme weather event performing simulation test cases	
Scenario demonstration	
System operators/ distributed energy resources	**System operators**

4.2.5 Use case 29

UC number	29
UC title	Event simulator of a progressing wildfire and assessment of its impact on distribution system
Involved R^2D^2 product(s)	C3PO
Description of demo and identified constraints	
Description 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. **Targets** • Provide a flexible modular simulator of wildfire events	

- Evaluate the trajectory of the progressing wildfires and damages on the network infrastructure
- Monitoring of the grid's resilience against such types of extreme events
- Provide an optimal scheduling of available resources to enhance resilience

Scope

- Product involved: C3PO
- Resilience monitoring and enhancement
- Minimization of the extreme event's impact on distribution network
- Enrich T3.3 functionalities which mostly includes windstorm events
- Lessons learned for better performance in similar situations

Approach

1. Definition:
    - 1.1 Detailed definition of targets, scope and evaluation criteria
    - 1.2 Definition of required parameters
    - 1.3 Use the wildfire propagation evaluation module to perform DC OPF and monitor the grid's resilience levels
    - 1.4 Determine the optimal scheduling of available resources to enhance resilience
    - 1.5 Define documentation to be delivered
2. Execution:
    - 2.1 Integration of the Greek Xanthi pilot site
    - 2.2 Integration of the model's required inputs
    - 2.3 Scenario generation and reduction algorithm to generate a wide number of scenarios to capture the uncertainties
    - 2.4 Use the wildfire propagation evaluation module to perform DC OPF and monitor the grid's resilience levels
    - 2.5 Enhance the resilience of the distribution network by providing an optimal scheduling of resources
    - 2.6 Record results and document the process.
3. Evaluation:
    - 3.1 Compare expected results with real outcomes to see how they meet success criteria.
    - 3.2 Calculate KPI(s)
    - 3.3 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- Data and parameters must be available

• An accurate weather forecast for the area of the grid is available and periodically updated
Risks
• Temporary communication failure between systems • Inefficient communication between C3PO and Weather Service Provider
Pilot site(s)
• Greece: HEDNO

Deployed Software and hardware	
Software	R^2D^2 Products: C3PO
Hardware	SCADA / DMS, AMI (Isolated environment for the purposes of R^2D^2 project)

Preliminary demonstration
• Initial assessment of tools functionalities under testing scenarios

Scenario demonstration	
System operators/ distributed energy resources	System Operators

4.2.6 Use case 23

UC number	23
UC title	Cooperative crisis handling in case of cascading event
Involved R^2D^2 product(s)	C3PO

Description of demo and identified constraints

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.

Targets

Proactive mitigation of cascading events

Scope

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

Approach

1. Definition:
    1.1 Detailed definition of targets, scope and evaluation criteria.

1.2 Define necessary documentation to be delivered upon UC finalization.
2. Execution:
2.1 Perform test cases and examine the usability of the solution.
2.2 Record results and document the process.
3. Evaluation:
3.1 Calculate KPI(s)
3.2 Report key findings and lessons learned.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Assets integration is not required in this UC.

Constraints and dependences

- Existence of communication channels between TSO-DSO
- The topology of the network is well known and modelled

Risks

- Temporary communication failure between systems

Pilot site(s)

- Greece: HEDNO

Deployed Software and hardware	
Software	R^2D^2 products: C3PO
Hardware	SCADA/ DMS, AMI

Preliminary demonstration

- Since the outcomes of UC23 are directly linked to the results of UC22, the preliminary demonstration of this UC is already covered by UC22.

Scenario demonstration	
System operators/ distributed energy resources	System operators

4.2.7 Use case 30

UC number	30
UC title	Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling
Involved R^2D^2 product(s)	C3PO

Description of demo and identified constraints

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.

Targets

- Reduce service interruption costs in distribution systems subject to catastrophic events by flexible MG formation and optimal scheduling them
- Boost the restoration process in distribution systems subject to catastrophic events

Scope

- Product involved: C3PO
- Resilience enhancement
- Minimization of service interruption in distribution network subject to extreme weather events
- Enrich T3.4 functionalities with MG-oriented frameworks and a robust restoration strategy
- Lessons learned for better performance in similar situations

Approach

1. Definition:
    - 1.1 Detailed definition of targets, scope and evaluation criteria
    - 1.2 Definition of required parameters
    - 1.3 Flexible MG formation
    - 1.4 Optimal scheduling of formed MGs
    - 1.5 Service restoration strategy
    - 1.6 Define documentation to be delivered
2. Execution:
    - 2.1 Integration of the Greek Xanthi pilot site
    - 2.2 Integration of the simulation model's required inputs
    - 2.3 Flexible MG formation
    - 2.4 Enhance the resilience providing an optimal scheduling of formed MGs
    - 2.5 Enhance the resilience of the distribution network by providing a tailored service restoration scheme
    - 2.6 Record results and document the process.
3. Evaluation:
    - 3.1 Compare expected results with real outcomes to see how they meet success criteria.
    - 3.2 Calculate KPI(s)
    - 3.3 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule																		
Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences
• Data and parameters must be available • Tool must be ready
Risks
• Temporary communication failure between systems
Pilot site(s)
• Greece: HEDNO
Deployed Software and hardware

Software	R^2D^2 Products: C3PO
Hardware	SCADA / DMS, AMI (Isolated environment for the purposes of R^2D^2 project)

Preliminary demonstration
• Initial assessment of tools functionalities under testing scenarios
Scenario demonstration

System operators/ distributed energy resources	System Operators

4.2.8 Use case 32

UC number	32
UC title	Operation and Planning of Advanced Multi-Energy Microgrids for Enhancement of Resilience
Involved R^2D^2 product(s)	C3PO

Description of demo and identified constraints
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.

Targets

- Cost-effectively to enhance the resilience of micro grids with the mobility and flexibility of mobile sources

Scope

- Product involved: C3PO
- Resilience enhancement
- Microgrid
- Mobile sources
- (essential) Load restoration process

Approach

1. Definition:
    - 1.1 Detailed definition of targets, scope and evaluation criteria.
    - 1.2 Definition of required parameters
    - 1.3 Microgrid formation
    - 1.4 Mobile source formation
    - 1.5 Definition of essential & non-essential loads
2. Execution:
    - 2.1 Intergation of the Greece Xanthi pilot site
    - 2.2 Integration of the model's input requirement
    - 2.3 Routing and scheduling of mobile sources
    - 2.4 Optimal power flow of microgrid
    - 2.5 Load restoration process
3. Evaluation:
    - 3.1 Load restoration simulation of essential and non-essential loads
    - 3.2 Operational cost of resilient microgrid
    - 3.3 Calculate KPI(s)
    - 3.4 Report key findings and lessons learnt

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Integrated ecosystem pre-deployment and final deployment are not used in this UC.

Constraints and dependences

- Data and parameters must be ready
- Microgrid formation must be ready
- Mobile source tool must be ready

Risks

• No significant risk	
Pilot site(s)	
• Greece: HEDNO, Xanthi	
Deployed Software and hardware	
Software	R^2D^2 Products: C3PO
Hardware	No
Preliminary demonstration	
• Initial assessment of tool functionalities under testing scenarios	
Scenario demonstration	
System operators/ distributed energy resources	Distribution System Operator

4.2.9 Use case 26

UC number	26
UC title	Cyber Threat Intelligence knowledge collection/sharing with external sources
Involved R^2D^2 product(s)	C3PO
Description of demo and identified constraints	

Description

This UC will demonstrate the capabilities of Cyber Threat Intelligence by collecting, correlating, producing added-value data ready to be ingested by security appliances and further disseminating related information to external parties.

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:

- CTI Source Establishment: Identify CTI sources relevant to the EPES context.
- Information Recipients Establishment: Identify external partners/channels that will receive information collected by the R^2D^2 system.
- Establish Interfaces: Establish connections between the CTI Collection & Gathering system and the Pilot Site defence mechanisms. This will allow the CTI tool to receive Cyber-Security event information from the Pilot Site, and to inform the existing defence mechanisms of received information.

Targets

- Provide a user-friendly, sustainable, and reliable way to receive relevant threat intelligence data from external sources, to be used with other R^2D^2 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.

Scope

- R^2D^2 products involved: C3PO
- 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.

Approach

1. Definition:
   - 1.1 Establish interface between existing security systems and the threat intelligence sharing system.
   - 1.2 Establish CTI communication with external sources.
   - 1.3 Receive CTI from external sources for the needs of R^2D^2
   - 1.4 Share CTI with external sources
2. Execution:
   - 2.1 Begin monitoring the information received by outside sources. Any information received will be analyzed and forwarded to other R^2D^2 modules to assist the creation of added value data.
   - 2.2 Begin monitoring the information generated by the Pilot Site (chosen) defense mechanisms. The information provided by other R^2D^2 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.
3. Evaluation:
   - 3.1 Information regarding threats on the Pilot Site ecosystem is analyzed, filtered, sanitized (to protect sensitive information) and shared to other CTI sources.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- The tool must be ready
- Cyber Threat Intelligence Collection and Sharing System to be successfully deployed to the Pilot Site environment, to both gather and provide CTI
- Data must be available and correctly communicated

Risks

- Issues with Cyber-threat information sharing policy by participating pilot sites

Pilot site(s)

- Greece: HEDNO, Xanthi

Deployed Software and hardware

Software	C3PO CTI Tool
Hardware	N/A

Preliminary demonstration	
• Establish interface between existing security systems and the threat intelligence sharing system in Pilot Site.	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.3 IRIS

This chapter presents description of demos, identified constraints and preliminary demonstration for R2D2 product IRIS.

4.3.1 Use case 11

UC number	11
UC title	DSO - TSO congestion and power quality coordination in application of system services
Involved R^2D^2 product(s)	IRIS, PRECOG
Description of demo and identified constraints	
Description With increased share of volatile RES in the power system, they will together with flexible loads participate in bigger extent in the ancillary services and balancing mechanism. The idea is, that not only TSO or any other actor can directly or indirectly engage ancillary service and flexibility providers in distribution network but also DSO in coordinated way. DSO-TSO Congestion and Power Quality Coordination in Application of System Services: This tool enables DSOs to monitor distribution network conditions, including voltage limits and potential congestions that can impact the availability of flexibility resources used for ancillary services by TSOs. The innovation lies in DSOs informing TSOs about these limitations, enhancing flexibility resource usage for ancillary services, and promoting cross-network collaboration. **Targets** • Estimation of flexibility availability during normal operation and congestion • Provide and send information about possible limitations in DSO network affecting availability of flexible resources (forecasts) • 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. **Scope** • Two R^2D^2 products involved: IRIS, PRECOG • Integrate 77 smart meters into SCADA/ADMS system over UniFusion system	

Approach

1. Definition:
    - 1.1 Check key partners and stakeholders and assign roles and responsibilities.
    - 1.2 Detailed definition of targets, scope and evaluation criteria.
    - 1.3 Determine a detailed schedule.
    - 1.4 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform use cases according to the defined scenarios.
    - 2.2 Keep key actors and stakeholders informed across the process.
    - 2.3 Examine the usability of the solution.
    - 2.4 Record results and document the process.
3. Evaluation:
    - 3.1 Review and analyse the results with relevant partners and stakeholders.
    - 3.2 Compare expected results with real outcomes to see how they meet success criteria.
    - 3.3 Calculate KPI(s)
    - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- The tool must be ready
- Assets must be operational and ready for sending data.

Risks

- Communication failures between different systems.

Pilot site(s)

- Slovenia: ELEK

Deployed Software and hardware

Software	R^2D^2 products: IRIS, PRECOG UniFusion system as communication gateway
Hardware	Server with UniFusion system

Preliminary demonstration

- Based on measurements close to real-time (1 minute) information from the billing meters, Advanced Distribution Management System (ADMS) provides information about possible limitations in distribution network affecting availability of resources

(forecasts) and definite limitations (on-line measurements) in case of congestions and/or power quality issues in particular part of the network. • ADMS sends limit violation to UniFusion, which sends MQTT message with flexibility restrictions to DSO and all aggregators • Based on limit violation flexibility restriction can be restricted for decreasing consumption (increasing generation) or for increasing consumption • Establish the secure communication between UniFusion and SCADA/ADMS over ICCP/TASE.2 communication protocol
Scenario demonstration
System operators/ distributed energy resources | System operators

4.3.2 Use case 35

UC number	35
UC title	Upstream studies to validate the use of TSO/DSO means during crisis situations
Involved R^2D^2 product(s)	IRIS
Description of demo and identified constraints	

Description

Use Case 35 focuses on enhancing the coordination between Transmission System Operators (TSOs) and Distribution System Operators (DSOs) to prepare and manage crisis scenarios effectively. The primary objective of this use case is to facilitate the validation of remedial actions by both TSOs and DSOs, enabling these actions to be implemented in real-time operations during a crisis.

The use case envisions a common platform where TSOs and DSOs can exchange network models and inputs related to remedial actions, allowing them to validate and coordinate these actions seamlessly before a crisis unfolds. This platform aims to integrate and streamline the decision-making processes related to crisis management, thereby improving response times and the effectiveness of interventions during emergencies.

Targets

- Develop a shared platform for exchanging and validating network models, enhancing collaborative crisis management.
- Ensure that remedial actions are thoroughly reviewed by both TSOs and DSOs before implementation to guarantee effectiveness.
- Reduce the lag between crisis detection and response by utilizing pre-validated actions and streamlined procedures.

Scope

- R^2D^2 product involved: IRIS

Approach

1. Definition:

    1.1 Identify potential crisis scenarios and develop preventive strategies.

1.2 Define the process for preparing and updating network models to be shared between TSOs and DSOs.

1.3 Ensure that all communication channels between TSOs, DSOs, and other stakeholders are open and functioning effectively to manage the crisis dynamically.

2. Execution:

2.1 Use the prepared network models to assess impacts and implement remedial actions efficiently during a crisis.

2.2 Execute the planned strategies and remedial actions during a crisis, utilizing the common platform for real-time data exchange and decision-making.

2.3 Actively manage the crisis using the established communication channels to exchange real-time information and coordinate responses.

3. Evaluation:

3.1 Assess how effectively the network models supported the crisis response. Identify any inaccuracies or outdated elements.

3.2 Preparing the ex post crisis report, documenting the crisis timeline, actions taken, their outcomes, and the overall effectiveness of the crisis response strategy.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Integrated ecosystem pre-deployment and final deployment are not used in this UC.

Constraints and dependences

- The tool must be ready
- Network models for both TSO and DSO must be ready for simulation

Risks

- Missing DSO Network Model: may not be available or sufficiently detailed for simulation.

Pilot site(s)

- Serbia: EMSS and SCC

Deployed Software and hardware

Software	R^2D^2 Products: IRIS PyPowSyBl, MinIO
Hardware	SCC's existing servers explained Annex I – IRIS hosting environment

Preliminary demonstration

• Simulating the exchange of network models between TSO and DSO on the IRIS communication platform to ensure data integrity and real-time usability. • Testing the real-time coordination and validation of remedial actions through simulated crisis scenarios, ensuring that both TSO and DSO models align and function as expected.
Scenario demonstration
System operators/ distributed energy resources System operators

4.3.3 Use case 7

UC number	07
UC title	Enhancement in DER control and management systems to participate in ancillary services procurement schemes for DSO and TSO to improve network operation security
Involved R^2D^2 product(s)	IRIS
Description of demo and identified constraints	
Description Increasing share of DER causing increased fluctuations in the network 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). **Targets** • Set up the system enabling us to procure system services form DER and optimally control them. • Estimation of DER flexibility available during normal operation and detected limits violations • Send command for DER control action in case of emergency **Scope** • One R^2D^2 product involved: IRIS • Involved 4 RES: 3 PV plants and one hydro power plant • Integrate special controller which enable receiving MQTT messages and send limitations to PV inverter or hydro power plant **Approach** 1. Definition: 1.1 Check key partners and stakeholders and assign roles and responsibilities. 1.2 Detailed definition of targets, scope and evaluation criteria. 1.3 Determine a detailed schedule. 1.4 Define documentation to be delivered. 2. Execution:	

2.1 Perform use cases according to the defined scenarios.

2.2 Keep key actors and stakeholders informed across the process.

2.3 Examine the usability of the solution.

2.4 Record results and document the process.

3. Evaluation:

3.1 Review and analyse the results with relevant partners and stakeholders.

3.2 Compare expected results with real outcomes to see how they meet success criteria.

3.3 Calculate KPI(s)

3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- The tool must be ready
- Assets must be operational and ready for sending data.

Risks

- Communication failures between different systems.

Pilot site(s)

- Slovenia: ELEK, ELOVE

Deployed Software and hardware

Software	R^2D^2 product: IRIS, UniFusion system as communication gateway
Hardware	• Server with UniFusion system • Special controllers for limiting PV inverters

Preliminary demonstration

- The flexibility management system at DSO will send information about possible needs for ancillary services. DER should respond accordingly with changing generation of active / reactive power to support grid operation inside allowed limits.

Scenario demonstration

System operators/ distributed energy resources	Distributed energy resources and System operators

4.3.4 Use case 10

UC number	10
UC title	Improving of LV network observability based on billing metering system by means of secure interface with SCADA-ADMS system
Involved R²D² product(s)	IRIS, PRECOG
Description of demo and identified constraints	

Description

SCADA/ADMS needs to have a completely clear picture of the power network state for optimal action in case of events.

An essential part of loads and in the 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.

With Advanced 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.

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.

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.

Targets

- Increased LV network observability based on metering data
- Implementation of procedures which fulfil requirements by the latest standard IEC 62351-3 for communication network and system security in communication protocols IEC 60870-5-104, ICCP/TASE.2 and MQTT.
- Implementation of access filtering from allowed IPs.
- Implementation of multi-level login procedures.

Scope

- Two R²D² products involved: IRIS, PRECOG
- Integrate measurements of 77 smart meters into SCADA/ADMS system over UniFusion system

Approach

1. Definition:

    1.1 Check key partners and stakeholders and assign roles and responsibilities.

    1.2 Detailed definition of targets, scope and evaluation criteria.

    1.3 Determine a detailed schedule.

    1.4 Define documentation to be delivered.

2. Execution:
   - 2.1 Perform use cases according to the defined scenarios.
   - 2.2 Keep key actors and stakeholders informed across the process.
   - 2.3 Examine the usability of the solution.
   - 2.4 Record results and document the process.

3. Evaluation:
   - 3.1 Review and analyse the results with relevant partners and stakeholders.
   - 3.2 Compare expected results with real outcomes to see how they meet success criteria.
   - 3.3 Calculate KPI(s)
   - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- The tool must be ready
- Assets must be operational and ready for sending data.

Risks

- Communication failures between different systems.

Pilot site(s)

- Slovenia: ELEK

Deployed Software and hardware

Software	R^2D^2 products: IRIS, PRECOG UniFusion system as communication gateway
Hardware	• Smart meters with long term evolution (LTE) communication and special firmware (FW) which enables 1-minute close-to-real time measurements • Server with UniFusion system

Preliminary demonstration

- Establish the secure communication between UniFusion and SCADA/ADMS over ICCP/TASE.2 communication protocol
- Improve LV network observability in SCADA/ADMS based on metering data

Scenario demonstration

System operators/ distributed energy resources	System operators

4.3.5 Use case 12

UC number	12
UC title	Emergency & Restoration - Over-frequency protection module
Involved R^2D^2 product(s)	IRIS
Description of demo and identified constraints	

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).

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:

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:
    a. Reduction of active power production on generators (group A)
    b. Disconnection of the generators from the transmission grid (group B)

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.

Targets

- Identify generators that can receive a signal from OFPM and respond to it
- Create a generator response algorithm in case of overfrequency to reduce active power
- Create an algorithm for turning off the generator in case of overfrequency
- Define the conditions that trigger one or the other algorithm, or both algorithms simultaneously

Scope

- R^2D^2 product involved: IRIS / OFPM Tool

Approach

1. Definition:

    1.1 Check key partners and stakeholders and assign roles and responsibilities.

1.2 Detailed definition of targets, scope and evaluation criteria.

1.3 Determine a detailed schedule.

1.4 Define documentation to be delivered.

2. Execution:

2.1 Perform use cases according to the defined scenarios.

2.2 Record results and document the process.

3. Evaluation:

3.1 Review and analyse the results with relevant partners and stakeholders.

3.2 Compare expected results with real outcomes to see how they meet success criteria

3.3 Remove detected bugs in the software and related databases

3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- OFPM tool must be ready
- SCADA system must be available

Risks

- Generating units are not part of the project, their participation in testing is voluntary

Pilot site(s)

- Serbia: EMSS

Deployed Software and hardware

Software	R^2D^2 product: IRIS / OFPM tool SCADA system software
Hardware	Servers

Preliminary demonstration

- Checking the correctness of algorithms for reducing active power and switching off generators in a simulated environment (sandboxing)

Scenario demonstration

System operators/ distributed energy resources	System operators

4.3.6 Use case 16

UC number	16
UC title	Phasor angles monitoring and prevention of instability
Involved R^2D^2 product(s)	IRIS

Description of demo and identified constraints

Description

Sometimes the fulfilment of security criteria 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.

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.

The greater the active power flow between these two observed points, the greater the angle difference measured by the PMUs. 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.

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.

Targets

- Define the parts of the network that have a problem with transient stability
- Determine the places in the network where the PMUs should be installed
- Calculate the critical angle for each pair of PMUs used for transient stability monitoring
- Install PMUs in specific locations in the network
- Carry out monitoring of transient stability in critical parts of the network

Scope

- R^2D^2 product involved: IRIS / SCADA (or WAMS)

Approach

1. Definition:
    - 1.1 Detailed definition of targets, scope and evaluation criteria.
    - 1.2 Determine a detailed schedule.
    - 1.3 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform use cases according to the defined scenarios.

2.2 Record results and document the process.

3. Evaluation:

3.1 Review and analyse the results with relevant partners and stakeholders.

3.2 Compare expected results with real outcomes to see how they meet success criteria

3.3 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- PMUs must be installed
- SCADA/EMS must be prepared to receive PMU measurements

Risks

- No significant risks

Pilot site(s)

- Serbia: EMSS

Deployed Software and hardware

Software	R^2D^2 product: IRIS / Phasor angle monitoring tool, SCADA
Hardware	PMUs and existing SCADA servers

Preliminary demonstration

- Checking the receipt of measurements in the SCADA system (Phasor angle monitoring tool) from PMUs in real time

Scenario demonstration

System operators/ distributed energy resources	System operators

4.3.7 Use case 18

UC number	18
UC title	Optimization of PMU installation points
Involved R^2D^2 product(s)	IRIS
Description of demo and identified constraints	

Description

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.

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 for the given power system to be fully observable.

Targets

- Create or import a network model in the form of a graph (branches and nodes)
- Create an incidence matrix
- Determine the optimized places of installation of PMUs according to the task criteria (in accordance with the use case scenarios)

Scope

- R^2D^2 product involved: IRIS / OPP (Optimal PMU Placement) Tool

Approach

1. Definition:
    - 1.1 Detailed definition of targets, scope and evaluation criteria.
    - 1.2 Determine a detailed schedule.
    - 1.3 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform use cases according to the defined scenarios.
    - 2.2 Record results and document the process.
3. Evaluation:
    - 3.1 Review and analyse the results
    - 3.2 Compare expected results with real outcomes to see how they meet success criteria
    - 3.3 Remove detected bugs in the software
    - 3.4 Report key findings and lessons learnt

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Integrated ecosystem pre-deployment and final deployment are not used in this UC.

Constraints and dependences	
• IRIS OPP tools must be ready	
Risks	
• No significant risks	
Pilot site(s)	
• Serbia: EMSS	
Deployed Software and hardware	
Software	OPP tool
Hardware	Personal Computer
Preliminary demonstration	
• Checking all software functionalities (going through as many algorithm branches as possible) for virtual network (e.g. IEEE network models)	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.3.8 Use case 19

UC number	19
UC title	Emergency & Restoration - System Split module
Involved R^2D^2 product(s)	IRIS
Description of demo and identified constraints	
Description: ENTSO-E rules determine procedures in case of major disturbances. However, their implementation during disturbances is difficult, as there are many complex rules. In addition, new European regulation 2019/943 envisages responsibility for Regional Control Centres (RCCs) in the event of major disturbances, such as: • Supporting the coordination and optimization of regional restoration as requested by transmission system operator. 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, this use case provides the following: • Detection of system split • 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 restoration process after system split. **Targets**	

- Detect system split and initiate TSO-RCC coordination via appropriate tool and according to predefined sequence of steps

Scope

- R²D² product involved: IRIS / Emergency & Restoration – System Split module (E&R-SSm), Communication (Operator Fabric – OF) Tool

Approach

1. Definition:
   - 1.1 Detailed definition of targets, scope and evaluation criteria.
   - 1.2 Determine a detailed schedule.
   - 1.3 Define documentation to be delivered.
2. Execution:
   - 2.1 Perform use cases according to the defined scenarios.
   - 2.2 Record results and document the process.
3. Evaluation:
   - 3.1 Review and analyse the results with relevant partners
   - 3.2 Compare expected results with real outcomes to see how they meet success criteria
   - 3.3 Remove detected bugs in the sofware and related databases
   - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- Emergency & Restoration – System Split module must be ready
- Communication (Operator Fabric – OF) Tool must be ready

Risks

- No significant risks

Pilot site(s)

- Serbia: EMSS, SCC, IMP

Deployed Software and hardware

Software	R²D² product: IRIS / Emergency & Restoration – System Split module (E&R-SSm), OF communication tool, SCADA/EMS
Hardware	Servers

Preliminary demonstration

• Checking Emergency & Restoration – System Split module functionalities • Checking TSO-RCC communication via OF communication tool
Scenario demonstration
System operators/ distributed energy resources | System operators

4.3.9 Use case 21

UC number	21
UC title	Remedial Actions Automation
Involved R^2D^2 product(s)	IRIS
Description of demo and identified constraints	

Description

Transmission element overload is detected in real-time contingency analysis or when a disturbance has already occurred. In this case, the Remedial Action (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.

Targets

- Detect contingency
- Choose appropriate RA from the predefined lists of RAs
- Send signals to SCADA for RA implementation

Scope

- R^2D^2 product involved: IRIS / Remedial Action (RA) Tool

Approach

1. Definition:
    - 1.1 Check key partners and assign roles and responsibilities.
    - 1.2 Detailed definition of targets, scope and evaluation criteria.
    - 1.3 Determine a detailed schedule.
    - 1.4 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform use cases according to the defined scenarios.
    - 2.2 Record results and document the process.
3. Evaluation:
    - 3.1 Review and analyse the results with relevant partners and stakeholders.
    - 3.2 Compare expected results with real outcomes to see how they meet success criteria
    - 3.3 Remove detected bugs in the sofware and related databases
    - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule																		
Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences
• RA tool must be ready • RA database must be prepared • SCADA/EMS system must be available

Risks
• No significant risks

Pilot site(s)
• Serbia: EMSS

Deployed Software and hardware	
Software	R^2D^2 product: IRIS / RA tool SCADA/EMS system
Hardware	Servers

Preliminary demonstration
• Checking all RA functionalities (going through as many algorithm branches as possible) for simulated network congestion and selected remedial actions

Scenario demonstration	
System operators/ distributed energy resources	System operators

4.3.10 Use case 15

UC number	15
UC title	TSO-DSO cooperation in Individual Grid Model creation
Involved R^2D^2 product(s)	IRIS

Description of demo and identified constraints
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:

- 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 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

Targets

- Create DER database
- Carry out DER forecasting
- Harmonize TSO and DSO standpoint on TSO-DSO interface interchange
- Include DER generation in IGM in appropriate way

Scope

- R^2D^2 product involved: IRIS / IGM-DER Tool
- TSO-DSO communcation tool (Operator Fabric)

Approach

1. Definition:
    - 1.1 Detailed definition of targets, scope and evaluation criteria.
    - 1.2 Determine a detailed schedule.
    - 1.3 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform use cases according to the defined scenarios.
    - 2.2 Record results and document the process.
3. Evaluation:
    - 3.1 Review and analyse the results with relevant partners and stakeholders.
    - 3.2 Compare expected results with real outcomes to see how they meet success criteria
    - 3.3 Remove detected bugs in the sofware and related databases
    - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- IGM-DER and OF tools must be ready

• DER database must be created and updated • DER forecasts must be available
Risks
• No significant risks
Pilot site(s)
• Serbia: EMSS
Deployed Software and hardware
Software: R^2D^2 product: IRIS / IGM-DER tool, OF tool
Hardware: Servers
Preliminary demonstration
• Checking functionalities of IGM-DER tool • Checking TSO-DSO communication via OF communication tool
Scenario demonstration
System operators/ distributed energy resources: System operators

4.4 PRECOG

This chapter presents description of demos, identified constraints and preliminary demonstration for R^2D^2 product PRECOG.

4.4.1 Use case 36

UC number	36
UC title	Validation of network model integrity
Involved R^2D^2 product(s)	PRECOG
Description of demo and identified constraints	
Description TSOs create IGMs and then share IGMs with RCCs, which use mathematical methods to generate CGMs. CGMs are then shared with other energy grid participants in order to use them in several different operational planning processes. It is important in every step, where data is stored, shared or used to trust the data integrity. KSI tool is implemented in SCC's premises, where the tool is tested for signing and verification of IGM and CGM files. CSS handles approximately 30 files (and 30 signatures) at once and then registers testing results. **Targets** • IGM (individual grid model)	

- CGM (common grid model)
- SCC's database
- TSO's database

Scope

- One R²D² products involved: PRECOG
- Provide 100% success rate with signing and verification requests

Approach

1. Definition:
   - 1.1 Check key partners and stakeholders and assign roles and responsibilities.
   - 1.2 Detailed definition of targets, scope and evaluation criteria.
   - 1.3 Determine a detailed schedule.
   - 1.4 Define documentation to be delivered.
2. Execution:
   - 2.1 Perform use cases according to the defined scenarios.
   - 2.2 Keep key actors and stakeholders informed across the process.
   - 2.3 Examine the usability of the solution.
   - 2.4 Record results and document the process.
3. Evaluation:
   - 3.1 Measure, review and analyze the results with relevant partners and stakeholders.
   - 3.2 Compare expected results with real outcomes to see how they meet success criteria.
   - 3.3 Calculate KPI(s)
   - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- The tool must be functional
- Required data must be available from pilot partner side
- Assets must be operational and ready for sending data.

Risks

- Communication failures between different systems.

Pilot site(s)

- Serbia: SCC, EMSS

Deployed Software and hardware

Software	KSI tool
Hardware	Virtual machine with following specifications: 2 vCPUs, processor type Intel Xeon E5620 2.40GHz, RAM 4 GB, storage 20 GB
Preliminary demonstration	
Test description	Tool to run as a web service and tested manually and automatically against defined KPIs
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.4.2 Use case 37

UC number	37
UC title	Energy data tokenization
Involved R^2D^2 product(s)	PRECOG
Description of demo and identified constraints	

Description

DSO collects measurements from AMI smart meters with 15 – 30 minutes granularity and then stores the data. When measurement data is being used (for analytics or billing calculations), it is crucial for DSO and other partners to trust the data. Tokenization tool provides extra layer of trust through tokenization.

Targets

- Measurement data from AMI smart meters
- DSOs database

Scope

- One R^2D^2 products involved: PRECOG
- Provide 100% success rate with tokenization and verification requests

Approach

1. Definition:
    - 1.1 Check key partners and stakeholders and assign roles and responsibilities.
    - 1.2 Detailed definition of targets, scope and evaluation criteria.
    - 1.3 Determine a detailed schedule.
    - 1.4 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform use cases according to the defined scenarios.
    - 2.2 Keep key actors and stakeholders informed across the process.
    - 2.3 Examine the usability of the solution.

2.4 Record results and document the process.

3. Evaluation:

3.1 Measure, review and analyze the results with relevant partners and stakeholders.

3.2 Compare expected results with real outcomes to see how they meet success criteria.

3.3 Calculate KPI(s)

3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- The tool must be functional
- Required data must be available from pilot partner side
- Assets must be operational and ready for sending data.

Risks

- Communication failures between different systems.

Pilot site(s)

- Greece: HEDNO

Deployed Software and hardware

Software	Tokenization tool
Hardware	N/A

Preliminary demonstration

Test description	Tool to run as a web service and tested automatically against defined KPIs

Scenario demonstration

System operators/ distributed energy resources	System operators

4.4.3 Use case 38

UC number	38
UC title	DSO grid balancing data tokenization

Involved R²D² product(s)	PRECOG

Description of demo and identified constraints

Description

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). Tokenization tool provides trust for the data through tokenization.

Targets

- Grid balancing data
- DSOs database

Scope

- One R²D² product involved: PRECOG
- Provide 100% success rate with tokenization and verification requests

Approach

1. Definition:
    - 1.1 Check key partners and stakeholders and assign roles and responsibilities.
    - 1.2 Detailed definition of targets, scope and evaluation criteria.
    - 1.3 Determine a detailed schedule.
    - 1.4 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform use cases according to the defined scenarios.
    - 2.2 Keep key actors and stakeholders informed across the process.
    - 2.3 Examine the usability of the solution.
    - 2.4 Record results and document the process.
3. Evaluation:
    - 3.1 Measure, review and analyze the results with relevant partners and stakeholders.
    - 3.2 Compare expected results with real outcomes to see how they meet success criteria.
    - 3.3 Calculate KPI(s)
    - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

• The tool must be functional • Required data must be available from pilot partner side • Assets must be operational and ready for sending data.
Risks
• Communication failures between different systems.
Pilot site(s)
• Slovenia: ELEK
Deployed Software and hardware

Software	Tokenization tool
Hardware	N/A
Preliminary demonstration	
Test description	Tool to run as a web service and tested automatically against defined KPIs
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.4.4 Use case 10

Already described in Section 4.3.4

4.4.5 Use case 33

UC number	33
UC title	Detection of anomalies associated with cybersecurity through the characterization of traffic in the perimeter, levels of control and supervision, operation and in physical environments.
Involved R^2D^2 product(s)	PRECOG
Description of demo and identified constraints	
Description The goal of this use case is to monitor EPES in order 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.	

Targets

- Detecting anomalies using machine learning.
- Developing APT detection in OT with the CARMEN tool.
- Ensuring secure communication protocols in a DSO.
- Deploying tools to monitor system traffic, vulnerabilities, and industrial protocols.
- Alerting the cybersecurity team upon anomaly detection in TSO/DSO/RCC systems.

Scope

- Focus on detecting threats affecting perimeter, control and supervision, operation and environment levels.
- Monitor and analyze traffic at various levels including perimeter and internal networks.
- Better data ingestion and threat detection across perimeter, control, supervision, and operation levels.
- Identify APTs in industrial environments.

Approach

1. Definition:
    - 1.1 Check key partners and stakeholders and assign roles and responsibilities.
    - 1.2 Detailed definition of targets, scope and evaluation criteria.
    - 1.3 Determine a detailed schedule.
    - 1.4 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform use cases according to the defined scenarios.
    - 2.2 Keep key actors and stakeholders informed across the process.
    - 2.3 Examine the usability of the solution.
    - 2.4 Record results and document the process.
3. Evaluation:
    - 3.1 Measure, review and analyze the results with relevant partners and stakeholders.
    - 3.2 Compare expected results with real outcomes to see how they meet success criteria.
    - 3.3 Calculate KPI(s)
    - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- Data from the SCC/EMSS pre-production environment
- PCAPS from ELEK
- Data from sandbox tool

• Developments made in T5.3	
Risks	
• Required data may not be available from the pilot partner side. • Assets may not be operational or ready for sending data.	
Pilot site(s)	
• Serbia: SCC, EMSS • Greece: HEDNO • Slovenia: ELEK	
Deployed Software and hardware	
Software	R^2D^2 Products: CARMEN Tool, Sandbox tool
Hardware	• Deploy a sandbox environment for safe data analysis and simulation. • Set up digital twin models and ensure they generate data streams for CARMEN. • Deploy a platform for simulating operational conditions and threats.
Preliminary demonstration	
• Testing the real-time coordination and validation of the CARMEN tool to ensure it connects to all data sources, including the sandbox, and verifies that data ingestion, threat detection, and alert generation function as expected.	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.4.6 Use case 34

UC number	34
UC title	Pattern detection and correlation with information from other cyberattacks in order to detect potential threats
Involved R^2D^2 product(s)	PRECOG
Description of demo and identified constraints	
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.	

Targets

- Detect unknown cyber threats (e.g., zero-day threats, APTs) by identifying patterns like known threats.
- Generate alerts for potentially dangerous behaviours that resemble known threats but are not identical, evading traditional cybersecurity tools.
- Enable early detection of threats, allowing for prompt mitigation and recovery actions by cybersecurity teams.

Scope

- Focus on detecting unknown threats affecting perimeter, control, supervision, operation and environment levels, based on their similarity to known threats.
- Utilize data gathered from demo sites and integrate with existing cybersecurity tools.

Approach

1. Definition:
   - 1.1 Check key partners and stakeholders and assign roles and responsibilities.
   - 1.2 Detailed definition of targets, scope and evaluation criteria.
   - 1.3 Determine a detailed schedule.
   - 1.4 Define documentation to be delivered.
2. Execution:
   - 2.1 Perform use cases according to the defined scenarios.
   - 2.2 Keep key actors and stakeholders informed across the process.
   - 2.3 Examine the usability of the solution.
   - 2.4 Record results and document the process.
3. Evaluation:
   - 3.1 Measure, review and analyze the results with relevant partners and stakeholders.
   - 3.2 Compare expected results with real outcomes to see how they meet success criteria.
   - 3.3 Calculate KPI(s)
   - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- Data from the SCC/EMSS pre-production environment
- PCAPS from ELEK
- Data from sandbox tool
- Developments made in T5.3

Risks	
• Required data may not be available from the pilot partner side. • Assets may not be operational or ready for sending data.	
Pilot site(s)	
• Serbia: SCC, EMSS • Greece: HEDNO • Slovenia: ELEK	
Deployed Software and hardware	
Software	R^2D^2 Products: CARMEN Tool, Sandbox tool
Hardware	• Deploy a sandbox environment for safe data analysis and simulation. • Set up digital twin models and ensure they generate data streams for CARMEN. • Deploy a platform for simulating operational conditions and threats.
Preliminary demonstration	
• Testing the real-time coordination and validation of the CARMEN tool to ensure it connects to all data sources, including the sandbox, and verifies that data ingestion, threat detection, and alert generation function as expected.	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.4.7 Use case 40

UC number	40
UC title	IoT data security enforcement
Involved R^2D^2 product(s)	PRECOG
Description of demo and identified constraints	
Description The 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 Tokenization tool signatures of the data 'at the edge' (where it is read, before sending it), and use this token signatures 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.

Targets

- IoT devices opt-in
- Data push/pull
- Data tampering detection and prevention from IoT platform

Scope

- This UC focuses on the IoT devices management activities and how they could benefit from the security enforcement paradigm and the set of tools proposed by R^2D^2. Scope covers the following topics:

Approach

1. Definition:
    - 1.1 Identify smart meter for testing
    - 1.2 Develop man-in-the-middle process gathers MQTT info and applies some change to data
    - 1.3 Develop malicious process at the DSO infrastructure that send fake MQTT messages
2. Execution:
    - 2.1 Start man-in-the middle attack in selected SLAM device. Modify data before being send to DSO
    - 2.2 Start fake messages generator process at the DSO infrastructure
    - 2.3 Wait for some hour to let system receive several fake or malicious messages
3. Evaluation:
    - 3.1 Check that no fake data has been stored in database
    - 3.1 Check that all attack attempts are logged in th system

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- SLAMS are deployed and accessible through VPN
- SLAMS can access Tokenization tool in the Internet

Risks

- Tests affects with the correct behaviour of the system: Fake data is actually stored
- Deployed SLAMS are affected by new features developed and become unresponsive or buggy

Pilot site(s)	
• Greece: HEDNO	
Deployed Software and hardware	
Software	R²D² Products: PRECOG (T5.1) in cooperation with EMMA (T6.2 ETER)
Hardware	ETRA's smart meters SLAM
Preliminary demonstration	
• Validate that SLAMs are updated with new features • Validate that ETER platform is updated with new features • Validate fake messages generation processes • Check performance of Tokenization tool for IoT communication scenario	
Scenario demonstration	
System operators/ distributed energy resources	System Operators

4.4.8 Use case 27

UC number	27
UC title	Monitor communications behaviour of newly deployed components in an EPES staging environment
Involved R²D² product(s)	PRECOG
Description of demo and identified constraints	
Description The "Sandbox Tool" will have the 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. The Sandbox tool consumes the S2 CARMEN tool (T5.4) API to retrieve Deep Learning traffic analytics, which are then processed and formatted to assist Cyber Security Analysts in classifying new components. The Sandbox tool consumes the Guard KSI tool (T5.1) API to sign the hash digest of new software or updates, or to verify the integrity of signed software, ensuring the results' integrity and immutability. 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: 1. Sandbox Deployment: 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. Communications Monitoring: During Sandbox deployment, the communications of the component are monitored by the System.
3. Communications Analysis: 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. Classification
5. A Cyber Security Analyst classifies a component (as Secure/Suspicious/Compromised) according to the traffic, collected and analysed during the defined test period, in the isolated staging environment and for the approved usage scenario. Besides the Deep Leaning analysis, the Analysts compare the collected traffic pattern against the against the baseline communication pattern.
6. Blockchain: Integrity check-values of the deployed components will be managed and safely distributed with the help of blockchain technology. Having assessed the component this information will be safely stored on the blockchain as additional proof of the component's integrity (T5.1).

Targets

- 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.

Scope

- Monitoring communications of newly deployed components to detect and prevent abnormal or malicious behaviour of newly deployed components.

Approach

1. Definition:

    1.1 Detailed definition of targets, scope and evaluation criteria.

2. Execution:

    2.1 Perform use cases according to the defined scenarios.

    2.2 Keep key actors and stakeholders informed across the process.

    2.3 Examine the usability of the solution.

    2.4 Record results and document the process.

3. Evaluation:

    3.1 Review and analyse the results with relevant partners and stakeholders.

    3.2 Compare expected results with real outcomes to see how they meet success criteria.

    3.3 Calculate KPI(s)

    3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences	
• The tool must be ready • Assets must be operational and ready for sending data.	
Risks	
• Misconfiguration or miscommunication between systems	
Pilot site(s)	
• Greece: HEDNO with ICCS, Xanthi	
Deployed Software and hardware	
Software	• Device Origin and Supply Chain Toolkit • Communications Monitoring System • Deep Learning System • R²D² products: PRECOG, CARMEN
Hardware	N/A
Preliminary demonstration	
• Re-enact existing scenarios in a secure sandbox. • Measure produced results and compare with expected results.	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.4.9 Use case 28

UC number	28
UC title	Adapt/Develop EPES specific vendor management & suppliers' audit practices
Involved R²D² product(s)	PRECOG
Description of demo and identified constraints	
Description This UC will use EPES specific vendor management & suppliers' audit practices to evaluate current practices and propose necessary enhancements. 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. **Targets**	

- Prevent supply chain attacks.
- Enhance trustworthiness in supplier practices.
- Identify weaknesses in vendor's development and production practices and minimize exploitability.

Scope

- Use the EPES-specific vendor management & suppliers' audit practices guidelines to evaluate Pilot Site suppliers/vendors.
- One R²D² tool - PRECOG

Approach

1. Definition:
   - 1.1 The pilot site will provide a sandbox system (e.g., test bed) to test the newly deployed components.
   - 1.2 The vendors are actors that provide the Pilot Site with infrastructure components.
   - 1.3 The Pilot Site will use the final system, created by CYBER, to test the communications of all newly deployed components.
2. Execution:
   - 2.1 Both the Pilot Site and the vendors perform self-assessment of their current practices.
3. Evaluation:
   - 3.1 Best practices guidelines developed and implemented for the Pilot Site and evaluated through an assessment tool improving their security posture.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- The tool must be ready
- Assets and sandbox system must be operational and ready for sending data.

Risks

- Issues with communication of deployed components

Pilot site(s)

- Greece: HEDNO, Xanthi

Deployed Software and hardware

Software	• Assessment tool • R²D² products: PRECOG
Hardware	

Preliminary demonstration

• Establish communication between deployed components • Pilots run test assessments
Scenario demonstration
System operators/ distributed energy resources | System operators

4.5 EMMA

This chapter presents description of demos, identified constraints and preliminary demonstration for R²D² product EMMA.

4.5.1 Use case 1

UC number	01
UC title	Improvement in overhead power lines inspection and maintenance using IA applied to UAV-captured images and data
Involved R²D² product(s)	EMMA ARGOS
Description of demo and identified constraints	

Description

UC01 is aimed at testing and validating some functionalities of the EMMA product developed in WP6, T6.1. 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.

Three different types of phenomena can be identified:

- 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:
  - Optical camera: short circuits or faults
  - Thermal camera:
    - lines overheating (matching of thermal images and SCADA data),
    - hot spot on insulators indicating damaged or potential faults
    - partial discharge, and 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”.

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:

- 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).

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.

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.

Targets

- Autonomous inspection of overhead lines.
- Develop a tool combining multi-spectral images acquired though 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.
- Improvement of the maintenance activities (faster and more effective procedure).

Scope

This use case is aiming at identifying different phenomena at the overhead lines infrastructure that might require some maintenance action from the system operator.

The UC covers the identification of:

- 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

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.

Approach

1. Definition:
    1.1 Set path of flight with buffer area to inspect
    1.2 Define the number of flights, heights, and payload (sensors) of the drone
    1.3 Authorization for flights
2. Execution:
    2.1 Perform the use case tests according to the defined scenarios
    2.2 Constant presence of O&M personnel of the selected infrastructure
    2.3 monitoring images acquired to visually assess the quality
    2.4 ensuring good overlap to avoid blind corners and poor density scanner (lidar)
3. Evaluation:
    3.1 Creation of the ortho mosaic (but for lidar)
    3.2 test algorithm with acquired images and double check results
    3.3 KPI calculation and reporting

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Integrated ecosystem pre-deployment and final deployment are not used in this UC.

Constraints and dependences

- Data resolution is high enough to perform calculations.
- Drone flight path is not at the sufficient altitude to have quality data.
- Not having the right flight certificates.

Risks

- Delay in the UC1 scheduling due to unexpected delay in GA Amendment process
- Not being able to detect certain anomalies
- Weather events can delay drone flights
- EMMA GIMAN is not able to receive alarms.

Pilot site(s)

- Portugal: E-REDES

Deployed Software and hardware

Software	R^2D^2 Products: EMMA ARGOS
Hardware	UAV
Preliminary demonstration	
• Validate EMMA ARGOS functionalities described (forest and vegetation detection, electrical anomalies and physical anomalies) based on drone flights done with available data. • Validate communication between EMMA ARGOS and EMMA GIMAN.	
Scenario demonstration	
System operators/ distributed energy resources	System operator

4.5.2 Use case 2

UC number	02
UC title	Substation component status of health calculation based on SCADA measurements and DGA data
Involved R^2D^2 product(s)	EMMA DYML, EMMA ETER, EMMA GIMAN
Description of demo and identified constraints	

Description

This UC 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.

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.

R^2D^2 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:

- 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:
    - 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.

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.

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 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.

Targets

- Integrate with substation automation SCADA systems
- Predict the stress conditions in critical power transformers based on DGA measurements
- Predict the probability of failure in different timespans for power transformers based on DGA measurements
- Automatic detection of component (serious) degradation in real time based on the SCADA measurements
- Alerting and informing operators when a replacement or a maintenance intervention is required through a proper UI
- Increase the reliability and efficiency of the substation

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).

Approach

1. Definition:
   - 1.1 Identify potential signals of degradation over the transformers and define the corresponding alarms to be sent to EMMA GIMAN
   - 1.2 Define the pipeline to train, store and download AI models in real time with the data coming from SCADA
   - 1.3 Ensure connection to SCADA system both for real time and historical data of the electric and temperature measurements.
2. Execution:
   - 2.1 Use the AI models trained to predict the transformer temperature in real time.
   - 2.2 Raise alarms when these predictions are indicating a possible deterioration within the transformer.

2.3 Send alarms to EMMA GIMAN tool in order to show and monitor this information to the maintenance personnel.

3. Evaluation:

3.1 Check with the maintenance personnel if the alarms were true or false positives with KPIs, so the models can be refined.

3.2 Evaluate if the actions taken during the alarm period were successful.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- Have access to a historical dataset of substations measurements and DGA performed.
- Enough historical data is available to build the models.
- Connection to real time SCADA and DGA data is available.
- Thermal variables are available historically and real time.

Risks

- Technical failure of SCADA system.
- Thermal cameras are not displayed correctly.
- Connection to real time measurements breaks.
- EMMA GIMAN is not able to receive alarms.

Pilot site(s)

- Slovenia: ELEK
- Greece: HEDNO

Deployed Software and hardware

Software	R^2D^2 Products: EMMA DYML, EMMA ETER, EMMA GIMAN
Hardware	SCADA

Preliminary demonstration

- Validate EMMA DYML functionalities (early deterioration/degradation detection of incipient failures) using historical data.
- Validate connection to real time data and proper display of monitoring system.
- Validate connection between EMMA DYML, EMMA ETER and EMMA GIMAN.

Scenario demonstration

System operators/ distributed energy resources	System operators

4.5.3 Use case 3

UC number	03
UC title	Malfunctioning detection of PV panels through autonomous UAV image acquisition
Involved R^2D^2 product(s)	EMMA ARGOS
Description of demo and identified constraints	

Description

UC 3 is aiming at detecting 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:

- 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)

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.

During the flight, cameras collect a set of thermal photos and after the mission is completed, they are streamed to GCS. 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.

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:

- Cell anomaly
- Cracking anomaly
- Diode anomaly
- Hot-spot anomaly
- Offline-module anomaly
- Shadowing anomaly
- Soiling anomaly.
- Vegetation anomaly.

After processed, results of the analysis will be sent to relevant databases and shown in a dedicated graphical user interface.

Targets

- Autonomous inspection of PV fields
- Identify PV problems based on the images captured
- Improvement of the maintenance activities (faster and more effective procedure)

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.

Approach

Definition:

1.1 Set path of flight with buffer area to inspect

1.2 Define the height of flights for ortho-mosaic and detailed capturing

1.3 Authorization for flights

2. Execution:

2.1 Perform the use case tests according to the defined scenarios

2.2 Constant presence of O&M personnel of the selected infrastructure

2.3 monitoring images acquired to visually assess the quality

2.4 ensuring good overlap to avoid blind corners and poor density scanner (lidar)or the mosaic reconstruction

3. Evaluation:

3.1 Creation of the ortho mosaic (but for lidar)

3.2 test algorithm with acquired images and double check results

3.3 KPI calculation and reporting

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Assets integration is not required in this UC. Integrated ecosystem final deployment is not used in this UC.

Constraints and dependences

- Data resolution is high enough to perform calculations.
- Drone flight path is not at the sufficient altitude to have quality data.
- Not having the right flight certificates.
- Not having enough validated data to train the models.

Risks

- Not being able to detect certain anomalies in the panels.
- Weather events can delay drone flights.
- New faults, damages not included in IEC 62446-3:2017
- EMMA GIMAN is not able to receive alarms from EMMA ARGOS.

Pilot site(s)

- Greece, Xanthi region

Deployed Software and hardware	
Software	R^2D^2 Products: EMMA ARGOS
Hardware	UAV
Preliminary demonstration	
• Validate EMMA ARGOS functionalities described (anomaly detection on PV panels) based on drone flights done by ourselves.	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.5.4 Use case 4

UC number	04
UC title	Detection of NTL through SCADA and AMI data, from a selected portion of the distribution grid
Involved R^2D^2 product(s)	EMMA ETER, EMMA GIMAN
Description of demo and identified constraints	
Description 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. The main idea is to apply to NTL tool developed in EMMA to the portion of the distribution grids participating as pilot sites. 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. 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. **Targets** • Obtain pattern of load profiles from SCADA and AMI • Developing a DL algorithm for detecting consumption anomalies in LV nodes or lines • Mapping potential thefts over the distribution system (identification of node/line and meter) and inform the operators **Scope** • LV lines under the same MV/LV secondary station	

Approach

1. Definition:
    - 1.1 Define the possible anomalies to be detected in relation to Non-Technical Losses.
    - 1.2 Gather historical validated energy theft data to train the models.
    - 1.3 Define the pipeline to train, store and download AI models in real time with the data coming from SCADA
    - 1.4 Ensure connection to SCADA system for real time data of the electric measurements.
2. Execution:
    - 2.1 Use the AI models trained to assess in real time the status of the selected feeders.
    - 2.2 Raise an alarm when the model has detected an anomaly.
    - 2.3 Send this alarm to EMMA GIMAN to be monitored and alert the maintenance personnel.
3. Evaluation:
    - 3.1 Check if the predictions made by the model are true or false positives, with its corresponding KPI.
    - 3.2 Evaluate if the actions taken during the alarm period were successful.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- Enough historical data is available to train the models.
- Real time data is available to create predictions in real time.
- Smart metering roll-out for full LV system observability.

Risks

- Low accuracy of resulting prediction models.
- The granularity of smar meters and SCADA data is not precise enough to perform the task.
- Real time data is not available.

Pilot site(s)

- Slovenia: ELEK

Deployed Software and hardware

Software	R^2D^2 Products: EMMA ETER, EMMA GIMAN
Hardware	AMI, SCADA

Preliminary demonstration

• Validate EMMA ETER functionalities (Non-Technical Losses) using historical data. • Validate connection to real time data and proper display of monitoring system. • Validate connection between EMMA DYML, EMMA ETER and EMMA GIMAN.
Scenario demonstration

System operators/ distributed energy resources	System operators

4.5.5 Use case 5

UC number	05
UC title	Automated ranking intervention of assets and optimal scheduling (including routing) of intervention workforce to perform maintenance task.
Involved R^2D^2 product(s)	EMMA GIMAN
Description of demo and identified constraints	

Description

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.

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:

- 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

Each criterion will be given a weight and the score for each intervention will be calculated accordingly.

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.

The main input data will be the ranking intervention of assets calculated in the other UC. These interventions will the decomposed in individual maintenance tasks that will be assigned to workers and scheduled so that they are carried out in the most optimal way.

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.

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.

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.

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.

Targets

- 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

Scope

- 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). 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.

Approach

1. Definition:

1.1 Check events registered by EMMA-ARGOS and EMMA DYML

1.2 Check probability failures evaluated by T3.3.1

1.3 acquire static information from the pilot area (critical users, crews, shed location, etc.)

1.4 Setting criteria for prioritization of interventions

2. Execution:

2.1 Perform use cases according to the defined scenario

2.2 Generate the optimal route to mitigate the alarms and the personnel and costs related to it.

2.3 Monitor in real time the status of the maintenance tasks.

2.2 Monitoring the creation of lists and workforce

2.3 include real-time feedback from field operators to update the list

3. Evaluation:

3.1 review intervention lists

3.2 KPIs calculation

3.3 Ex-post assessment on grid's infrastructure

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- Alarms and interventions are correctly received from other tools and products.

Risks

- No alarms and interventions are received

Pilot site(s)

- Greece: HEDNO

Deployed Software and hardware

Software	R^2D^2 Products: EMMA GIMAN, C3PO cascading effects analysis
Hardware	N/A

Preliminary demonstration

- Validate retrieval of alarms and connection to UC 1, 2, 4 and 12.

Scenario demonstration

System operators/ distributed energy resources	System operators

4.5.6 Use case 6

UC number	06
UC title	Substation components degradation detection by analysing images (Conventional & thermal)
Involved R²D² product(s)	EMMA DYML,, EMMA SURVEILLANCE, EMMA GIMAN
Description of demo and identified constraints	

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:

- Defects on electric equipment: power transformers circuit, and breakers, insulators, SPD, disconnectors, if available.
- 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.

Targets

- Develop a tool combining multi-spectral images acquired though 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)

Scope

- This UC 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

Approach

1. Definition:
    - 1.1 Set the areas of the substation to take images and set up the cameras accordingly.
    - 1.2 Ensure connection to real-time videos and images.
    - 1.3 Define the pipeline to train, store and download AI models in real time with the data coming
2. Execution:
    - 2.1 Use the AI models trained to assess in real time the status of the selected equipment.
    - 2.2 Raise an alarm when the model has detected an anomaly.

2.3 Send this alarm to EMMA GIMAN to be monitored and alert the maintenance personnel.

3. Evaluation:

3.1 Check if the predictions made by the model are true or false positives, with its corresponding KPI.

3.2 Evaluate if the actions taken during the alarm period were successful.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- Images have enough resolution and the metadata to train the models and calculate the hot spots.
- Enough historical data is available to build the models.
- EMMA GIMAN correctly receives the alarms.

Risks

- Delay in the UC6 scheduling for Portuguese pilot due to unexpected delay in GA Amendment process
- Thermal cameras are not displayed correctly.
- Real time data connection breaks.

Pilot site(s)

- Portugal: E-REDES
- Greece: HEDNO

Deployed Software and hardware

Software	R^2D^2 Products: EMMA ARGOS, EMMA ETER, EMMA GIMAN
Hardware	Thermal and fixed cameras

Preliminary demonstration

- Validate connection to real time data and proper display of monitoring system.
- Validate the detection of corresponding alarms with data from demonstration period.

Scenario demonstration

System operators/ distributed energy resources	System operators

4.5.7 Use case 8

UC number	8
UC title	Outage planning optimization
Involved R^2D^2 product(s)	EMMA
Description of demo and identified constraints	

Description

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.

In addition, the TSO must coordinate outages with neighbouring TSOs and Regional Coordination Centres (RCCs). The name of this pan-European process is Outage Planning Coordination (OPC).

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.

Within the Horizon 2020 project called TRINITY [13.], 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.

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.

Targets

- Defining the methodology for optimization of outage planning
- Development of software for collecting data on requested outages and for distribution of final results of outage planning - communication tool (Operator Fabric - OF)
- Development of software (OP Tool) for:
    - Visualization of outage planning requests (hourly and yearly view) and results obtained from the security analysis tool (eTNA) through a user-friendly interface

- Manipulation of outage planning requests (as the preparation for running manual/automatic assessment)
- Configuration management (adding and modifying network elements, including EIC vs CIM ID mapping)
- Development of an API for eTNA software that checks the fulfilment of optimization criteria

Scope

- R^2D^2 product involved: EMMA / Outage Planning Optimization tool (OP) Tool, communication tool (Operator Fabric)

Approach

1. Definition:
   - 1.1 Check key partners and stakeholders and assign roles and responsibilities.
   - 1.2 Detailed definition of targets, scope and evaluation criteria.
   - 1.3 Determine a detailed schedule.
   - 1.4 Define documentation to be delivered.
2. Execution:
   - 2.1 Perform use cases according to the defined scenarios.
   - 2.2 Record results and document the process.
3. Evaluation:
   - 3.1 Review and analyse the results with relevant partners
   - 3.2 Compare expected results with real outcomes to see how they meet success criteria
   - 3.3 Remove detected bugs in the sofware and related databases
   - 3.3 Calculate KPI(s)
   - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- OP tool must be ready
- OF tool must be ready
- eTNA must be ready

Risks

- Communication issues between different systems

Pilot site(s)

- Serbia: EMSS, SCC

Deployed Software and hardware

Software	• R^2D^2 product: EMMA / OP tool, OF tool • eTNA power flow calculation software
Hardware	Servers
Preliminary demonstration	
• Checking the functionality of the OF tool • Checking the functionality of the OP tool • Checking the communication between OP tool and eTNA software	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.5.8 Use case 9

UC number	9
UC title	Automation of calculation of emission levels of electricity quality parameters
Involved R^2D^2 product(s)	EMMA
Description of demo and identified constraints	

Description

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).

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.

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.

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.

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.

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.

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. 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.

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.

Targets

- Development of software according to UC scenario

Scope

- R^2D^2 product involved: EMMA / PQEL tool

Approach

1. Definition:
    - 1.1 Detailed definition of targets, scope and evaluation criteria.
    - 1.2 Determine a detailed schedule.
    - 1.3 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform use cases according to the defined scenarios.
    - 2.2 Record results and document the process.
3. Evaluation:
    - 3.1 Review and analyse the results with relevant partners
    - 3.2 Compare expected results with real outcomes to see how they meet success criteria
    - 3.3 Remove detected bugs in the sofware and related databases
    - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Integrated ecosystem pre-deployment and final deployment are not used in this UC.

Constraints and dependences

- EMMA PQEL tool must be ready
- Power quality measurements must be available
- Grid model must be available
- Connecting facility model must be available

Risks	
• No significant risks	
Pilot site(s)	
• Serbia: EMSS	
Deployed Software and hardware	
Software	R^2D^2 product: EMMA / PQEL tool DIgSILENT Power Factory
Hardware	Power Quality meters, servers
Preliminary demonstration	
• Checking all software functionalities: power quality emission levels calculation (compliance simulation scenario), comparation of calculated and measured emission level (compliance monitoring scenario), equivalent grid parameters calculation (in the connection point) scenario	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.5.9 Use case 13

UC number	13
UC title	Cost-sharing of remedial actions with cross-border impact
Involved R^2D^2 product(s)	EMMA
Description of demo and identified constraints	

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.

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).

These network codes become mandatory for the Western Balkans TSO based on:

- Synchronous Area Framework Agreement concluded among TSOs of Continental Europe (April, 2019) – SO GL
- Decision of the Ministerial Council of the Energy Community (Dec, 2022) – CACM

This use case proposes CSm based on 4 elements:

- 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)

Targets

- Defining CSm on the basis of socialization of costs, which is assessed to be adapted to the needs of the region
- Development of software based on the CSm methodology, which would quickly calculate the redistribution of the costs of the implemented coordinated RAs between the involved TSOs in the region
- Development of the TSO-RCC communication tool (Operator Fabric – OF tool)
- Presentation of the methodology and the software to TSOs in the region

Scope

- R^2D^2 product involved: EMMA / RACS (Remedial Actions Cost Sharing) Tool
- TSO-RCC communication tool (Operator Fabric)

Approach

1. Definition:
    - 1.1 Check key partners and stakeholders and assign roles and responsibilities.
    - 1.2 Detailed definition of targets, scope and evaluation criteria.
    - 1.3 Determine a detailed schedule.
    - 1.4 Define documentation to be delivered.
2. Execution:
    - 2.1 Perform testcases according to the defined scenarios.
    - 2.2 Record results and document the process.
3. Evaluation:
    - 3.1 Review and analyse the results with relevant partners and stakeholders.
    - 3.2 Compare expected results with real outcomes to see how they meet success criteria - Calculate KPI(s)
    - 3.3 Remove detected bugs in the sofware and related databases
    - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Integrated ecosystem pre-deployment and final deployment are not used in this UC.
Constraints and dependences
• RACS and OF tools must be ready • eTNA must be ready to calculate PTDF matrixes
Risks
• No significant risks
Pilot site(s)
• Serbia: EMSS, SCC
Deployed Software and hardware

Software	R^2D^2 product: EMMA / RACS tool, OF tool eTNA power flow calculation software
Hardware	Servers

Preliminary demonstration
• Checking all software functionalities (going through as many algorithm branches as possible) for simulated network congestion and selected remedial actions based on fictitious costs • Checking TSO-RCC communication via OF communication tool
Scenario demonstration

System operators/ distributed energy resources	System operators

4.5.10 Use case 14

UC number	14
UC title	Automation of transient stability calculations
Involved R^2D^2 product(s)	EMMA
Description of demo and identified constraints	
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 DIgSILENT Power Factory program), which would automate the described process.

Targets

- Create script to check transient stability in case of self- extinguishing fault
- Create script to check transient stability in case of a fault removed by circuit-breaker operation

Scope

- R^2D^2 product involved: EMMA / Transient Stability Calculation (TSC) script

Approach

1. Definition:
   - 1.1 Detailed definition of targets, scope and evaluation criteria.
   - 1.2 Determine a detailed schedule.
   - 1.3 Define documentation to be delivered.
2. Execution:
   - 2.1 Perform use cases according to the defined scenarios.
   - 2.2 Record results and document the process.
3. Evaluation:
   - 3.1 Review and analyse the results
   - 3.2 Compare expected results with real outcomes to see how they meet success criteria
   - 3.3 Remove detected bugs in the script

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Integrated ecosystem pre-deployment and final deployment are not used in this UC.

Constraints and dependences

- TSC script must be ready

Risks

- No significant risks

Pilot site(s)

- Serbia: EMSS

Deployed Software and hardware

Software	R^2D^2 product: EMMA / TSC script DIgSILENT Power Factory
Hardware	Personal Computer

Preliminary demonstration	
• Checking all software functionalities - Transient stability check for self-extinguishing fault and fault removed by circuit-breaker operation	
Scenario demonstration	
System operators/ distributed energy resources	System operators

4.5.11 Use case 17

UC number	17
UC title	Outage coordination and automated creation of topology files for Individual Grid Models
Involved R^2D^2 product(s)	EMMA
Description of demo and identified constraints	

Description

The goal of this use-case is to devise a way to enter planned outages into the topology file, which includes the following data:

- 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).

Creating a topology file from TTA application should include the following activities:

- 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

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.

Targets

- Adapt the existing Works application for approving requests for outages of network elements and create an interface to the TTA tool
- Create an interface to the Asset Management database
- Develop a TTA tool that imprints topology changes due to approved grid elements outages into the default topology file

Scope

- R²D² product involved: EMMA / Topology Transfer Application (TTA)

Approach

1. Definition:
   - 1.1 Detailed definition of targets, scope and evaluation criteria.
   - 1.2 Determine a detailed schedule.
   - 1.3 Define documentation to be delivered.
2. Execution:
   - 2.1 Perform use cases according to the defined scenarios.
   - 2.2 Record results and document the process.
3. Evaluation:
   - 3.1 Review and analyse the results with relevant partners and stakeholders.
   - 3.2 Compare expected results with real outcomes to see how they meet success criteria
   - 3.3 Remove detected bugs in the sofware and related databases
   - 3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Integrated ecosystem pre-deployment and final deployment are not used in this UC.

Constraints and dependences

- TTA tools must be ready

Risks

- No significant risks

Pilot site(s)

- Serbia: EMSS

Deployed Software and hardware

Software	R²D² product: EMMA / TTA Application 'Radovi'
Hardware	Servers

Preliminary demonstration

- Checking all software functionalities - Making changes to the default topology file based on approved requests for outages of network elements and creating appropriate reports

Scenario demonstration

System operators/ distributed energy resources	System operators

4.5.12 Use case 20

UC number	20
UC title	Physical security enhancement in core network components (Primary Substations) HV/MV and MV/LV substations
Involved R²D² product(s)	EMMA

Description of demo and identified constraints

Description

This Use Cases focuses on physical substation security enhancement through the installation of equipment to 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 visibility or metering equipment to take the necessary actions. Moreover, in the case 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 and to quicker power restoration.

Targets

- Prevention or mitigation of potential infrastructure loss
- Prevention of equipment damage
- Limitation of potential outages
- Minimization of potential cascading effects

Scope

The purpose of this Use Case is the enhancement of physical substation security through the installation of equipment, in order to prevent possible damage to substation infrastructure. One 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 quick notification and 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 the following network infrastructure:

- Primary substations HV/MV
- Secondary substations MV/LV

Approach

1. Definition:
    - 1.1 Detailed definition of targets, scope and evaluation criteria.
    - 1.2 Detailed definition of equipment needs
    - 1.3 Determine a detailed schedule for equipment installation and tools integration.
    - 1.4 Define necessary documentation to be delivered upon UC finalization.
2. Execution:
    - 2.1 Procurement plan of necessary equipment

2.2 Integration of the tools developed with the installed equipment
2.3 Perform test cases and examine the usability of the solution.
2.4 Record results and document the process.
3. Evaluation:
3.1 Calculate KPI(s)
3.2 Report key findings and lessons learned.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Constraints and dependences

- Visibility cameras installed in the perimeter of the HV/MV substation
- Sensors installed to MV/LV substations (e.g. metering devices, accelerometer)
- Data must be available
- Tools must be developed

Risks

- Temporary communication failure between systems

Pilot site(s)

- Greek: HEDNO

Deployed Software and hardware

Software	R^2D^2 product: EMMA,
Hardware	CCTV, NVR Recorder, Sensors

Preliminary demonstration

- Establish RTSP connection between CCTVs and EMMA tool
- Send alarms and incidents detected to EMMA GIMAN

Scenario demonstration

System operators/ distributed energy resources	System operators • HV/MV substation: Physical incident inside or near the substation infrastructure • HV/MV substation: Vandalism attack to primary substation components • Vandalism or theft attack to MV/LV substation • MV/LV substation: physical/natural disaster affecting the substation

4.5.13 Use case 31

UC number	31
UC title	DLR integration with IGMs and SCADA/EMS
Involved R²D² product(s)	EMMA
Description of demo and identified constraints	

Description

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 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:

- 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)
- Visualization, which allows the user to see the data from the DLR server on the website and download it in CSV format
- Integration into the SCADA system, which provides the visual display of dynamic limits
- Installing additional sensors to improve the accuracy of dynamic limits estimation (data exchange between sensors and DLR server is provided by mobile phone provider)

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:

- 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)
- 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).

Targets

- Transfer the current limits calculated by the DLR system to the individual network models (system operation planning)
- Transfer the current limits calculated by the DLR system to SCADA system (real-time system control)

Scope

- R²D² product involved: EMMA / DLR Tool

Approach

1. Definition:

1.1 Detailed definition of targets, scope and evaluation criteria.

1.2 Determine a detailed schedule.

1.3 Define documentation to be delivered.

2. Execution:

2.1 Perform use cases according to the defined scenarios.

2.2 Examine the usability of the solution.

2.3 Record results and document the process.

3. Evaluation:

3.1 Review and analyse the results

3.2 Compare expected results with real outcomes to see how they meet success criteria

3.3 Remove detected bugs in the sofware and related databases

3.3 Calculate KPI(s)

3.4 Report key findings and lessons learnt.

Preliminary Integration, deployment and demonstration schedule

Month:	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
1. Assets integration																		
2. Product integration																		
3. Integrated ecosystem pre-deployment																		
4. Integrated ecosystem final deployment																		
5 Preliminary demonstration																		
6. Final demonstration																		

Integrated ecosystem pre-deployment and final deployment are not used in this UC.

Constraints and dependences

- DLR tool must be ready

Risks

- No significant risks

Pilot site(s)

- Serbia: EMSS

Deployed Software and hardware

Software	R^2D^2 product: EMMA / DLR tool SCADA system
Hardware	Servers

Preliminary demonstration

- Checking all software functionalities (overwriting line limits in SCADA and IGMs using DLR calculated limits)

Scenario demonstration

System operators/ distributed energy resources	System operators

4.6 PILOT SITES, USE CASES AND R2D2 PRODUCTS SUMMARY

C3PO product involves demonstration of 9 UCs tested in 2 pilot sites:

- 8 UCs in Greece,
- 1 UC in Serbia.

IRIS product involves demonstration of 10 UCs tested in 2 pilot sites:

- 7 UC in Serbia,
- 3UCs in Slovenia.

PRECOG product involves demonstration of 13 UCs in 3 pilot sites:

- 5 UCs in Greece,
- 3 UCs in Serbia,
- 5 UCs in Slovenia.

EMMA product involves demonstration of 16 UCs in 4 pilot sites:

- 6 UCs in Greece,
- 6 UCs in Serbia,
- 2 UCs in Slovenia,
- 2 UCs in Portugal.

One UC tested in Greek pilot is involved in two R^2D^2 products, i.e. C3PO and EMMA and two UCs tested in Slovenia pilot are involved in two R^2D^2 products, i.e. IRIS and PRECOG.

5 Demonstration reporting

In the next months of the project the work will be focused on preliminary deployment and testing of the R^2D^2 products in real conditions. The goal of this task is to test a core set of functionalities in four demonstration sites, before to deploy the final version of each solution. Two main targets are:

- to define the tests to be performed with the previously mentioned software products, assets and infrastructure in order to check that the main functionalities work properly,
- to publish the results obtained during the tests.

Procedures how the demonstration activities (preliminary and final) will be reported are summarised in in the template below.

Table 1: Demonstration reporting template

Experiment number	Each experiment will have unique number
Name of the experiment	
UC title	
Preliminary /Final	Is this preliminary or final experiment?
Timeframe	Mention only date of the experiment, examples: • August 2024 • 10/08/2024 – 28/08/2024
Targets	
Actors	Partners and their roles in experiment
R^2D^2 product(s)	Example: EMMA, C3PO
Assets and systems	
Description of the experiment	
Datasets required for the experiment	
Field data to be gathered	
Related KPIs	Examples: KPI_01, KPI_07, et.
Results of the Experiment	
KPIs results	

Graphs, pictures tables, text	
Conclusions	
Provide the conclusion based on the obtained results	
Planning update for Final Demonstration phase	
What you will do in Final demonstration.	
Expected results	
Actual results	
Recorded variances	If variances from expected results exist
Propose remedies	In case thar recorded variances exist

6 Sandboxes and digital twins

6.1 OVERVIEW OF SANDBOXING AND DIGITAL TWINS IN SCOPE OF R²D² PROJECT

This section provides an overview of sandboxes and digital twins. By exploring the literature, particularly their application in the Electrical Power and Energy System (EPES), various definitions of these terms are discussed. This foundational understanding is crucial before delving into the specific sandboxes and digital twins for developed tools of the R²D² project. Despite the rising popularity of these concepts in both research and industry, they remain vaguely represented in various resources, making it difficult to define their precise scope across different domains. To address these challenges, various approaches to sandboxes and digital twins are outlined in the following subchapters, which lay the groundwork for describing the architecture of the tools, aligned with the proposed definitions.

6.1.1 Sandboxing

In a sandbox, security mechanisms are typically used to isolate applications or processes in a controlled environment, preventing them from affecting the host system or other applications. This technique is crucial for testing and development, especially in cybersecurity and software engineering [5.].

Sandboxes are usually employed whenever software components need to be tested or used but cannot currently be verified, meaning they cannot be considered reliable. Examples of sandboxes are encountered, often unknowingly, by users of standard software in their daily use. All popular web browsers (Microsoft Edge, Google Chrome, etc.), standard word processing and spreadsheet tools (Microsoft Word, Microsoft Excel, etc.), as well as the cores of modern operating systems, apply sandboxes to some extent to protect users from malware. Users of virtualized environments, such as VMware Workstation and Oracle VirtualBox, also use sandboxes, even when virtualization is not the primary reason for their use [6.].

In the context of software security, the term sandbox is often vaguely defined. In one of the first papers referencing this term, it was used in the context of the software technique of "fault isolation" between software components interacting in a shared memory space. However, the aforementioned examples of sandboxes in commercial software products provide a much broader definition of sandbox than that used in the literature [7.], and many academic papers have attempted to systematize the term, e.g. in [8.].

According to the reference [8.], most definitions of sandboxes can be divided into two main groups:

- Sandbox in the form of encapsulation
- Sandbox in the form of applying security policies

A sandbox in the form of encapsulation is best analogous to the English term sandbox (a children's play area with sand, which simultaneously protects the child from injury, and the fence around the sandbox prevents sand from spilling into the surroundings). An encapsulated sandbox simultaneously provides protection for the environment from the failure or harmful impact of the isolated software module, and the module from harmful

impacts from external systems. However, in principle, sandboxes usually protect external systems from the unwanted impacts of the isolated ("encapsulated") module. An example of an encapsulated sandbox could be a software module running within a virtualized environment, a virtual machine, which cannot affect external systems (and can simultaneously be protected from external system impacts).

A sandbox in the form of applying security policies implies that there is a software environment and/or hardware equipment that can isolate certain software systems/modules by applying security policies that define what is allowed or prohibited for the isolated system, which resources from the environment it is allowed to access, and which it is not. A possible example of this type of sandbox is software running on a computer behind a firewall with rules defined to isolate it from the rest of the system – the network.

The application of sandboxes in the power industry is originally linked to the use of sandboxes in protecting industrial control systems and SCADA systems, whose security is of extreme importance to the power infrastructure [9.]. Sandboxes in SCADA systems can be applied in the following scenarios:

- Testing and validation: Sandboxes allow safe testing of new software and software patches before deploying them to production SCADA platforms. This way, potential issues can be identified without compromising the active system.
- Malware protection and impact analysis: This allows testing the resilience of SCADA systems to malware in a controlled environment without compromising the production system. By identifying weaknesses and potential security vulnerabilities, preventive measures can be taken to protect the production system from malware attacks.
- Incident response: In case a security breach is identified in the production system, isolating parts of the system can prevent the intrusion from spreading to other parts of the system and allow analysis of the breach in the isolated part of the system. For these measures to be truly effective, it is desirable to have predefined rules and isolation mechanisms, including automatic mechanisms, which would enable quick isolation before the problem spreads to other parts of the system.
- Training and simulation: Sandboxes can be used as training environments for both end users and staff responsible for SCADA system security, allowing them to analyse different scenarios in a simulated and isolated environment and prepare for incident response activities.

For the R^2D^2 project, it was decided that any solution fitting any of these definitions and types of sandboxes would be considered a sandbox.

6.1.2 Digital twins

In the literature, there are multiple definitions of digital twins, but they are not always consistent, and the details of the definition usually depend on the specific industrial sector in which digital twins are applied. The concept of the digital twin has been in use since 2002, when it was utilized in a presentation by the University of Michigan on product lifecycle management [10.].

The concept and terminology of digital twins have not been particularly popular or mentioned in the domain of power systems and power system management until recently, even though the issues of managing and modelling power systems are very interesting for the application of digital twins. It should be noted that models and tools that at least partially

fit the definitions related to digital twins have been used in power system management for decades, but without using the terms and definitions associated with digital twins.

Significant changes in modern power systems have led to increased complexity of the systems and the models that describe them in various domains, leaving the participants in the power systems challenging issues to solve in the domain of management and power system planning. Digital twins have been recognized as one of the ways to overcome these new requirements [11.].

In the literature [12.], a systematic review of the possibilities of applying digital twins in the power industry and definitions of digital twins in the power industry is provided. According to reference[12.], the definition of a digital twin in the power industry is as follows: "A digital twin in the power industry is a virtual representation of an existing or future real object, consisting of identifying components, descriptions of its attributes, and its functional properties. The digital twin is connected to the real object and follows it from the initial idea to recycling. This connection with the real object should be performed autonomously through digital communication infrastructure, although manual indirect connection is also possible."

The digital twin of an object or system consists of two main components: the description of attributes and the functional description, where the attribute description includes the model description and specific attribute values. Access to attributes, as well as attribute processing, for example, within analysis, monitoring, optimization, evaluation functions, is enabled through the functional description.

The model used by a digital twin in the power industry (DTPI) must simulate the behaviour of the physical object or system with sufficient accuracy and fidelity, in accordance with the use case. The primary property of a DTPI is to provide a description of the object's state that can be updated or adjusted throughout the object's lifecycle.

For simulation purposes, a "snapshot twin" can be created, which freezes information from a specific moment in time to perform analyses such as planning, "what-if" scenarios, real-time simulations, training systems, etc. Following the paradigm of storing all information about the real object within the DTPI, the snapshot twin and the results of its simulation should also be stored in the DTPI database.

The above definitions significantly limit what can be considered a digital twin, particularly the restriction regarding the existence of a constant communication interface with the physical system. In this sense, and especially in the context of the connection between digital twins and isolated systems, within the R^2D^2 project, as digital twins are considered both modules and systems that may or may not have a constant connection with the physical system and that perform some functions of digital twins in "simulation mode" as a kind of "snapshot twin."

6.2 TOOLS USED FOR DEMONSTRATION IN PILOT SITE 1 - GREECE

This chapter presents the sandbox and/or digital twins architecture and characteristics for different tools used in Greece pilot.

6.2.1 Specific environment for C3PO product

6.2.1.1 Sandbox for Dynamic Risk Assessment tool (UC25)

For the purpose of UC25, a dynamic cybersecurity vulnerability management tool will be deployed within the sandbox environment provided by the Greek Pilot site. This sandbox emulates a Supervisory Control and Data Acquisition (SCADA) system, integrated with an Advanced Metering Infrastructure (AMI) consisting of smart meters (SLAMs) installed across various sites, including Mesogeia, Kythnos, and Athens city center. The SLAMs are interconnected through a VPN network and collect power system-related data such as active power and voltage measurements from individual households. This isolated sandbox environment offers a secure and controlled space for testing, ensuring the safety of critical IT/OT systems during the development and evaluation phase.

The architecture of the sandbox environment is depicted in Figure 1.

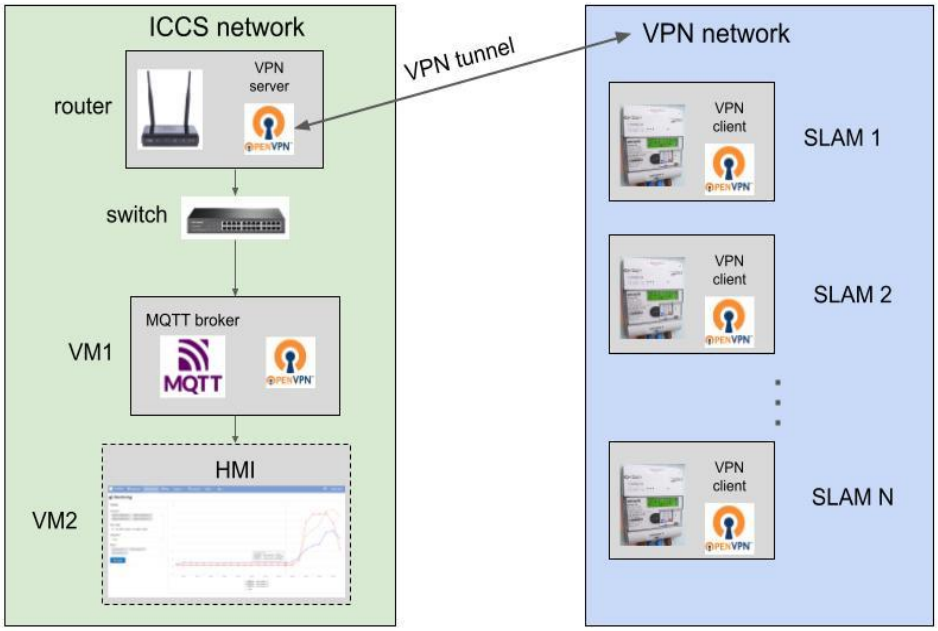

Figure 1: Staging environment high level architecture

As data is collected by the SLAMs, it is transmitted via an MQTT broker located within the same VPN network. A Python-based software application consumes this data and stores it in various dedicated servers (SQL Server, MongoDB, etc.) deployed across the VPN. Each server handles data specific to particular SLAM clusters, ensuring separation of datasets from different locations. These servers expose their data through web-based APIs that serve as the Human-Machine Interfaces (HMIs) for the infrastructure.

The UC25 use case will leverage this secure, isolated environment to facilitate dynamic cybersecurity risk management. This tool will assess the critical assets, calculate risk scores, and offer actionable mitigation strategies for identified vulnerabilities.

This dynamic risk assessment focuses on real-time evaluation of both existing and emerging technical vulnerabilities within the converged IT-OT environment. It assesses the likelihood of threat actors exploiting these vulnerabilities and the potential impact on the organization. Unlike the static risk assessment performed by UC38, UC25 prioritizes continuous, near-real-time updates based on newly discovered vulnerabilities and evolving threats. This allows organizations to maintain a robust security posture by responding swiftly to emerging risks.

6.2.1.2 Digital twin for C3PO cascading simulators (UC22)

Cascading failure models for resilience analysis are critical to simulate cascading events and identify methods to enhance resilience on the power networks. AC Cascading failure model (AC-CFM) is specifically designed for resilience analysis and fits effortlessly into pre-established frameworks for measuring resilience. It can handle large contingencies and extreme conditions by addressing convergence issues. The model is validated by the approaches of IEEE PES working group on cascading failures. A cascading failure is governed by successive activation of protection mechanisms. This can cause disintegration of the network into islands; in which case the cascade may continue within each island independently. The implemented functionalities include:

- Recursive Application of Protection Mechanisms: A cascading failure is governed by successive activation of protection mechanisms. This can cause disintegration of the network into islands; in which case the cascade may continue within each island independently.
- Implementation of Protection Mechanisms: The AC-CFM model applies different types of system protection, including under- and over-frequency load shedding, etc.
- Cascade Visualization: AC-CFM provides a novel way of visualizing cascading failures as a tree-like graph. The graph expresses causalities in cascading failures and helps mitigating the impact of large and wide-spread blackouts.
- Integration into Resilience Metric Frameworks: The straightforward and seamless integration with established resilience metrics enhances comparability and applications of AC-CFM to existing works and is a main advantage over other models, which have not addressed this need.

Figure 2 and Figure 3Figure 2 Figure 2and show the flowcharts of the main steps of cascading model.

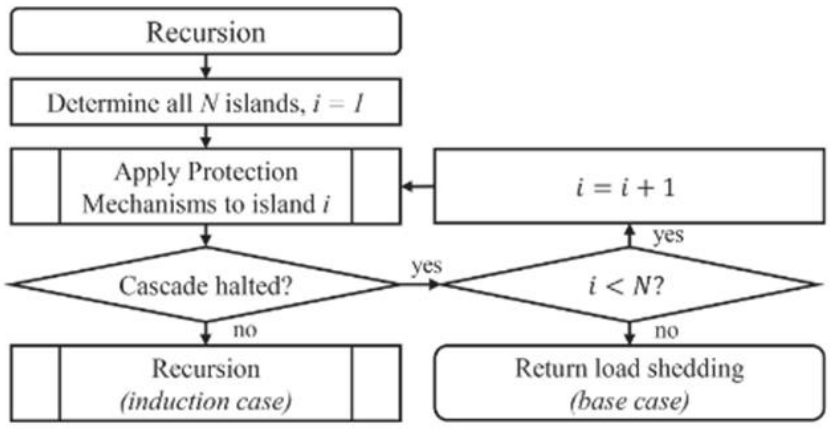

Figure 2: Flowchart illustrating the recursive approach of AC-CFM

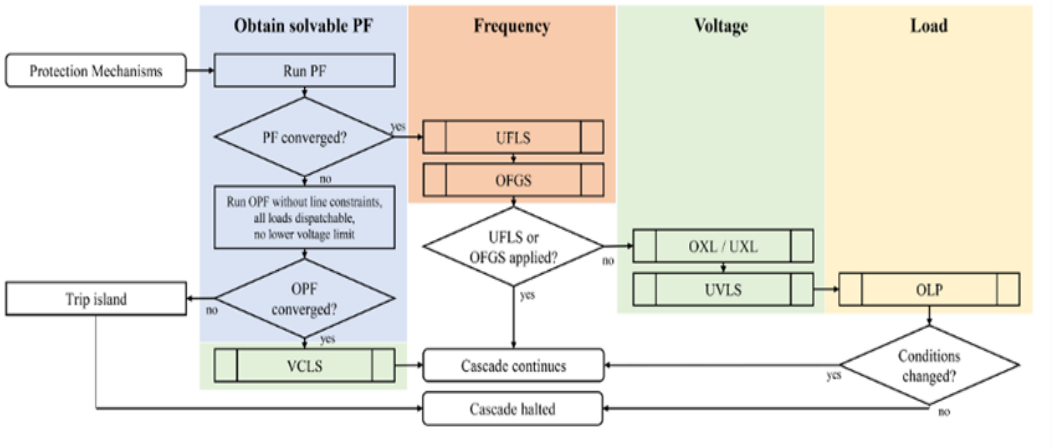

Figure 3: Flowchart illustrating the implementation and succession of protection mechanisms in AC-CFM

For the purpose of the UC22 data provision from the Greek pilot site an on-premises Ubuntu VM will be provided by HEDNO (isolated from the rest of HEDNO systems). Data from the actual SCADA system, along with AMI datasets (collected in HEDNO's telemetry center), involving all telemetered consumers and producers, are available periodically via APIs to the HEDNO IT Department. The aforementioned data is further stored in an additional Data Server Database, thus a replica of the actual systems is provided. As also stated above, the Data Server Infrastructure consists of an isolated environment, where the same security protocols as the actual SCADA & AMI systems are applied.

6.2.1.3 Digital twin for Planning and operation of advanced multi-energy microgrid for resilience enhancement (UC32)

The operation and planning of advanced multi-energy microgrids for enhancement of resilience is a simulation-based tool based on Greece pilot site – Xanthi distribution power network. The tool aims to optimize the pre-positioning as well as the routing and scheduling decisions of mobile sources within the Xanthi network to maximize the load restoration process, with an emphasis on the requirements of essential loads. The detailed architecture of the tool is illustrated in Figure 4. Specifically, the tool includes four steps, which can be described as below:

Step 1: Data collection. The tool will collect the real-world data of the Xanthi network, including the network topology, line resistance and reactance, bus location and voltage, load location and active and reactive power, generator location and active and reactive power capacity, and load types of essential and non-essential loads.
Step 2: Python coding. The tool will construct the network simulation environment based on the Python-Gurobi interface for testing planning and operation strategies for mobile sources as well as the load restoration process of resilience enhancement.
Step 3: Outage scenario. The outage scenarios will be generated to evaluate the load conditions of the entire network based on the Python-based network simulation environment.
Step 4: Resilience strategy. The planning and operation dispatches of mobile sources will be optimized and tested based on the Python-based network simulation environment.

Step 5: Load restoration. The load restoration process of the entire network will be evaluated based on the Python-based network simulation environment once the resilience strategies of planning and operation are implemented.

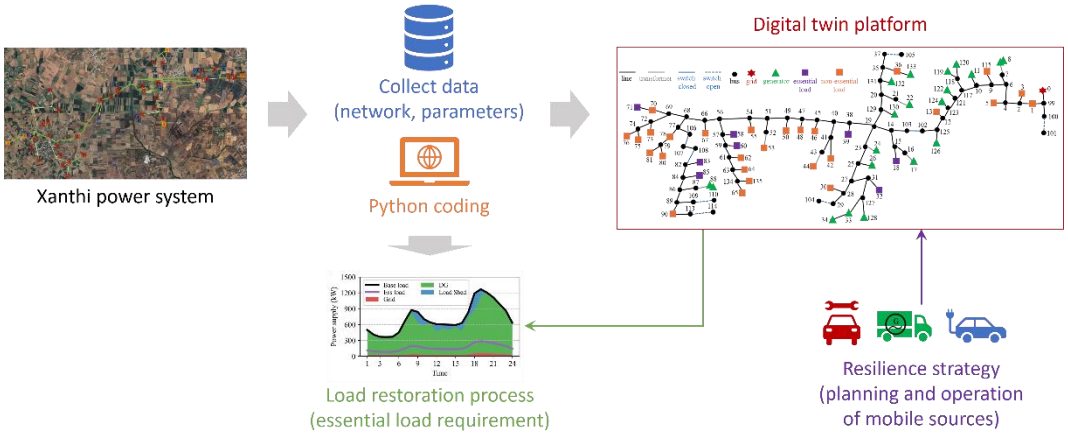

Figure 4: The architecture of the tool for UC32

Digital twin

As it is already stated above, this is a simulation-based tool but using the real-world system and data of the Xanthi power distribution network, it can be claimed as the "digital twin" of the real system. Near real-time data via MQTT communication protocol will be provided. All necessary databases and static data will be used to build up the digital twin platform for the tool. Data of outage scenarios can be generated and manually modified as the inputs for the tool to create a real-time representation of the Xanthi power distribution network.

6.2.2 Specific environment for PRECOG product

6.2.2.1 Sandbox for Sandbox Tool (UC27)

For UC27, the same sandbox environment as described in 6.2.1.1 UC25 will be utilized to test and monitor newly deployed components. This sandbox serves as a staging area where components are deployed in an isolated environment, mimicking operational conditions without impacting production systems.

In UC27, the Communications Monitoring System will observe the interactions of these newly deployed components. Communications will be analyzed in real-time using a deep learning module (T5.4) to identify any anomalies. This process ensures that each component is classified as safe, suspicious, or compromised before full deployment into a production environment.

The analysis is conducted in several phases, starting with the sandbox deployment of the component, followed by communications monitoring, deep learning analysis, and ultimately classification by a cybersecurity analyst. The results are compared to baseline communication patterns to determine the component's safety. Integrity checks for each

deployed component will also be managed via blockchain technology (T5.1), ensuring the integrity of all classified components is safely recorded and traceable.

6.2.2.2 Sandbox for Tokenization tool (UC37)

Regarding the implementation and deployment process of R^2D^2 modules, HEDNO provides all available pilot data, though a continuous process of data integration to each R^2D^2 tool as requested per Use Case. Specifically, as far as Tokenisation tool is concerned, an on-premises Ubuntu VM will be provided by HEDNO, which will be (networking-wise) isolated from the rest of HEDNO systems, thus providing increased security for research Projects purposes. Data from the actual SCADA system, along with AMI datasets (collected in HEDNO's telemetry center), involving all telemetered consumers and producers, are available periodically via APIs to the HEDNO IT Department. The aforementioned data is further stored in an additional Data Server Database, thus a replica of the actual systems is provided. As also stated above, the Data Server Infrastructure consists of an isolated environment, where the same security protocols as the actual SCADA & AMI systems are applied. Testing of UC37 will involve executing binaries on the VM since it is a safe virtualised environment, and collaboration shall then take place with GUARD regarding the DSO's feedback on the results. Figure 5 and Figure 6 below illustrate the Project's data path procedure.

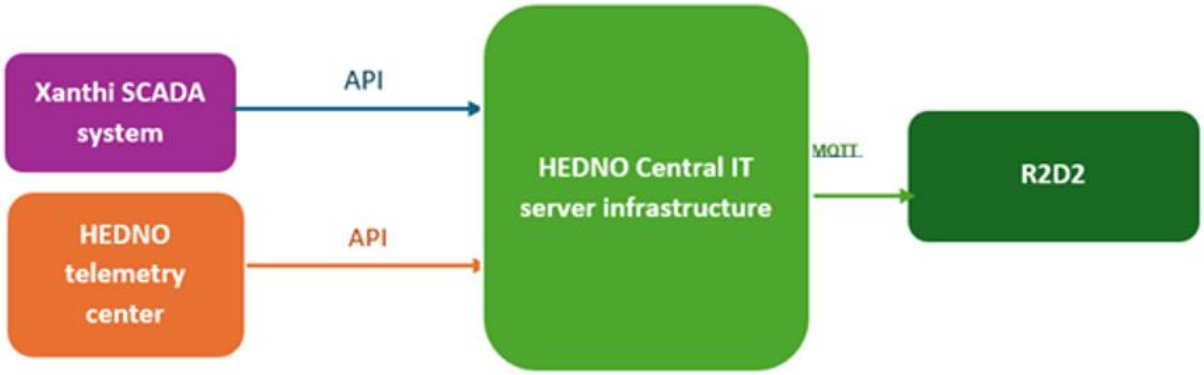

Figure 5: Greek pilot data flow from infrastructure to R^2D^2 tools

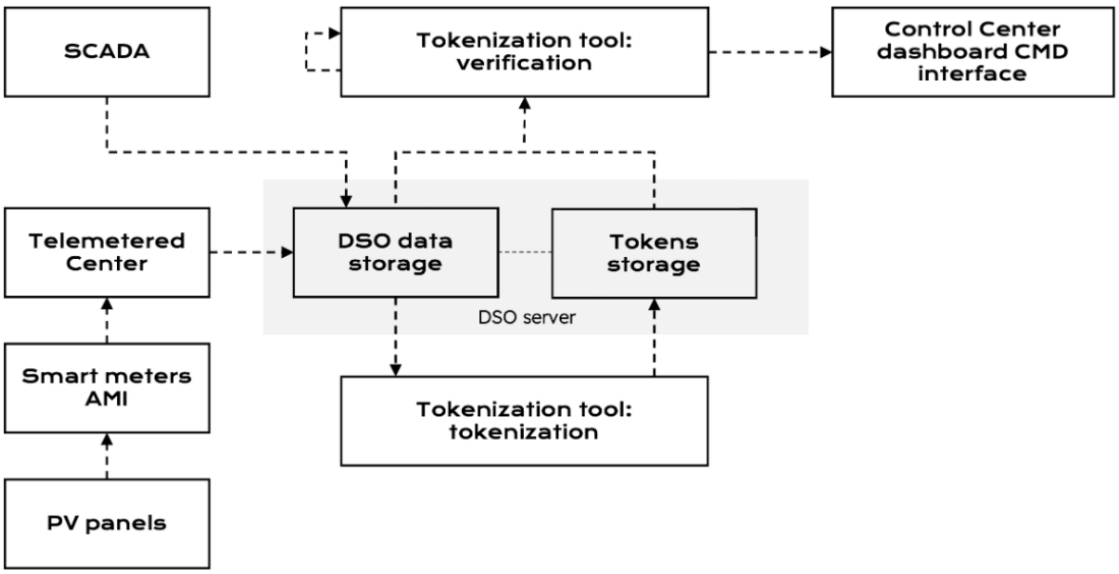

Figure 6: Energy Data Tokenization tool

6.2.3 Specific environment for EMMA product

6.2.3.1 Digital twin for EMMA GIMAN tool (UC5)

Use case 5 is aiming to develop an "Automated ranking intervention of assets and optimal scheduling (including routing) of intervention workforce to perform maintenance task". This will take as input the following data:

- Workforce details (personnel details, vehicles, skills, etc.)
- Location of assets to maintain
- List of tasks to perform by the workforce, including assets affected and location of the intervention. It also includes details like priority of the task, time to complete, users affected, etc.
- Calendar data

The list of tasks is updated continuously, as it reflects the maintenance requirements that appear in the system operation. Tasks can be categorized as follows:

- There are tasks programmed according to a predefined schedule, like periodic cleaning or painting of the assets. These are not depending on the real status of the assets, but are tasks aiming to prevent the assets for failing or degrading
- There are tasks that triggered on the identification of an existing issue with an asset. This identification can be done automatically by some of the systems, manually by the workforce or indirectly by the citizens contacting the DSO. This task involves the duties required to correct or fix the assets to restore the normal behavior of the grid and are normally given a very high priority.
- There are maintenance tasks that appear from the analysis of data or status captured from the assets, like temperate or vibrations. This analysis might lead to the creation of tasks for the workforce to commute to the assets and assess its level of health, eventually applying corrective action if necessary.
- DSO periodically make visual inspections of the assets, with the support of fixed cameras and drones. These inspections are analyzed using AI techniques towards

identifying hidden or beyond-the-eye issues with the assets. This analysis might lead to the creation of tasks for the workforce to commute to the assets and assess its level of health, eventually applying corrective action if necessary.

In real systems this list can become huge, and it is important to cope with all these tasks in an optimal way, considering the limits of human and economical resources for maintenance. The new features developed in R^2D^2 UC5 for the GIMAN tool aims at optimizing the scheduling and planification of the workforce duties.

For the use case to be realistic, a relatively big amount of maintenance tasks is needed, so that optimizations actually make sense and provides a benefit. This is the reason for the creation of a maintenance infrastructure digital twin. It will mimic the behavior of the system from the point of view of how maintenance tasks appear, are assigned to (a limited set of) workers and take some time to complete.

The Digital twin will make the following:

- All real assets will be imported to the digital twin
- On a continuous way, it will randomly generate maintenance tasks by simulating the appearance of problems in the network. This generation will be stochastic and configurable.
- It will also be simulated that maintenance/inspections tasks identified that are not addressed by workers for a long time could evolve to real failures, thus requiring immediate and costly actions. The longer the maintenance/inspection is postponed, the higher the possibility to become an error.
- Some internal features of GIMAN that require maintenance operator actions will be automated, so that the whole process can run unattended
- The behavior of the workers will be simulated. For each one, at the appropriate time, the system will automatically start the next task in GIMAN tool, and close it after a certain time, that considers the commuting time and the repair time (all of this randomized to some extent)

The architecture of this digital twin will have the form of python scripts that simulate the different behaviors. The data and simulated interactions from workforce will reach GIMAN tool through a set of web services developed for this purpose. These web services will allow to:

- Generate the tasks
- Simulate the starting and ending of the tasks

GIMAN will run as if the system will be real and will automatically calculate the optimal schedules according to the simulated current status of the system.

By the usage of this infrastructure, the benefits of the automatic ranking of interventions and the optimization of the duties' executions will be analyzed.

6.3 TOOLS USED FOR DEMONSTRATION IN PILOT SITE 2 – SERBIA

This chapter presents the sandbox and/or digital twins architecture and characteristics for different tools used in Serbian pilot.

6.3.1 Specific environment for IRIS product

6.3.1.1 Digital twin and sandbox for Over-Frequency Protection Module (UC12)

Over-Frequency Protection (OFP) Module within Serbian pilot site is hosted at EMS (Serbian TSO). OFP will be integrated in existing SCADA/EMS system and it will interact with SCADA data (sending commands, receiving necessary telemetry, etc.) as shown in Figure 7.

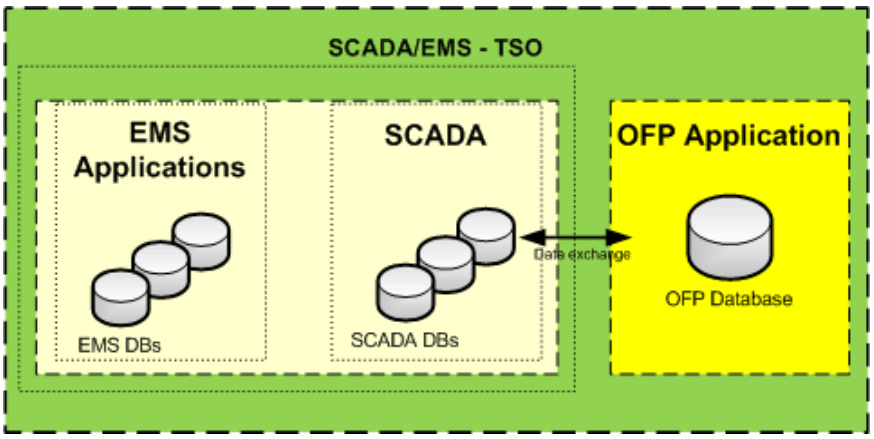

Figure 7: OFP - real-time system

SCADA/EMS system – existing View4 SCADA/EMS system in EMS TSO applications and their databases.
OFP Application - Over-Frequency Protection application with database.

6.3.1.1.1 Sandboxing

The copy of the OFP module will be located on the VM and it will be completely isolated from other parts of the system, and only access to it is to be via VPN or directly from host machine, see Figure 8.

Necessary databases for OFP – databases required for OFP module operation.

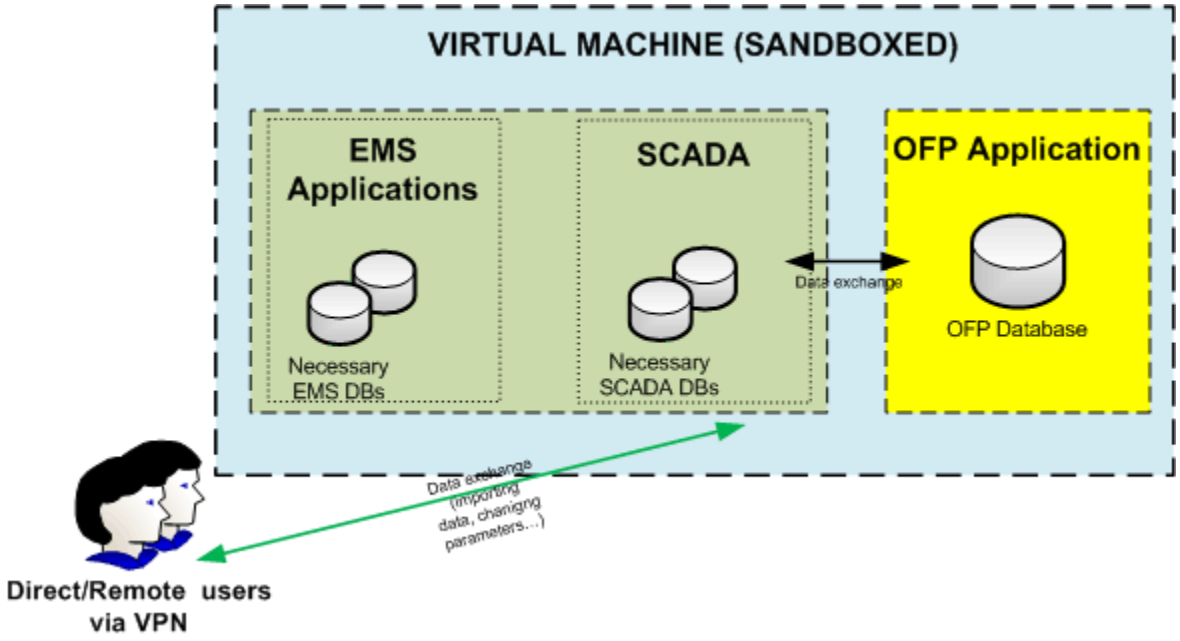

Figure 8: OFP Sandboxed environment

6.3.1.1.2 Digital twin

VM shown in Figure 8 will have copied version of SCADA/EMS system from real time system. It will contain all necessary databases and static data for OFP functionality.

Data from production (real-time) system may be exported into sandboxed environment on VM (snapshot from real system). Data can be modified to create different scenarios for testing response of system. The same mechanism was created in MATLAB/Simulink environment, but this environment was for algorithm testing purpose, see Figure 9.

MATLAB/Simulink – Simulation environment for testing algorithms for OPF module.

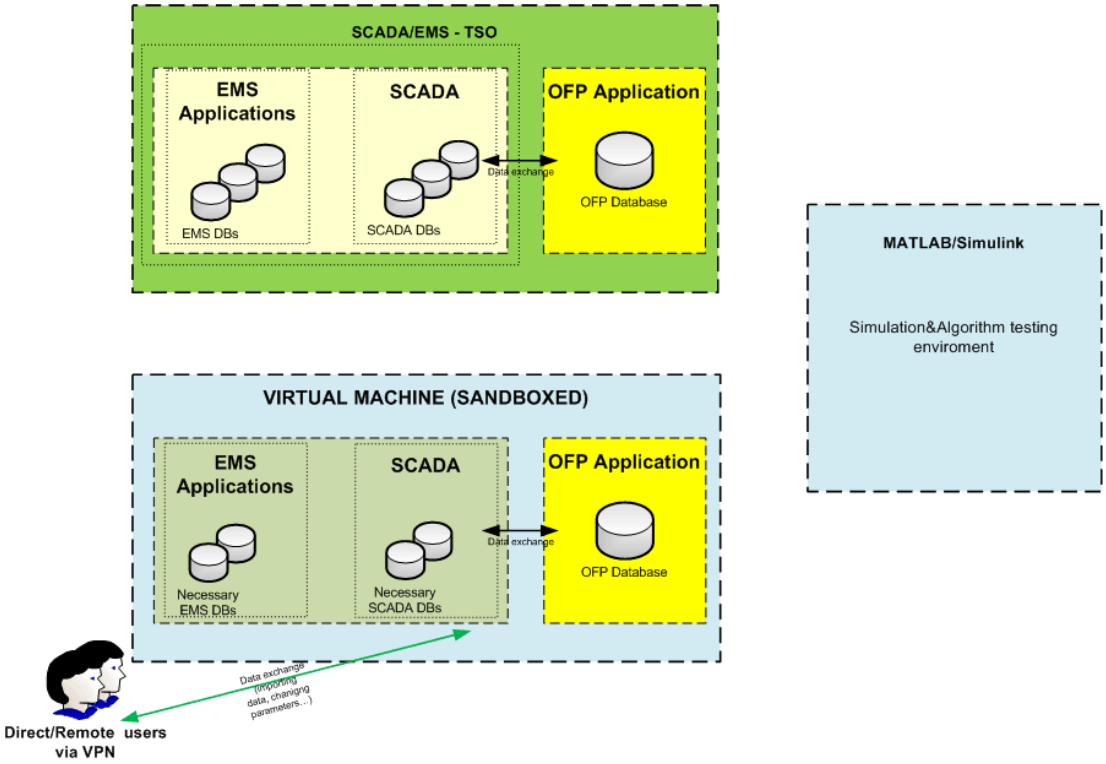

Figure 9: OFP Complete environment

6.3.1.2 Digital twin and sandbox for Emergency & Restoration - System Split module (ER-SSM) (UC19)

Emergency & Restoration - System Split module within Serbian pilot site is hosted at SCC. Overview of network and virtualization at SCC site is given in Figure 10.

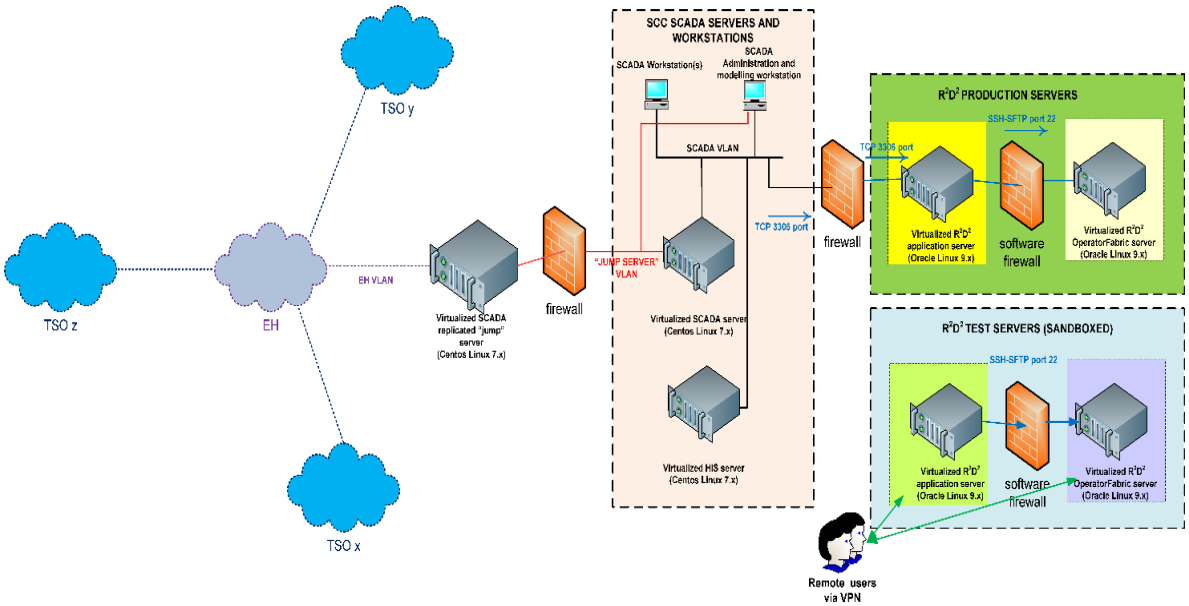

Figure 10: Overview of network and virtualization at SCC site

As it can be seen from Figure 10, production system is separated in three main network security zones:

- **"Electronic highway"** (EH) zone that provides RCC SCADA connectivity with TSO SCADA. This secure zone is isolated from all other SCC networks, only SCADA "jump" server provides connectivity with SCC "production" SCADA server(s).
- **SCADA zone** in which SCC virtualized production SCADA system servers and workstations reside. Only unidirectional link towards R²D² servers is allowed (SCADA-> R²D²).
- **R²D² Zone** where virtualized R²D² servers reside - R²D² production servers and R²D² test servers (sandboxed).

Overview of logical structure of ER System Split tool in production (real-time) is given in Figure 11.

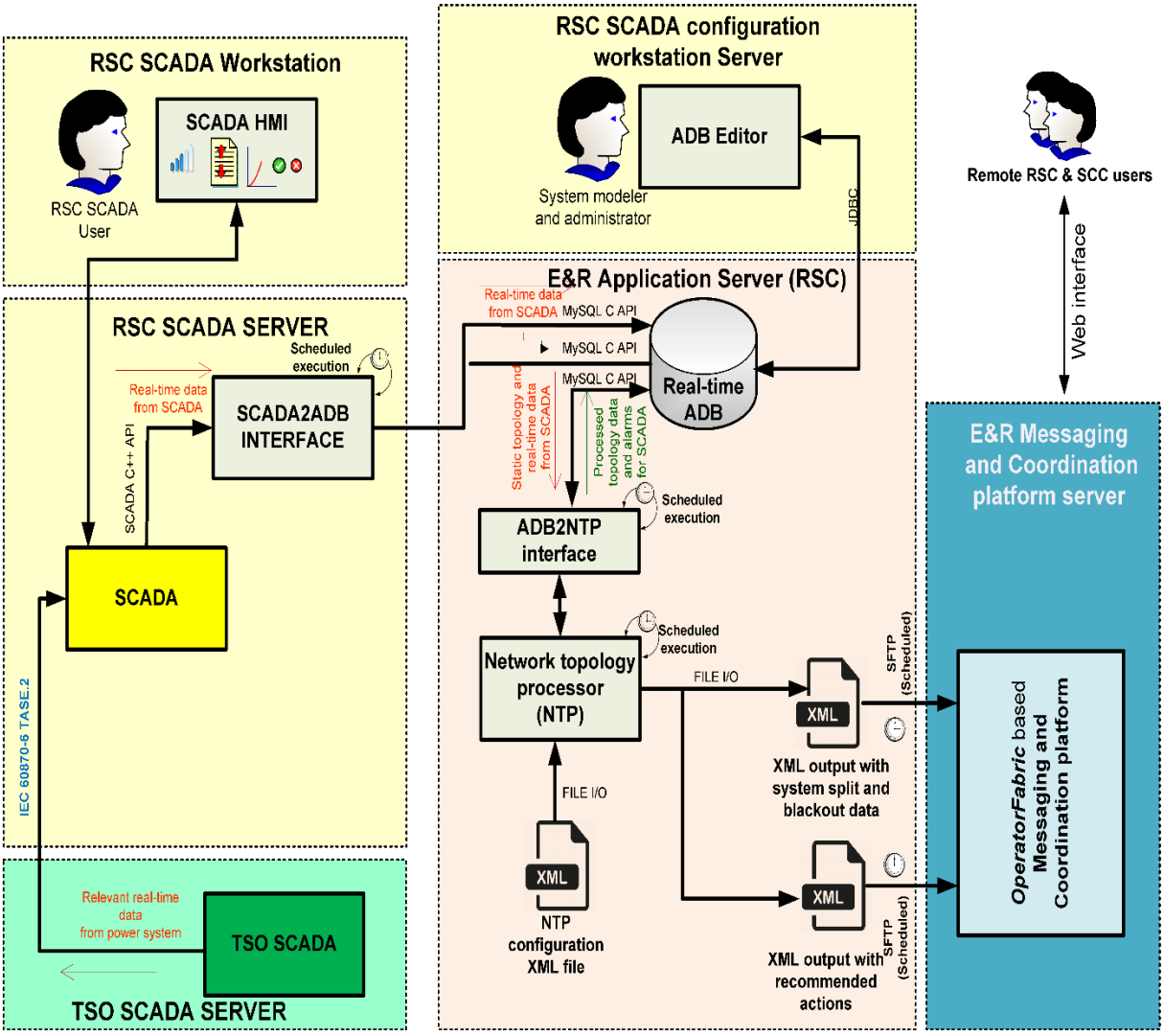

Figure 11: Logical overview of system split module – Production (Real-time) environment

In **production** (real-time) environment following components are used:

- **SCADA system** which provides (provided to RCC via TSO SCADA systems)
  - Relevant telemetry is forwarded to Real-time Application Database (ADB)
  - In Real-time ADB telemetry points are matched with power system model data-points creating digital representation of physical system
- **Real-time ADB** contains static digital power system model
  - Model in Real-time ADB contains power system topology and parametrization of power system components
  - "Digital twin" image of power system state is created when SCADA telemetry is matched with static model
- **ADB Editor in real-time** is used to enter, modify and maintain power system model and to match SCADA telemetry with physical quantities ((re)active powers, voltages, tap changer positions, etc.) and switching equipment states.
- **Network topology processor (NTP)** uses the model in ADB to detect relevant system states and state changes (like the occurrence of system split or total or partial blackout, etc.). It also creates XML exports for Messaging and coordination platform for coordination process.

As seen from Figure 10, there are two R^2D^2 production servers:

- Virtualized R^2D^2 application server – where Real-time ADB, ADB Editor in real-time and Network topology processor will be deployed
- Virtualized R^2D^2 Operator Fabric server – where Operator Fabric instance will be deployed, as well as the accompanying backend applications needed for the communication with OF and NTP

6.3.1.2.1 Sandboxing

While the above presented production environment is reasonably secure, and might be considered as sandboxed, additional test and demonstration Study environment is created **("R^2D^2 Test servers (Sandboxed)"** in Figure 10). This environment is completely isolated from other parts of the system, and only access to it is to be via VPN.

Logical overview of this environment is shown in Figure 12.

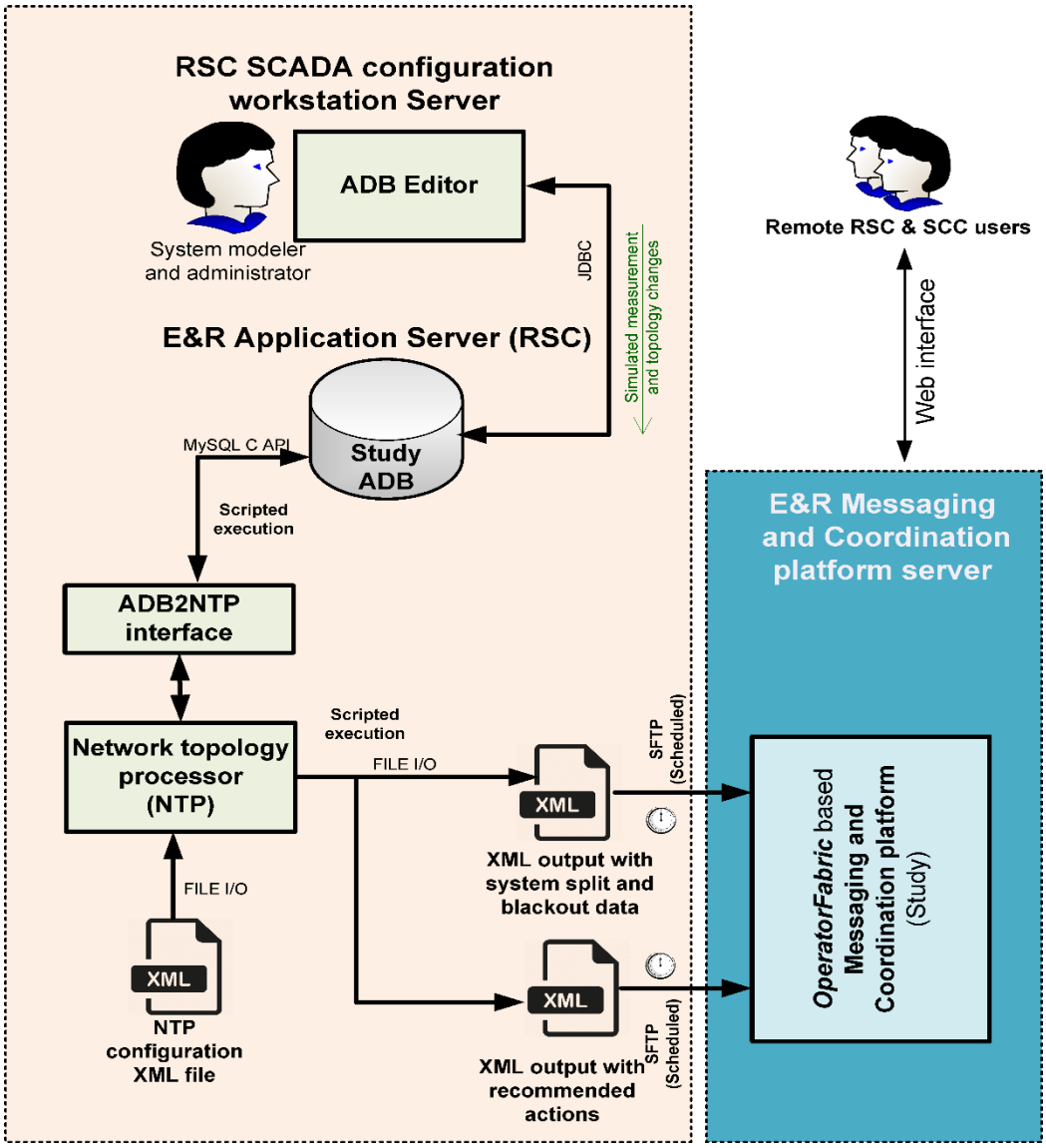

Figure 12: Logical overview of system split module – Study environment (Sandboxed)

In **study (sandboxed)** environment following components are used:

- **Study ADB** that contains static digital power system model, but also Savecase/snapshot of system state in some previous timepoint.
  - Without manipulation of system snapshot the Study ADB represents image of observed power system state "frozen" at some time instance in past
  - By using ADB editor it is possible to manually modify snapshot and to create new system state (for example to create system split by removing tie-lines from operation)
- **ADB Editor in study mode** which is used to modify data in Savecase/snapshot to create new simulated power system state.
- **Network topology processor** in study mode.

6.3.1.2.2 Digital twin

As it is already stated above, ADB database contains a model of power system which may be used as "digital twin" of real system. ADB contains "static" model of network connectivity and relevant parameters of power system equipment. In the production environment real-time and manually replaced data are used to create a real-time representation of the power system state for use by the topology processor and related applications.

Data from production (real-time) system may be exported into "snapshot" which is to be used into Study (sandboxed) environment. This "snapshot" (or save-case) may be also manually modified in order to create different scenarios starting from some actual system state as recorded in some instant.

6.3.1.3 Sandbox for Crisis situation coordination tool (UC35)

Crisis situation coordination tool developed in UC35, together with certain parts of Operation and Planning of Advanced Multi-Energy micro-grids process from UC32 and T4.2 Integration activities will be deployed in SCC's IT system. IRIS hosting environment for these tools is consisted of 3 Kubernetes clusters (master + 3 nodes each) built on Oracle Linux 9.2 VMs with 20GB of disks space. This hosting environment is consisted of 3 environments, each placed in different Kubernetes cluster:

- DEV – Development environment;
- INT – Integration or Acceptance environment;
- TST – Test environment.

IRIS hosting environment is segregated from other R^2D^2 tools testing environments that will be deployed in SCC's pilot site, as well as from SCC's production environment for core business. Access to this environment is provided using controlled VPN users for tool developers, and via web browser using internet access through secure Nginx web server for beneficiaries that will test tool functionalities during demonstration phase of the project.

More non-confidential info about IRIS hosting environment is provided in Annex I – IRIS hosting environment of this document, while detailed confidential design of IRIS hosting environment is provided in document "IRIS suite platform hosting and development" that is available only to the R^2D^2 consortium partners.

6.3.2 Specific environment for PRECOG product

6.3.2.1 Sandbox for KSI tool (UC36)

KSI tool will be deployed in SCC's IT environment in segregated Linux Virtual Machine (VM) where only this tool will be tested. This VM is located on a dedicated IT network which is isolated from other IT networks in SCC used for core business. User access to the mentioned VM will be established only via VPN connection for approved user accounts. VM will also have access to the internet since it is one of the preconditions for proper tool work (in order to obtain necessary information for the creation of signature file, KSI tool must have access to the internet KSI Blockchain).

6.3.3 Specific environment for EMMA product

6.3.3.1 Sandbox for Outage Planning (OP) Tool (UC8)

OP Tool will be deployed in SCC premises, on Oracle Linux Virtual Machine (VM), network-isolated from other systems, providing levels of isolation and security. As VM runs in an isolated environment, the risk of different applications interfering with each other is entirely removed, thus establishing the security of the system, as the application runs without affecting the SCC production system or other VMs.

As another level of security, the services comprising the OP tool will run in a docker environment – creating an isolated virtual docker network. As docker containers encapsulate all dependencies and configurations that are needed to run the application, it ensures that it behaves the same across different environments (development, testing, production). In the case of OP tool, for the development and testing purposes, separate components of OP tool will be sandboxed in docker containers, enabling secure testing on a local environment, before deploying the application on SCC premises.

The components of OP tool are:

- Outage Planning Application (OPA) - frontend application in charge of visualization and manipulation of the outage plans.
- Outage Planning Processor (OPR) - (backend application in charge of processing all necessary data, preparation of input files for eTNA, and communication with other components.
- Outage Planning Database (OPDB) - database collecting outage plans and network elements.

These three components will be deployed in three docker containers, forming a docker network.

Besides OP tool, two additional applications will be integrated in the entire system:

- Operator Fabric (OF) – used for the gathering of outage planning requests and distribution of the final results of the outage planning coordination process. OF consists of several services, each of these running in separate docker containers.
- eTNA software – used for performing the security analysis on a chosen set of inputs. eTNA is used only in the production environment (deployed in SCC premises), and for the testing (sandbox) environment, separate mock service will be created – on a certain combination of inputs, it will provide corresponding outputs and will be wrapped in a docker container.

Figure 13 depicts OP tool comprising components of production / sandbox environment.

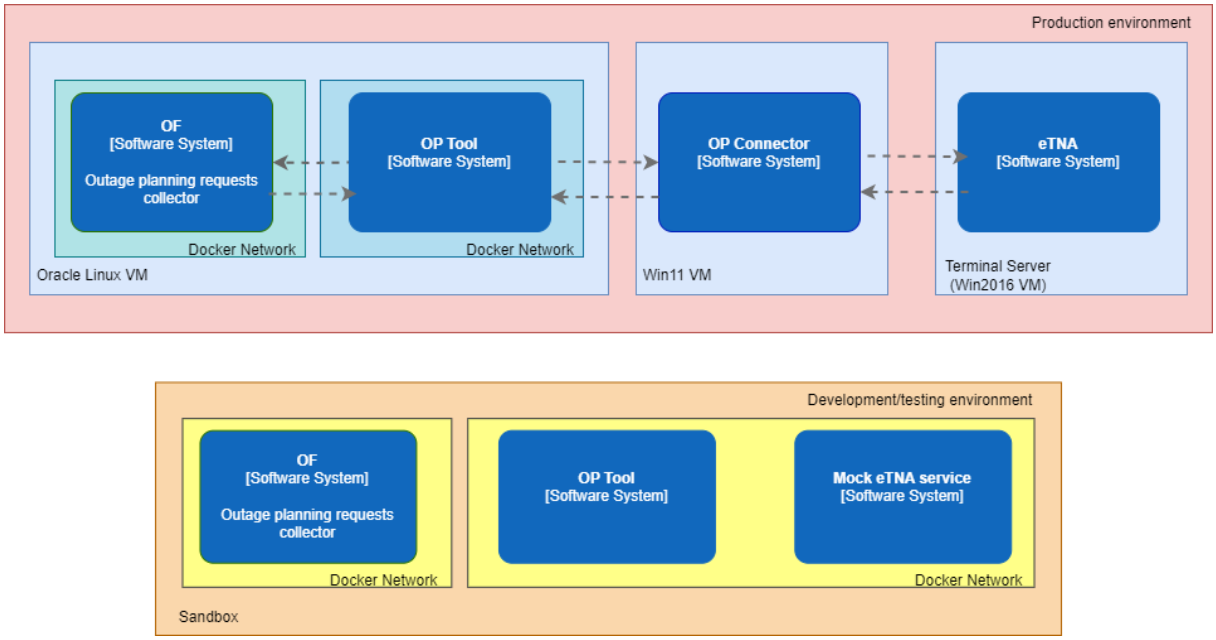

Figure 13: Production vs. Sandbox environment

6.4 TOOLS USED FOR DEMONSTRATION IN PILOT SITE 3 – SLOVENIA

This chapter presents the sandbox and/or digital twins architecture and characteristics for different tools used in Slovenian pilot.

6.4.1 Specific environment for PRECOG product

6.4.1.1 Sandbox for Tokenization tool (UC38)

ELEK has supplied an on-premises Ubuntu virtual machine (VM) that is network-isolated from other systems to host and run the Tokenization tool, hence offering higher security and isolation levels. Tokenization tool is subscribed to topic where ELEKs Flexibility management system publishes messages for tokenization. ELEK has provided credentials so Tokenization tool will receive MQTT messages.

Flexibility management system runs in real-time system and it publishes messages to Message queuing system. The Tokenization tool in the sandbox is subscribed to the same topic as real-time system. This setup can be considered as sandboxing approach (Figure 14). Because of the real-time operation of MQTT server, the output of Tokenization tool will be written to new MQTT server on VM sandbox.

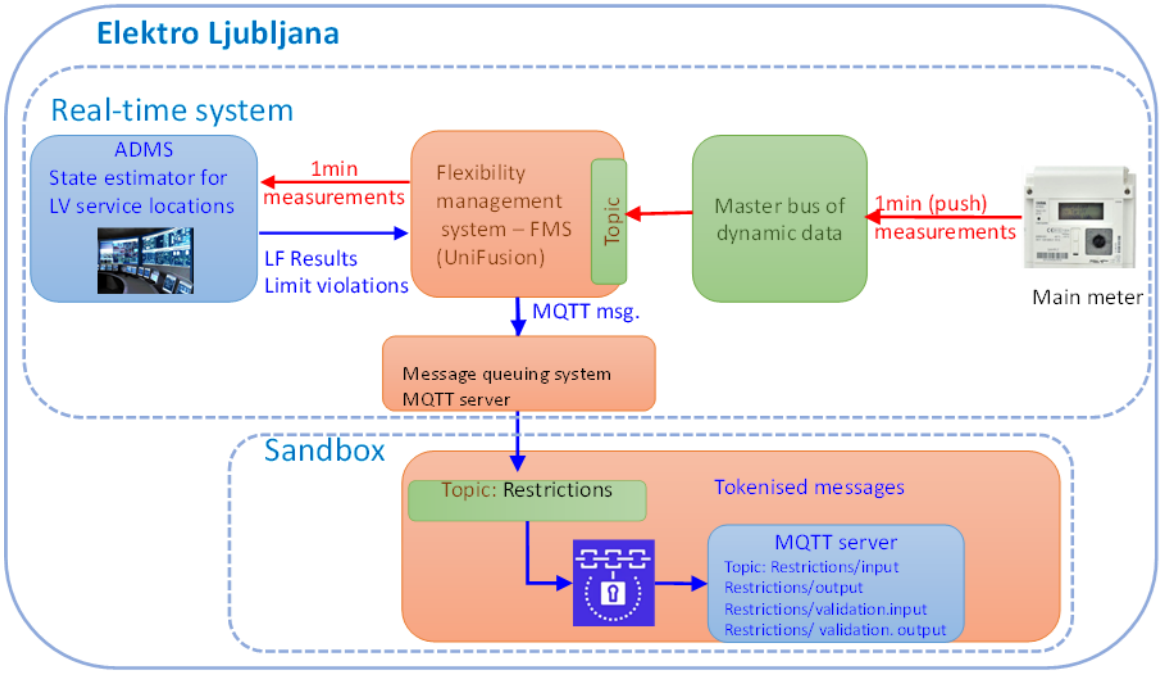

Figure 14: Sandbox architecture for Tokenization tool (UC38)

6.5 TOOLS USED FOR DEMONSTRATION IN PILOT SITE 4 – PORTUGAL

At the moment of the writing and submission of this deliverable, the grant agreement amendment concerning replacement of the Spanish pilot with the Portuguese pilot is under preparation. Having that in mind, and considering the role, the infrastructure available, and the involvement of the new pilot, there are no sandboxes / digital twins for the Portuguese pilot site in D7.1. However, the work on the Task 7.2 continues after the submission of this deliverable, and if there are some sandboxes / digital twins detected by the Portuguese pilot in the meanwhile, they will be addressed in the second version of this deliverable D7.2 at the end of the project.

6.6 SUMMARY AND CONCLUSIONS

Based on the information provided in the previous chapters, summarized information about planned sandboxes and digital twins is shown in Table 2. There are 9 sanboxes and 5 digital twins reported in total, while the distribution by pilots is:

- Greece: 3 Sanboxes and 3 Digital Twins
- Serbia: 5 Sanboxes and 2 Digital Twins
- Slovenia: 1 Sandbox

For sandboxes, all reported tools provide some kind of an isolation in a controlled environment (via VMs, docker containers, security policies) from the production systems. Therefore, it can be considered that all tools satisfy the requirements for sandbox environments.

For digital twins, the requirements regarding models and attributes (mentioned in 6.1.2) were relaxed in the sense that models whose attributes and functional descriptions relate to particular aspects of the observed system were considered digital twins, without insisting that they cover all or most aspects of the entire system model. For example, if one is interested in the behavior of the dynamic topology of the physical power grid, it was not considered necessary to model other functional aspects and attributes of the grid. This holds as long as the chosen aspects and attributes provide a sufficiently accurate representation of the dynamic topology of the physical system. Additionally, in isolated environments where digital twins appear as snapshot twins, it was not considered crucial for the snapshot twin to be on the same system or share the same databases as the "real" digital twin. The key requirement is having mechanisms to transfer the "snapshot" from the digital twin's databases to those of the snapshot twin on the isolated system. Furthermore, synchronization and updating of models (functional descriptions and attributes) between systems should be ensured.

Table 2: Overview of sandboxes and digital twins per pilot site

Pilot Site	Tool (UC)	Sandbox	Digital twin
Greece	Dynamic Risk Assessment tool (UC25)	X	
	C3PO cascading simulators (UC22)		X
	Planning and operation of advanced multi-energy microgrid for resilience enhancement (UC32)		X
	Sandbox Tool (UC27)	X	
	Tokenization tool (UC37)	X	
	EMMA GIMAN tool (UC5)		X
Serbia	Over-Frequency Protection Module (UC12)	X	X
	Emergency & Restoration - System Split module (ER-SSM) (UC19)	X	X
	Crisis situation coordination tool (UC35)	X	
	KSI tool (UC36)	X	
	Outage Planning (OP) Tool (UC8)	X	
Slovenia	Tokenization tool (UC38)	X	

7 Conclusions and next steps

Within this deliverable, assets and product integration as well as the preliminary deployment activities have been carried out in a coordinated way between different R^2D^2 partners, who have delivered the first version of the products' prototypes at each specific pilot site.

According to the R^2D^2 project plan, this report is prepared in month 24 of the project duration, while the work package itself lasts until the end of the project i.e. month 36, when the final report on this topic needs to be prepared.

Therefore, it is necessary to next further steps in this report to complete the work in WP 7, in accordance with the requirements of the project assignment. In addition, this section presents the main conclusions on the results of WP7 so far. The following paragraphs briefly describe the next steps and conclusions related to:

- assets and product integration
- deployment and demonstration activities
- sandboxing and digital twins.

At this moment, the work related to assets and product integration at pilot sites is mostly finished for majority of use cases which will be deployed and demonstrated in the following months. Some of the use cases have already started with pre-deployment and preliminary demonstrations.

For each use case are defined the targets, scope and approach for execution and evaluation of developed tools. Additionally, are listed the constraints and dependencies as well as risks which will be monitored and mitigated until the end of the project to achieve the desired goals. Moreover, for each use case is defined preliminary schedule of activities.

Since some use cases cannot be tested in the real system of the pilot site due to the security issues thus nine sandboxes and five digital twins will be used for demonstration purpose.

The next months will be dedicated to the deployment and testing in real conditions of the four products developed in R^2D^2. The goal of this task is to test main functionalities in the four real demo sites, before to deploy the final version of each solution. .

Following this deliverable, R^2D^2 ecosystem integration and testing together with the results of the integration and testing processes in the different pilot sites will be reported in D7.3. If some difficulties will be encountered during the integration of different software tools and services into the real and simulated systems in the preliminary phase, they will be reported and dealt with accordingly in the preliminary deployment and demonstration phase. Therefore, the work done in the preliminary phase will also pave the way to the next phase of the project, when the final deployment activities will deliver the final version of the prototypes. In this way, the final demonstration activities will to possible to begin.

Following this deliverable, the final integration, deployment and validation will be reported in D7.2. It will therefore gather the lessons learnt during the preliminary phase to avoid repeated issues.

8 References

[1.] "R²D² Description of Action," in Annex I to the Grant Agreement. EC, 2022.

[2.] "R²D² Grant Agreement. EC, 2022".

[3.] R²D² D2.2 - Report on pilot sites survey and related regulatory frameworks, https://cordis.europa.eu/project/id/101075714/results

[4.] R²D² D2.3- Final version of the R2D2 Requirements and Detailed Architecture Design, https://cordis.europa.eu/project/id/101075714/results

[5.] Karagiannis, S., Magkos, E., Ntantogian, C., Ribeiro, L.L. (2020). "Sandboxing Cyberspace for Cybersecurity Education and Learning. In: Boureanu, I., et al. Computer Security", ESORICS 2020. Lecture Notes in Computer Science, vol 12580. Springer, Cham. https://doi.org/10.1007/978-3-030-66504-3_11

[6.] Michael Maass, Adam Sales, Benjamin Chung, Joshua Sunshine, "A systematic analysis of the science of sandboxing", PeerJ Computer Science 2:e43; https://doi.org/10.7717/peerj-cs.43 , 2016

[7.] Robert Wahbe, Steven Lucco, Thomas E. Anderson, and Susan L. Graham. 1993. "Efficient software-based fault isolation". Proceedings of the fourteenth ACM symposium on Operating systems principles (SOSP '93). Association for Computing Machinery, New York, NY, USA, 203–216. https://doi.org/10.1145/168619.168635

[8.] Z. Cliffe Schreuders, Tanya McGill, Christian Payne, "The state of the art of application restrictions and sandboxes: A survey of application-oriented access controls and their shortfalls", Computers & Security, Volume 32, 2013, Pages 219-241, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2012.09.007.

[9.] https://publicsafety.ieee.org/topics/cybersecurity-of-critical-infrastructure-with-ics-scada-systems

[10.] Michael Grieves, John Vickers, "Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems (Excerpt)", 2016, https://doi.org/10.13140/RG.2.2.26367.61609

[11.] Timo Wagner, Chris Kittl, Joshua Jakob, Johannes Hiry, "Digital Twins in Power Systems: A Proposal for a Definition", IEEE Power and Energy Magazine, Volume: 22, Issue: 1, Jan.-Feb. 2024

[12.] Erhard Aumann, Thomas Benz, i drugi, „The Digital Twin in the Network and Electricity Industry", VDE-Verband der Elektrotechnik Elektronik Informationstechnik e.V. Energietechnische Gesellschaft (ETG), 2023

[13.] H2020 project TRINITY: https://trinityh2020.eu/

9 Annex I – IRIS hosting environment

9.1 SUMMARIZING THE SITUATION

Following successful collaboration in TRINITY project [13.] regarding hosting of T-COO platform, IT system acquired in TRINITY project is used in R²D² for hosting IRIS platform. SCC provided the required equipment and hosting for IRIS platform in R²D², considering the security requirements as per ISO/IEC 27001 and ENTSO-E OPDE Security Plan. After completion of the system, the following is provided by SCC:

- a datacentre suitable to support Development, Integration and Test environments of all IRIS products;
- necessary number of virtual machines on the said datacentre;
- high availability based on network design and VMware cluster;
- all necessary means to establish secure multifactor VPN access to the datacentre taking into account standard ISO/IEC 27001 and ENTSO-E OPDE Security Plan;
- the administration and maintenance of the datacentre and
- help and assistance in creation of necessary virtual machines.

The developing parties can securely access and freely use the datacentre and install whatever software is required for their development purposes.

9.2 ENVIRONMENTS

TRINTY servers are within one VMware cluster, so it is flexible and possible to allocate available resources as required for 3 IRIS environments:

- DEV – Development environment;
- INT – Integration or Acceptance environment;
- TST – Test environment.

9.3 DATACENTRE INSTALLED IN SCC

All IT equipment acquired in TRINITY project for hosting of T-COO platform is at disposal for hosting of IRIS platform in R²D² project. SCC provides necessary equipment for development, integration and testing environments of IRIS hosting environment.

Based on defined hardware requirements from Grant Agreement of TRINITY project, following three servers (see next figure) were purchased and configured for the needs of the TRINITY data VMware cluster as shown in Figure 15:

- h8.scc.local, see Figure 16;
- h9.scc.local, Figure 17;
- H10.scc.local, Figure 18.

Figure 15: View from vSphere client – three host servers

The characteristics (used hypervisor, server model, processor type, number of logical processors, number of virtual machines, etc.) of the mentioned three host servers are given the following figures, respectively. Also, od the right side of each of three mentioned figures current usage of CPU, RAM and Storage is presented.

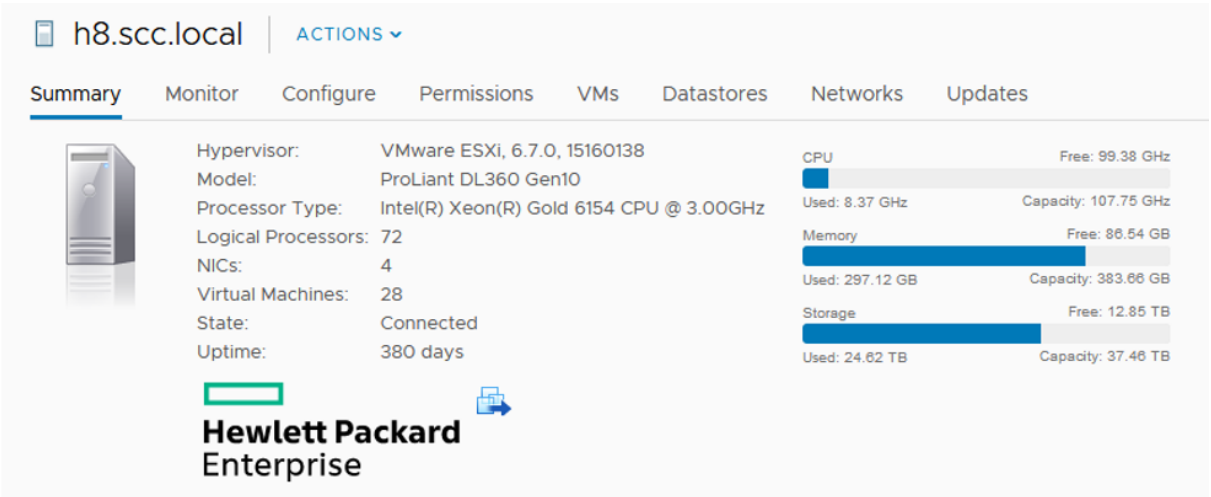

Figure 16: View from vSphere client – h8.scc.local server

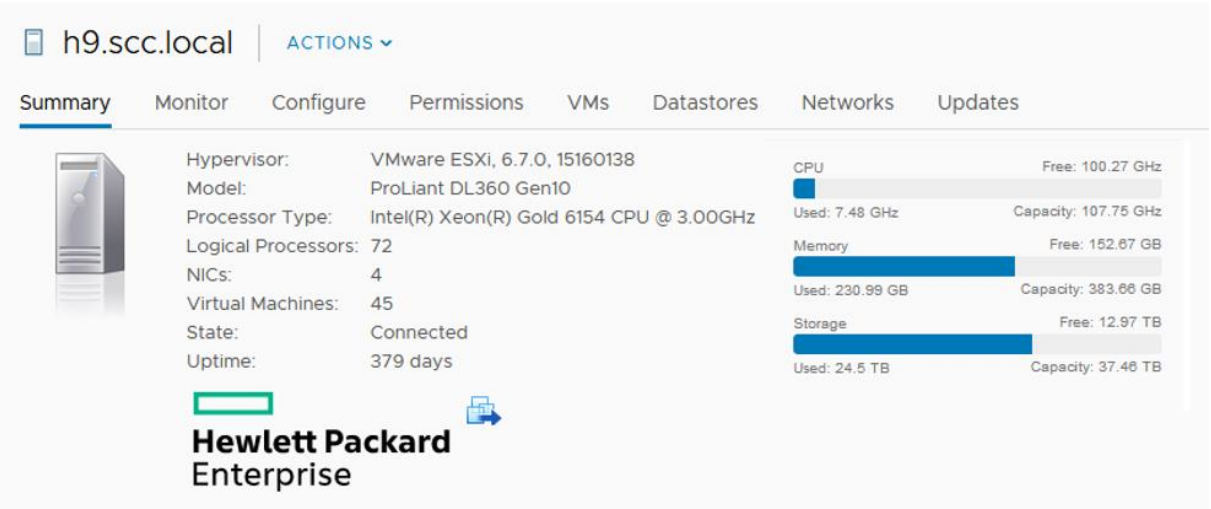

Figure 17: View from vSphere client – h9.scc.local server

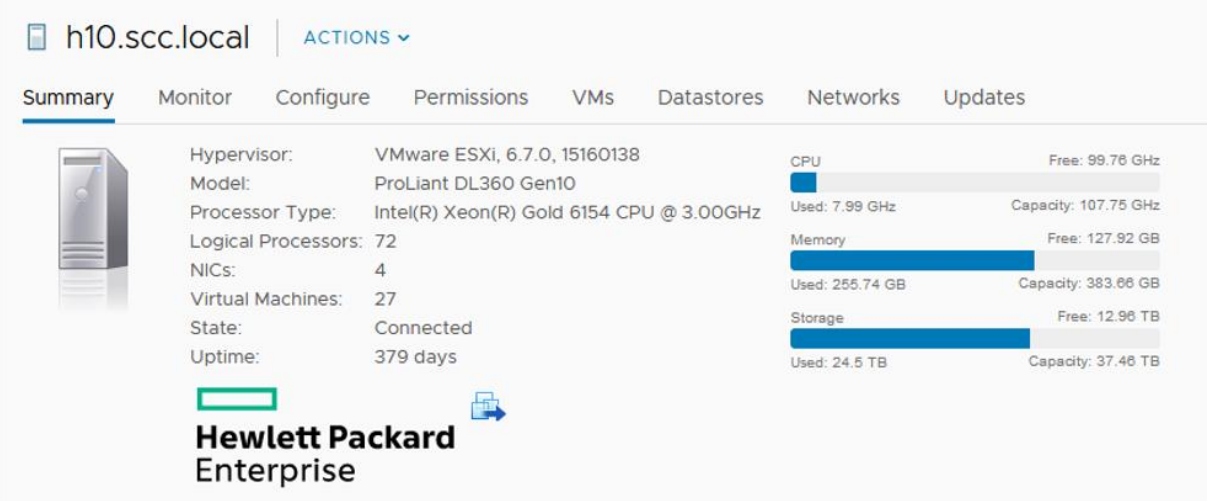

Figure 18: View from vSphere client – h10.scc.local server

NETAPP AFF A220, 24x960GB SSD Storage was purchased for the purposes of forming the TRINITY VMware cluster. The physical installation of SSD storage and mentioned three servers was realized in the Tier III server room in the existing server rack of SCC. Additionally, following items are also bought using TRINITY budget in order to fulfil defined requirements:

- For the purposes of establishing the TRINITY cluster, the Vmware Vsphere 6 Essentials plus licence was purchased;
- For the needs of expansion of SAN switches, appropriate SFP interfaces and expansion of licenses were purchased;
- For the purpose of providing remote access, appropriate licenses for VPN (Cisco Annyconnect plus) and MFA (Entrust Identity Guard) have been purchased;
- For the purpose of segregation and protection of SCC's official production environment redundant CISCO ASA firewall was purchased and installed (CISCO ASA 5508).

9.4 APPLICATIONS INSTALLED AND MANAGED BY SCC

List of applications necessary for the development and deployment of the IRIS hosting environment is following:

- VPN access for developers;
- Kubernetes:
  - Minimum version 1.28.3,
  - KubeAPI access,
  - Ingress Controller: nginx-kubernetes,
  - Helm on all clusters,
  - Kubernetes clusters for RTEi (rti-dev, rti-int and rti-tst),
  - cluster machines are propagated with developer accounts, so kubectl and helm are immediately accessible for all developers on all machines,
  - The Kubernetes cluster must be configured to access an external Docker registry. This access is crucial for pulling necessary images and maintaining the flexibility of deployment processes. This access does not compromise the security and integrity of the system as it is managed using a token.

- Ticketing system – Redmine;
- Managed databases:
  - MongoDB – Version: 6.0.12,
  - MariaDB – Version: 10.11;
- Single Sign On – Keycloak:
  - Single Sign On for all the Web base applications deployed,
  - Version: 22;
- Grafana – Version: 10.2.1;
- Kibana – Version: 8.11.1;
- Nginx – Version: 3.3.2;
- Helm – Version: 3.13.2;
- NFS storage – Persistent volume (50 GB) for saving configurations and files during restart or new deployment;
- sFTP server – sFTP server that is accessible by Imperial College team.

Although SCC is not a commercial cloud provider, they will do their best to support RTEi on open hour (restart machine, service, restoration, patching, etc …).

The usage of RAM and CPU should be monitored as the creation of 3 separate clusters will use most of the physical RAM and CPU available.

9.5 EXPECTED ALLOCATION OF IT RESOURCES

OperatorFabric needs about 10 docker images and Let's Co about 2 docker images. Most of these images are java spring applications. So, hosting environment provides about 2.6GBs of RAM by module and about less than one vCPU core (0.6) by module.

The actual version of OperatorFabric is heavier than Let's Coordinate. Maybe 75% of this resource will be for OperatorFabric and 25% for Let's Coordinate.

About storage, as developers do not have yet messages used, RTEi cannot precisely define storage capacity, but it will be about 50% for Operator Fabrics and 50% for Let's Coordinate. Most of the storage for App Data will be used as temporary storage. DB Storage must take in account separately:

- one mongodb
- one mariadb

The actual estimations are the following one, but developers expect to have them change a bit, depending on the development phases:

- It depends on the size of the file message received and sent exchanged with the other tools.
- It depends on their frequency and expected lifespan before deletion.

Minimal hardware resources that are required/recommended for IRIS hosting environment are provided in Table 3.

Table 3: Minimal hardware resources recommended for IRIS hosting environment

Components	Development Team	CPU (vCore)	RAM *(GB)*	Number of nodes *(#)*	Docker images *(GB)*	App Data *(GB)*	DB Data *(GB)*
Let's Coordinate	RTE Group	8	32	4	1	50	50
OperatorFabric				8	4		

SCC confirms that it will provide the above requirements during the execution of R²D² project.

9.6 UPGRADE MANAGEMENT AND MAINTENANCE

Special attention is given to the update management and maintenance of the various environments (DEV, INT, TST). The following points have been agreed upon to ensure the operational maintenance of the application:

- **Technical stack review**: A comprehensive review of the technical stack will be conducted every six months. This process is aimed at ensuring that all components of infrastructure are up-to-date and functioning optimally.
- **Response to security issues**: In case of a confirmed security issue, updates will be performed more frequently. Reactivity to security vulnerabilities is important to maintain the integrity and safety of system.
- **Use of the TST environment**: The TST environment will be used to test upgrades of R²D² infrastructure system. This allows for testing changes in a controlled environment before deploying them to development and integration environments.
- **Tracking and communication via Redmine**: Redmine will serve as the central platform for keeping all stakeholders informed about planned updates and tests conducted. Regular communication via Redmine will ensure transparency and efficient coordination of maintenance. Activities.

Updates to the new version for all tools will be done based on the RTE-i's request with the RTE-i's approval.

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.