R2D2

Reliability, Resilience and Defense technology for the griD

D3.1 – Design of the Multi-risk assessment framework for power system

Date: 30/09/2023

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	WP	Version
Design of the Multi-risk assessment framework for power system	3	1.0 (Final)

Contractual delivery date	Actual delivery date	Delivery type*
30/09/2023	29/09/2023	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
Ektor Stasinos	ICCS
Aris Dimeas	ICCS
Andrew Syrmakesis	ICCS
Kevin Pang	ICCS
Nikos Hatziargyriou	ICCS
Kostas Papadatos	CYBERNOESIS (CYBER)
Kostas Rantos	CYBERNOESIS (CYBER)
George Aslanidis	CYBERNOESIS (CYBER)
Tilemachos Valkaniotis	CYBERNOESIS (CYBER)
Angeliki Zapalidi	CYBERNOESIS (CYBER)
Mathaios Panteli	UCY
George Paphitis	UCY
Mohammadamin Akbari	UCY
Goran Strbac	ICL
Dawei Qiu	ICL
Danny Pudjianto	ICL
Yi Wang	ICL

Version	Date	Person	Action	Status*	Dissemination**
V0.1	12/06/2023	Ektor Stasinos (ICCS)	Table of Contents	Draft	CO
V0.2	23/05/2023	Ugo Stecchi (ETRA)	Table of Contents	Draft	CO
V0.3	26/6/2023	Ektor Stasinos (ICCS)	Table of Contents	Draft	CO
V1.0	1/09/2023	Task Leaders (ICCS, CYBER, UCY, ICL)	Tools Description (First round)	Draft	CO

V1.1	11/09/2023	Task Leaders (ICCS, CYBER, UCY, ICL)	Tools Description (Second round)	Draft	CO
V1.2	15/09/2023	Ektor Stasinos, Andrew Syrmakesis (ICCS)	Final Draft sent for Peer Review	Draft	CO
V2.0	25/09/2023	RTEi, IMP	Peer Review	Draft	CO
V2.1	29/09/2023	Ektor Stasinos, Andrew Syrmakesis (ICCS)	Integration of reviewers' comments	Approved	CO
V3.0	29/09/2023	Ektor Stasinos, Andrew Syrmakesis (ICCS)	Final Document Submission	Final, 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

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.

To effectively address these challenges, this delivery document introduces C3PO, a product that will be developed through WP3 activities within the R^2D^2 project. C3PO comprises an advanced toolkit designed to offer a comprehensive set of innovative solutions for system operators. These solutions aim to significantly enhance the overall defense of the grid against a growing number of hazards and threats across the energy value chain.

The proposed toolkit encompasses both physical resilience and cybersecurity assessment and enhancement tools. Hence, it brings these two domains together to provide a systematic, disciplined, and repeatable approach for evaluating an energy system security strategy with a comprehensive 'Multi-risk assessment framework for power systems.' This document provides a detailed description of the architectural design and general structure of the C3PO product, its functionalities, features, and required resources, as well as the data exchanges and interconnections between its various tools.

The C3PO product will be developed through 6 Tasks, within which the following tools will be created:

- Security assessment through advanced IT technologies – Cyber Risk Assessment Tool
- Dynamic Cyber-Risk Status Evaluation
- Spatial and Temporal Modelling and Quantification of Cascading Physical Events
    - Spatial and temporal event and fragility modelling
    - Cascading modelling and quantification
    - Event simulator of a progressing wildfire and assessment of its impact on distribution system
- Resilience-driven investment and operational planning to mitigate or prevent cascading effects
    - Resilience-driven investment and operational planning to mitigate or prevent cascading effects
    - Post-disruption distribution system operation and restoration strategy based on flexible microgrid formation and scheduling
- Operation and Planning of Advanced Multi-Energy micro-grids for Enhancement of Resilience
    - Advanced control of mobile power sources in enhancing micro-grids resilience
    - Resilience-driven optimal design of micro-grids
- Knowledge sharing – Cyber Threat Intelligence and cascading events

The tools and data exchanges among them will be integrated in the C3PO Platform, utilizing two applications developed within WP3 to address the cybersecurity and the resilience tools separately due to their different nature.

The overall C3PO Suite will provide valuable practices and insights, offering static and dynamic frameworks for enhancing cybersecurity as well as resilience-oriented planning, preventive and restorative strategies, enabling stakeholders to efficiently evaluate and improve the overall defense of the grid.

This deliverable, together with the other technical deliverables D4.1, D5.1 and D6.1, contributes to achieve the Milestone #3 “Design of the four Products”, due by M12. As matter of fact, each of these documents describes in detail the design of the product to which it refers along with the methodology and techniques used.

Keywords

Extreme weather events, Cyberattacks, Resilience, Cybersecurity, C3PO, Architectural design, Integration.

Copyright statement

1. Index

1.1 LIST OF TABLES

1.2 LIST OF FIGURES

2. Introduction

2.1 PURPOSE AND SCOPE OF THE DOCUMENT

The objective of this delivery document is to provide a comprehensive description of the architecture and design of the 'Multi-risk assessment framework for power systems.' This document aims to present the main functionalities and define the specifications of the C3PO product, laying the groundwork for assessing its impact within the broader R^2D^2 project.

This presentation involves a detailed exploration of the various tools within the framework. Each tool is described in terms of its technical functionalities, workflow, data exchanges, triggering events, and the methodologies it employs. Additionally, an initial overview of the User Interface for the final C3PO application is included.

This document serves as a precursor to deliverable D3.2, which will encompass the complete development of the C3PO product, demonstrate the results of its tools at the designated demo sites, and showcase the integration of its components into a unified User Interface, scheduled for M24 of the R2D2 project.

Furthermore, the document conducts an analysis of the innovation and solutions that C3PO can offer to stakeholders, comparing them to existing technologies in the current state of the art, addressing both resilience and cybersecurity challenges. These technical solutions are reflected through the development of Use Cases for each tool, offering a step-by-step depiction of their workflows and defining the various engaged actors. The Use Cases developed within WP3 are engaged to the Greek pilot site of the R^2D^2 project. The technical requirements of these Use Cases towards pilot sites are also outlined.

Finally, the document presents the implementation plan and outlines the necessary next steps for developing all described tools and integrating them into a cohesive User Interface, thereby realizing the C3PO Suite.

2.2 STRUCTURE OF THE DOCUMENT

The document is structured as follows:

First, Section 2 presents an overview of the C3PO product design, reflecting its scope and objectives.

Furthermore, in Section 3, the document describes the current state of the art and common practices in existing cybersecurity and resilience-oriented tools, along with the innovative solutions that C3PO features can provide to stakeholders. Additionally, this section introduces the diverse Use Cases that each tool comprises, detailing their workflow, technical requirements, correlated actors, and the pilot sites they are engaged with for the needs of the R^2D^2 project.

Subsequently, Section 4 provides a comprehensive presentation of all the C3PO – WP3 tools, including their internal architecture, features, workflow, data exchanges, and triggering events. The design of both cybersecurity and resilience-oriented tools is described in detail to effectively frame the context of the C3PO product features and shape the final outcome. Moreover, the design of the two separate knowledge sharing repositories for cybersecurity

and resilience-oriented best practices, respectively, is presented to capture the impact of diverse EPES threats, provide valuable insights, operational and technical feeds, and enable systematic conclusions and recommendations for the most suitable, cost-efficient practices to enhance the overall defense of the grid.

Finally, Section 5 concludes the document and summarizes the most relevant points of the C3PO design. It also introduces the implementation plan and outlines the required next steps for the second phase of the development of the C3PO Suite.

3. Background

3.1 OVERVIEW OF THE PRODUCT

The C3PO product is designed to bring together the distinct domains of cybersecurity and resilience, aiming to provide a holistic approach for efficiently assessing and enhancing the overall defense of the EPES. To get a thorough understanding of C3PO's capabilities, a presentation of the overview of the features of its constituent tools is necessary. This section will provide a brief introduction to the features of each tool, laying the groundwork for Section 4, which will comprehensively describe their features, architecture, data exchanges, and the required resources.

With regard to the "Security Assessment through Advanced IT Technologies – Cyber Risk Assessment Tool" (T3.1), contemporary EPES necessitate the identification of existing cyber threats. The primary objective of T3.1 is to identify the assets and controls within the EPES, recognize the associated threats and vulnerabilities, and ultimately generate an assessment of the current cyber risk status of the EPES. This approach ensures that the system operator remains continuously informed about the status of the EPES, enabling them to implement appropriate modifications or upgrades to enhance its cyber resilience.

With respect to the "Dynamic Cyber-Risk Evaluation" (T3.2) tool, it is highly important to possess methods capable of identifying potential cyber threats that may arise during the operation of the EPES, along with proposing corresponding countermeasures to mitigate their impact. T3.2 plays a crucial role in achieving this objective by receiving information from the cyber risk assessment and cyber threat intelligence components, assessing threat's likelihood, and vulnerabilities criticality and the risk levels associated with them in a dynamic manner. Furthermore, it conducts an evaluation of the EPES's cyber risk status and implements recommended countermeasures promptly, when a cyber threat is identified. This approach ensures the immediate elimination of the impact caused by cyber threats through the utilization of the proposed defense tools.

The "Spatial and Temporal Modelling and Quantification of Cascading Physical Events" resilience tool in T3.3 examines the response of the distribution system (DS) to natural disasters. This tool incorporates a modular simulator designed to efficiently model windstorm events and assess their spatiotemporal impact on the network. This assessment is based on fragility curves that define the probabilities of malfunctions for power system infrastructures. Additionally, the tool employs an AC Cascading failure model to disintegrate the examined network into islands, aiding in mitigating the impact of large and wide-spread blackouts through the successive activation of protection mechanisms. Also, it employs machine learning models along with feature selection techniques to identify critical components in the network. Furthermore, within the premises of T3.3, a modular simulator for modelling wildfire events is developed. Its primary objective is to evaluate the impact of a progressing wildfire and determine an optimal operational strategy to mitigate its disruptive effects on the DS.

In T3.4, a "Resilience-driven investment and operational planning to mitigate or prevent cascading effects" tool is developed. This tool incorporates a two-stage stochastic programming model aiming at optimizing the re-dispatching of Distributed Energy Resources (DERs) and the reconfiguration of radially operated meshed-designed distribution networks with resiliency improvement goals. Consequently, it introduces a resiliency-driven long-term infrastructure planning approach for DS to facilitate investment decision-making for system operators and planners by establishing a cost-effective optimization model. This model can be effectively employed in disaster-preventive scheduling, post-fault scheduling, dynamic

restoration, DS expansion planning, DERs integration, DS hardening, switch placement, and DS reconfiguration, based on the results and resilience metrics obtained from T3.3. In addition, within the context of T3.4, a "Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling" tool is developed. It aims to reduce service interruption costs and support fundamental facilities in a DS subject to catastrophic failures by separating the system into multiple microgrids to maintain the electrical connection between distributed generators and critical loads. Furthermore, this tool provides a restoration scheme to clear the existing outages and restore the system back to the normal operating state. The tools of T3.4 receive outage information as inputs from the advanced simulator of T3.3.

T3.5 encompasses the development of an "Operation and Planning of Advanced Multi-Energy Microgrids for Enhancement of Resilience" tool. This tool is designed to create resilience-driven planning strategies for the optimal sizing of mobile power sources (MPSs) in the context of microgrids, including mobile energy storage systems (MESSs) and mobile emergency generators (MEGs). Additionally, it focuses on the development of resilience-driven operation strategies for microgrids under the concept of networked-microgrid (NMG), where the system resilience can be enhanced by switching tie-lines and sharing energy resources among NMGs. Furthermore, the tool works on the development of real-time smart control strategies for MPSs and repair crews (RCs) to enhance microgrid resilience given their mobility and flexibility compared to static energy resources.

Regarding the "Knowledge sharing – Cyber Threat Intelligence and cascading events" (T3.6) tool, there is a critical need for a pool of information that will keep track of historical events (cyber and physical) against the investigated EPES. The T3.6 tool gathers this knowledge by collecting information about cyber incidents based on external resources and standards and organizing the aforementioned information in a form that provides a cyber threat intelligence through Big Data analysis methods. Moreover, it collects information about cascading events based on the models of previously developed tools and stores them in a repository in order to identify the most critical incidents and make recovery recommendations. In this way, relative information can be provided to other tools (e.g., T3.2, T5.4) in order to generate their metrics or produce other types of critical knowledge.

3.2 STATE OF THE ART

3.2.1 Cybersecurity tools

3.2.1.1 Background

Traditional information security risk assessment (RA) methodologies and standards, widely adopted by information security management systems and frameworks as foundational pillars for robust environments, encounter significant challenges in modern, rapidly evolving environments where the threat landscape constantly changes, leading to the discovery of new vulnerabilities exploitation methods. This issue becomes even more pronounced in diversified environments that encompass an EPES infrastructure.

Within the EPES environment, the diversified nature necessitates the formulation of distinct strategies in approaching cybersecurity risk management, as not all contemporary methods adequately address the unique characteristics of digitalized energy systems and their subsectors, such as generation, transmission, and distribution, where cyber risks are

prevalent. The importance of deploying effective risk management systems to bolster measures in the digitalized energy sector is further emphasized by recommendations from the EECSP-Expert Group and the SGTF Expert Group to the European Commission [1].

However, despite the growing importance of cybersecurity in the energy sector, there are currently no specialized risk management methodologies in the industry and literature that specifically target energy systems, including transmission and distribution subsystems. Consequently, organizations often resort to standardized methodologies such as ISO/IEC 27005 [2], ISA 62443-3-2[3], NIST 800-82 Industrial Control Systems specific standard [4], Cyber Security Evaluation Tool (CSET®) [5] developed by Cybersecurity and Infrastructure Security Agency (CISA), and other widely recognized approaches developed and adopted by the industry. Converged IT/OT environments present significant challenges when employing conventional cybersecurity risk management approaches, primarily due to the considerable transformation of the threat landscape and the vulnerabilities inherent in what were previously isolated legacy systems.

EPES and power grids infrastructures cannot rely on rigid and static risk assessment processes, since they are ill-suited to adapt to the dynamic and rapidly changing environments in which they are operating. These inflexible approaches, not only fail to accommodate the evolving threat landscape, but also contribute to misconceptions about the nature of threats and their potential impacts. It's worth noting that many of the aforementioned methodologies are often standalone solutions, lacking integration with other security solutions. Consequently, they miss out on valuable feedback that could enhance the risk assessment processes, limiting their overall effectiveness. Embracing a dynamic and real-time approach in risk assessment decisions is imperative, as it allows operators/administrators to promptly respond to emerging threats, adapt to changing conditions, and bolster their cybersecurity measures accordingly.

The European Union (EU) has recognized the significance of developing new approaches, frameworks, and tools to conduct cyber risk assessments for Smart Grid infrastructures. Several research projects have been funded by European countries and the European Commission to provide cyber risk assessment models for Smart Grids. Smart Grid Security Guidance (SG)2 is an Austrian research project that has developed a cybersecurity risk assessment method for existing and near-future power distribution systems. This risk evaluation tool considers Smart Grid's dynamic nature and different national guidelines, such as prevailing systems, regulatory restrictions, and legal requirements. This technique is based on a reference guide of the Austrian's power grid, and it can be implemented both for already-used systems and future approaches. The level of cyber threats is evaluated based on practical security measures and it is integrated with a theoretical analysis of upcoming upgrades that are inspired by threat models proposed by British Standard Institution (BSI) and European Union Agency for Cybersecurity (ENISA). Results of this analysis are then applied to the reference model and their probability along with the potential consequences are validated in a semi-quantitative manner. To make this analysis more realistic, system knowledge from various DSOs was acquired and utilized regarding system information and attack scenarios.

Another initiative that attempts to provide a risk assessment tool to evaluate cyber threats in Smart Grids is the Artemis-funded EMC2 project[1] led by Schmittner et al. This research project has expanded the FMEA safety analysis procedure to investigate the

[1] http://www.emc2-project.eu/

possibility of a cyberattack to occur and its effects on the investigated system. The research team has implemented this approach to multicore embedded systems that are deployed in industrial automobility. The proposed technique needs to be further examined to distinguish security from safety-related events and provide cybersecurity measures considering the involved threat agent. While the EMC2 project focuses on embedded systems, it can be easily expanded and specially designed for different Smart Grid modules and subsystems.

Besides the aforementioned research projects, the EU-funded HyRiM project[2] (Hybrid Risk Management for Utility Providers), proposed novel risk analysis strategies that are feasible to be implemented in industrial-based systems, such as power grids, natural gas industries and transport networks. The innovation of these techniques is the consideration of the cascading effects in their analysis, where an undesired event in the electricity sector could possibly affect the natural gas systems and vice versa. Within the scope of this project, the issue of cascading effects is handled by combining game theory methodologies and network theory techniques. Strategies obtained from HyRiM can be applied to the Smart Grid environment composed of information and communication technologies, and physical power systems, along with their submodules.

A similar approach is followed by the EU-funded SECCRIT project[3] (Secure Cloud computing for Critical Infrastructure IT) which investigates how to strengthen high-availability infrastructures of information and communication services. Such technologies include some cloud operations that are necessary for the proper functionality of modern cyber-physical systems. To this end, the research team has created a database that reports threats and vulnerabilities that are mainly targeting cloud systems to identify underlying patterns in such infrastructures. In the utilized database, the categorization of the threats and vulnerabilities is based on cloud technologies, such as network virtualization, software-defined decision-making processes, etc. An existing risk assessment method is expanded and specially redesigned for cloud-based case studies to be applied to the aforementioned database to evaluate the threat scenarios. This risk evaluation is similar to those performed in a Smart Grid environment and hence, it can also be applied in such situations.

Finally, SPARKS[4] (Smart Grid Protection Against Cyber Attacks) project, funded by the EU, explores both the physical and the cyber resilience of Smart Grids. The research team of this project has considered the results of previous projects to investigate new risk assessment approaches. In this project, a wide variety of cyberattacks were modelled and simulated to examine their effects on the physical part of the power system. For this purpose, a software tool that emulates communication network traffic, like OMNeT++[5],is integrated with another software environment, like GridLAB-D[6] , that simulates the dynamic behaviour of power systems. The objective of this integration is to mimic the interaction between physical and cyber parts of a modern electrical grid and launch realistic types of cyberattacks. With this technique, the sensitivity level of a power system against different types of cyberattacks can be investigated. Apart from that, the project developed models that evaluate the effects of false data injection attacks on the control methods used in Smart

[2] https://cordis.europa.eu/project/id/608090
[3] https://cordis.europa.eu/project/id/312758
[4] https://cordis.europa.eu/project/id/608224/reporting
[5] http://omnetpp.org/
[6] https://www.gridlabd.org/

Grids. This analysis is based on a previously EU-funded project, called Viking[7],that was focused on power transmission systems. In this way, cyber threat levels of the utilized control algorithms can be evaluated.

Apart from the European Commission and European countries, the scientific community worldwide has directed its attention towards exploring novel methodologies concerning cybersecurity risk assessment in Smart Grids and EPES infrastructures [10].

A risk-based approach is presented in [6] as a feasible solution to tackle cybersecurity issues within a Smart Grid infrastructure and preserve its operational state. The introduced assessment takes into consideration the typical technologies that are utilized within Smart Grids and focuses on the smart meters health risks that are related to radio frequency (RF) radiation. In this work, cyber risk is modelled as the possibility of a threat agent to exploit a Smart Grid vulnerability and cause damage to a computer, a network system, or a utility, leading to undesired consequences to both operational and business processes. This framework performs a coordinated assessment of cyber and power system threats to satisfy security and safety goals for the entire grid.

In [7], a probabilistic risk analysis framework is proposed to assess the cybersecurity threats and vulnerabilities that are introduced when a Smart Grid is upgraded. The primary objective of this approach is to numerically evaluate the overall advantages and drawbacks associated to Smart Grid network expansions and the employment of new team members in cyber defence workgroups. In this way, decision makers are provided with a tool that enables them to analyse the trade-offs and their priorities under limited resources. The methodology is based on Bayes-adaptive network security model, which is a redesign of the classic "Multi-armed Bandits" (MAB) problem. While the solution to the standard MAB problem is addressed with uncertain success probabilities, the proposed model handles the uncertainty of potential attacks on network nodes with uncertain Poisson-distributed rates. Authors refer to their method as "Multi-node bandits" due to its conceptual similarity to MAB. The presented methodology offers a dynamic approach on cyber security investment and explores the optimal allocation of cyber defence teams among nodes, giving emphasis to the deployment of proactive measures towards the strengthening of cyber defence.

An analytical game-theoretic approach is proposed in [8], which attempts to assess the security of SCADA systems deployed in the Smart Grid environment against cyber-attacks. This technique provides a tool for security administrators which allows them to make informed decisions promptly to guarantee the uninterrupted operation of Smart Grid SCADA systems even under cyber-attacks. This research technique develops a payoff formula (or game utility function) that tries to mimic the behaviours of both the attacker and the defender within a SCADA system platform. Particularly, the developed model represents a sequential, non-zero-sum, two-player game between an attacker and a SCADA security administrator. By utilizing the backward induction technique on the game tree that is generated by the formulated payoffs, a decision analysis can be acquired. The necessary game payoffs are analytically derived and applied on a real-world scenario of Sybil and node compromised attacks at sensor level. Results of this analysis enable security administrators to effectively respond to cyber-attacks and verify the constant and optimal operation of the Smart Grid SCADA system.

[7] https://cordis.europa.eu/project/id/225643

In [9], a cybersecurity assessment framework is designed that can evaluate security risks within a Software-Defined Networking (SDN)-enabled Smart Grid. This work mainly focuses on quantifying cybersecurity vulnerabilities of Intelligent Electronic Devices (IEDs) that communicate over an IEC 61850 network during Denial of Service (DoS) attacks. To this end, a security score model is developed that considers the criticality of each IED and assesses its impact on the total Smart Grid network. This security score model is based on the Smart Grid's resilience score, that is derived after a successful mitigation of an attack. Resilience metrics that are taken into consideration to form the aforementioned model are the following: recovery time of the backup server or IED, packet capturing/sniffing time, average recovery process duration, data loss percentage during recovery phase, recovered data quality, user experience complexity and downtime amount in the absence of continuous protection. With this model, a clear comprehension of the potential vulnerabilities within the investigated system is provided.

3.2.1.2 Innovation provided

The interdependencies within the grid, the highly complex environment which introduces an expanded attack surface, introduce major challenges that will be addressed by R^2D^2. The aim is to:

- elaborate on International Standards and widely accepted methods in order to define and implement security baselines and risk management methodologies that will address the peculiarities of each subsector's energy systems, focusing on threats and vulnerabilities that legacy systems and complex grid infrastructures can face, especially in respect to the converged IT/OT environment and the various energy subsystems, as well as Supply Chain Cybersecurity Risks. The developed methodologies will not only consider the different cybersecurity challenges for each subsector (Bulk Generation, Control Centre, DER, Demand Side) but also, Cross-Organizational Risks. The adoption of such a tool will assist operators in the energy sector to work on comparative results to identify gaps in their security posture compared the levels demonstrated by others in the community.
- develop dynamic risk posture evaluation tools that will provide advanced risk management solutions that will go beyond the conventional risk management methodologies and take advantage of valuable information provided by cyber-threat intelligence, vulnerability assessments, and event-management security infrastructures, aiming to monitor risk levels to confront any deviations from acceptable risk levels by the moment they are identified.
- utilize a foundation of diverse data sources, including asset information, asset criticality assessments, network topology, Cyber Threat Intelligence (CTI) feeds, vulnerability scanner outputs, and SIEM, to obtain access to a comprehensive dataset. This compilation empowers us to foster a holistic understanding of EPES's security landscape. By correlating this diverse data, our objective is to formulate an advanced risk assessment methodology tailored to effectively address the unique challenges posed by EPES infrastructure.
- create a Dynamic Cyber-Risk Status Evaluation component, which is able to correlate and analyse data sourced from a diverse range of inputs in real-time, leveraging state-of-the-art algorithms, including cutting-edge machine learning techniques, across its various components. This novel approach is singularly focused on addressing the complexities of the diversified IT/OT

environment within EPES infrastructure. Through continuous monitoring of the EPES infrastructure, our model promptly identifies new and emerging threats at the very moment they occur, enabling an immediate and decisive response that effectively reduces risk to an acceptable level. This dynamic, real-time risk assessment process guarantees that the R^2D^2 Dynamic Cyber-Risk Status Evaluation component, significantly enhances its proficiency in detecting potential cyber threats and proposing relevant and timely mitigation measures in light of the ever-evolving threat landscape.

- incorporate domain-specific CTI to enable the R^2D^2 Dynamic Cyber-Risk Status Evaluation component to take a proactive stance in cybersecurity. By continuously monitoring and analysing the ever-changing threat landscape specific to EPES, our tool can anticipate potential threats and weaknesses within the infrastructure. This proactive approach allows for timely implementation of preventive measures, reducing the likelihood of successful cyber-attacks that may target critical components of EPES. The dynamic nature of the EPES domain demands a model capable of adapting to new and sophisticated threats. By utilizing real-time, domain-specific CTI, our approach equips the Dynamic Cyber-Risk Status Evaluation component to identify and analyze the most current and relevant threats specifically targeting EPES infrastructure. This up-to-date threat intelligence empowers the model to continuously evolve and refine its risk assessment strategies, ensuring its adaptability and responsiveness to the ever-evolving cyber threat landscape.
- integrate CARMEN tool, that collects, processes and analyses information in order to generate security-related intelligence, mainly from the network traffic. The aforementioned tool will be tailored to cover the complexities of diversified IT/OT environment within EPES infrastructure. This process will be further enhanced by deep learning data analytics in order the Dynamic Cyber-Risk Status Evaluation component to be able to detect APTs.
- match the behaviour of the system against each known APT group in order to assess the possibility of being under an attack carried out by one of the APT groups. Additionally, it is possible to alert cybersecurity analysts about other actions typically associated with these APT groups. This allows them to proactively search for these actions, especially if they have gone unnoticed previously, or to prepare for the next stages of the attack.
- integrate contributions developed within the scope of task T5.3 Cybersecurity Event Management Tools of the project with the Dynamic Cyber-Risk Evaluation component. These contributions aim at developing new capabilities for data ingestion and threat detection for CARMEN, as well as at improving the existing ones of the tool. CARMEN is the tool developed by S2 Grupo together with Spain's National Cryptologic Centre to identify compromises by Advanced Persistent Threats (APTs). These contributions to the Dynamic Cyber-Risk Status Evaluation task of R^2D^2 will be based on the alerts raised by CARMEN's different agents and analysers already existing before R^2D^2 and those raised by the new capabilities and developments specifically carried out within the scope

of the project. These alerts will contribute as an input to the whole risk assessment process.

- integrate APT detection and attribution capabilities based on threat characterization and similarity developed within the scope of the task T5.4 Deep Learning Data Analytics for Security of the project with the Dynamic Cyber-Risk Evaluation component. These capabilities raise an alarm when an anomalous behaviour is observed and detected and stablishes a degree of similarity to different APT groups, assessing the possibility of being under an attack carried out by one of them. In this way, it is possible estimate the possibility of other actions carried out against the system in the past or in the future based on those usually associated to these APT groups to which the observed anomalous behaviour resembles more, considering different threat intelligence aspects such as potential final motivations of the attacker, other potential targets in the organization, industry sector, country, etc.

3.2.2 Resilience Enhancement Tools

3.2.2.1 Background

Cascading Analysis and Quantification:

Cascading failures are the main mechanisms causing extensive blackouts on power network. Understanding the mechanisms of cascading failures is a critical aspect of improving the resilience of the system [11-13]. The propagation of cascading failures is facilitated by overloading, angular instability, voltage stability, and other conditions identified by the IEEE Task Force on Understanding, Prediction, Mitigation, and Restoration of Cascading Failures [14]. Resilience is, in terms of a power network, usually interpreted as the ability to "rapidly recover from such disruptive events and adapt its operation and structure to prevent or mitigate the impact of similar events in the future" [15]. Cascading failure models play a crucial part in many resilience studies [15]–[17], and a large number of cascading failure models is reported in the literature. The work in [18] gives an overview of a broad range of approaches, and groups them based on their characteristics into topological models [19-21], stochastic simulation models [22], high-level statistical models [23]–[25], dynamic simulation models [13], [26], and other interdependent or specialist models. Moreover, there is a wide area of research on identifying critical components of the network that are more prone to failure and patterns that are more likely to cause cascading outages. The authors in [27] used utility data to identify the most frequent patterns that are likely to result in a cascade failure. In [28] data from the North America blackout were used to obtain statistics of cascading events. Moreover, recently we can see an increase of interest in applying machine learning models for cascade failure identification and analysis [29]. These models can leverage huge amounts of data to find patterns and once they are trained, they can make predictions very fast, which is crucial in making decisions. Several authors are using deep learning techniques to identify faults and cascade failures in the power network [30],[31]. A study on predicting cascade failures using graph neural networks was carried out on [32]. The authors in [23] used bayes network to predict the cascade failure propagation.

Resilience analysis to extreme events requires cascading failure models that reliably converge and thus provide meaningful results even for large contingencies. Additionally, models often have to be applied to large datasets and networks and, therefore, need to be computationally fast. Dynamic models provide comprehensive details about cascades but require extensive and often unavailable input data describing the dynamic characteristics of a power system. Additionally, dynamic models are often computationally expensive, which makes them impractical in large networks. DC-based models are, hence, frequently used in resilience studies [13], [15], [17], [34]–[36]. However, past outages have shown the significant role of voltage deviations and reactive power flows (PFs), such as during the 2003 blackout in the United States and Canada [37] or the 2009 blackout in Brazil [38]. While DC PF models are fast and numerically stable, they fail to incorporate these aspects. AC PF models usually suffer from nonconverging PFs, which regularly occur when considering stressed networks and large contingencies. Resilience analysis, however, depends on the analysis of such extreme conditions and thus requires dedicated cascading failure models. Some AC PF models, such as [39], do not address the matter of nonconverging PFs at all. Other models, such as [40], particularly address nonconverging PFs, but do not consider reactive power and voltage limits and lack subsequent reactions by protection mechanisms, such as excitation limiters and undervoltage load shedding (UVLS). These mechanisms play a crucial part in large cascading failures [14]. Additionally, resilience analysis requires a whole-systems approach, thus, models need to be able to link seamlessly to established resilience evaluation frameworks.

Wildfire event simulator and impact assessment:

Natural disasters can provoke serious damage to power grids. In recent years, extreme weather events around the world have underlined the need for operative strategies that can significantly strengthen the power grid and enhance its resilience against those incidents. The effects of climate change are increasing both the frequency and the intensity of disruptive High Impact Low Frequency (HILF) events such as wildfires, floods, windstorms which often cause power outages to consumers and damages in power system infrastructure. Any operational framework dealing with the enhancement of power system (physical) resilience must take into account the unique nature of diverse HILF events. That means that each extreme weather event has different spatial and temporal impact on power system infrastructure. Among natural disasters, wildfire is one of the most dangerous HILF events that can threaten its infrastructure, jeopardizing its reliable operation. Many countries experience such catastrophic events (e.g., Greece, Spain, Portugal, etc.) especially during summer periods. In these countries, distribution systems passing through dense vegetation or forested areas are extremely vulnerable to wildfires. Additionally, ignitions caused by power lines are not uncommon.

In the existing literature, the diverse strategies for enhancing power grid resilience mostly focus on extreme weather events [41]-[46], while the grids' ability to withstand potential wildfires has not been adequately addressed. In reference [47], a methodology is introduced for quantifying the damage inflicted by wildfires on a city's distribution system. However, this approach does not propose any measures for mitigating the wildfire threat. Reference [48] explores the impact of a advancing wildfire on transmission system line ratings. Additionally, it employs an optimal power flow method aiming at minimizing the generation cost while considering reduced line capacities resulting from the wildfire. A similar study on the impact of a progressing wildfire on transmission system line ratings is outlined in [49]. The reference also utilizes an optimal power flow method to minimize the generation cost, incorporating the constraints imposed by the reduced line capacities due to

the wildfire. References [50] and [51] propose a method for optimizing the distribution system operation in the face of an progressing wildfire. These studies delve into the contribution of microgrids and demand response in enhancing resilience. The utilization of the steady-state heat balance equation, as outlined in [49] and [50], is in accordance with the principles described in IEEE Std 738 [51], assuming that the electrical current, conductor temperature, and weather conditions are constant across all times. Reference [52] provides a comprehensive wildfire characterization package which can spatiotemporally monitor and analyze the behavior of the wildfire. Also, the study of [53] propose a real-time monitoring of the wildfire event, while it evaluates the risk exposure in each simulation step, by considering a number of aspects, such as the available topology of the network, environmental conditions and the severity of the event. Reference [54] presents an optimal hardening strategy for improving the distribution system resilience against any approaching wildfire considering vegetation management, pole upgrading and overhead distribution branches undergrounding. Finally, in [55], a probabilistic proactive generation redispatch strategy to enhance the operational resilience of power grids during wildfires is proposed, using a Markov decision process to model system state transitions given component failure probabilities, wildfire spatiotemporal properties, and load variation.

Resilience Driven Planning:

Today's power grids are designed in such a way that they can be resistant to high-probability and low-effect events. However, low-probability and high-impact faults can still cause heavy losses to power networks from an economic point of view. Recent years have witnessed more frequent natural disasters causing severe power outages, which result in great economic losses, etc. Therefore, the concept of resilience has been raised in the past decades in the planning studies of power networks. Resilience is a measure of the network's ability to withstand sudden shocks caused by extreme events such as hurricanes, floods, earthquakes, etc., and recovery of normal performance. Such disturbances affect entire electricity networks, especially all users connected to the faulty section of the system.

Table 1. Resilience-driven planning strategies

Resilience-driven planning		Strategies
Short-term or operational planning	Pre-disaster	Optimum resources allocation (MPSs, repair crew)
	Post-disaster	Optimum resource dispatch and network reconfiguration (DS partitioning using switches, DERs, and MPSs)
Long-term or infrastructure planning		Optimal hardening, and DGs/switch placement

Resilience-driven DS operation and planning practices, as represented in Table 1, can be used for enhancing DS resilience. The network operation (short-term or operational planning) is employed in two ways, i.e., pre-disaster operation when the imminent fault is predicted, and post-disaster operation. As a means of ensuring rapid response to disasters, early allocation of mobile resources is essential in pre-disaster operational planning. This includes repair crews and mobile power sources that can be deployed within a limited area when an event occurs [56]–[59]. Post-disaster operational planning refers to the process of

restoring services following extreme events by utilizing a reconfiguration program and forming potentially self-sufficient microgrids [60]–[68]. Hence, the optimal allocation of resources can significantly improve network resilience characteristics in the restorative mode. Besides, the long-term planning (infrastructure planning) looks for the optimal allocation of resources (switches, DERs, and MPSs) and network hardening to improve DS resilience from the perspective of duration and system function in the face of possible natural disasters in the future [69]–[72]. Therefore, infrastructure planning can be an effective strategy in improving the DS resilience over all modes of the network resilience curve.

Pre-disaster Operational Planning:

Network utilities often employ flexible solutions for rapid restoration purposes such as allocating MPSs and repair crews prior (days ahead) to the upcoming extreme events. This problem is primarily concerned with minimizing expected operating costs [56]–[59]. The variables considered during the decision process include the allocation of MPSs, reconfiguration, the position and number of crews, and the operation of Distributed Generators (DGs). Due to the uncertain nature of the events, these resources are optimally allocated for possible scenarios through stochastic programming. However, this problem is among the most challenging and large-scale problems that are computationally complex. To address this issue, some studies have developed heuristic-based methods to increase computation speed [56]. There is however no guarantee that the final solution will be optimal. Additionally, some articles have employed two-level or multi-level stochastic programming techniques [57]–[59]. Among these techniques are benders decomposition, progressive hedging (PH) [59], and block coordinate descent (BCD) [57].

Post-disaster Operational Planning:

Network functionality is directly impacted by the speed and accuracy of restoration process. After an extreme event, healthy sections must be separated from damaged sections. Afterward, a restoration program is implemented to re-feed the health sectors by partitioning the system into multiple supply-sufficient microgrids. As a problem of optimization, network restoration requires consideration of optimal operation of DERs, MPSs, network reconfiguration, and dispatch of repair crews with the aim of maximizing service restoration [60]–[68]. As a main constraint, the restoration problem requires the network's radial structure to be maintained. Radial structure constraints can be represented as a set of linear equations using two approaches: the spanning tree [68] and the fictitious network [62]. These two approaches can be used to optimize the radial structure of a system, allowing for greater flexibility and more efficient use of resources. To solve the restoration problem, various methods are available, including heuristic-based methods [64], and stochastic programming [66], [67]. Heuristic-based methods are used when the problem is too complex to solve directly, and the goal is to find an approximate solution. Stochastic programming, on the other hand, is used when the problem involves random variables such as load profile and repair crew time, and the goal is to find an optimal solution to minimize the operating cost after an extreme event.

Resilience-driven Long-term Planning:

To improve grid resilience and efficiency, several options such as line hardening, switch placement, distributed energy resources, such as advanced energy storage technologies, renewable energy sources, and distributed energy resources, can be strategically deployed when developing a resiliency-driven investment plan [69]–[72]. By utilizing these resources, utilities can ensure that their grid is resilient, efficient, and cost-effective. These resources

can reduce the need for large, centralized power plants and upgrade the bulk power system. Additionally, distributed energy resources can provide backup power in the event of a grid failure, ensuring grid resilience even during extreme weather events. This problem seeks to find the most economical solution by reducing the costs associated with power outages in critical situations over time. This involves finding ways to reduce the amount of energy lost when an anticipated disaster occurs, as well as finding ways to restore power more quickly and efficiently, such as using DERs, MPSs, MG forming, and repair crew dispatching.

Researchers typically have implemented multi-level and two-stage optimization models to formulate this problem since it includes goals and operational limitations caused by uncertainties. For example, resilience-driven planning has been formulated as multi-level optimization model in [70]–[72]. At the first level, planning decision variables, including line hardening, switch installation position, and the location and size of the DGs, are determined with a specified maximum budget. The second level determines the worst-case scenario of N-k outages caused by a disaster. Optimally operational planning is implemented at the third level to minimize unsupplied energy in the worst-case scenario using flexible solutions (i.e., post-disaster planning). However, this type of optimization cannot be solved directly and must be converted into a bi-level problem and solved in an iterative process such as CCG [69], and greedy search method [70].

On the other hand, two-stage stochastic programming techniques have the advantage of including most of fault scenarios in the resilience-driven programming problem [72]. The first level of planning is the same as the multi-level method of determining decision variables, including line hardening, switch installation position, and DG placement. The second level involves optimal operational planning to minimize expected load shedding or economic cost under N-k fault scenarios. The Monte Carlo technique generates hazard scenarios, and scenario reduction techniques such as clustering methods are used to reduce the number of scenarios [71], [72] Furthermore, scenario-based solution methods are utilized to reduce the computational burden of the problem [72].

Post-disruption distribution system operation and restoration based on flexible microgrid formation and scheduling:

The ever-increasing penetration of Renewable Energy Resources (RES) into present-day distribution systems calls for appropriate dispatch and control of the system, especially during catastrophic events. In this post-disruption scenario, IEEE Standard 2030.7-2017 [73] suggests separating the faulted distribution system into multiple microgrids to maintain the electrical connection between distributed generators and critical loads. Microgrid techniques can provide exceptional support to distribution system resilience enhancement for their key role in microgrid formation, scheduling, and restoration. However, these processes are treated as separate problems in existing methods, and their interaction remains to be investigated [74, 75]. Therefore, the proposed resilience enhancement tool provides an integrated solution to coordinate the chronological post-disaster processes from microgrid formation, scheduling, to restoration. During the microgrid formation process, existing approaches mainly focus on the performance of the last stage of microgrid formation, i.e., deciding the microgrid topology that maximizes load restoration [76]. The proposed tool fills the research gap of dynamic microgrid formation by providing a set of sequential switch operations to form the desirable microgrids after fault occurrence. In the microgrid scheduling stage, the high penetration of RES with stochastic generation poses new challenges for a robust dispatch scheme [77]. The proposed tool models the source-load stochasticity as joint chance constraints in the microgrid scheduling problem to address the overall violation possibility. Lastly, during the microgrid-based restoration stage, the formed

microgrids are extended and interconnected, and the faulted system returns to the normal operating state gradually. The practical and significant issue during this stage is to coordinate the repair crew dispatch and cold load pickup [78]. To address this issue, the proposed tool provides a dynamic distribution system restoration scheme considering the coordination between repair crew dispatch and cold load pickup. In summary, the proposed tool provides an integrated operation and restoration strategy for distribution systems subject to catastrophic events. After faults are detected in the distribution system, microgrids are first formed to reduce losses and support critical loads, and then the formed microgrids are scheduled in real time to guarantee a safe and robust operation. Lastly, the system is restored to normal operation by dispatching repair crews and picking up cold loads.

Operation and planning for resilient multi-energy microgrid:

To fully enable the solutions of MGs and MPSs for resilience enhancement, some specific challenges must be addressed:

1. Previous work has developed various planning strategies for the cost-effective investment of modern power systems. However, most existing literature only considers power system operations under normal contingencies. Thus, it is urgent to develop a resilience-driven planning model for the optimal sizing problem of power systems, given the high-impact nature of extreme events. Furthermore, MPSs, as an emergency technology, have been gradually integrated into power system operations towards effective load restoration via realistic routing and scheduling behaviours. However, most research focuses on the operation level rather than the planning level, which might not fully exploit the key benefits of these MPSs on resilience enhancement [81].
2. The urgent need for resilience enhancement requires distribution systems to be managed in an efficient and secure manner. In this context, a paradigm shift from a centralised to a decentralised control may enhance resilience. As an emerging operation paradigm recently, microgrids provide a viable solution by constructing a hierarchical infrastructure to manage DERs in distribution networks [79]. In contrast to the centralized supervision in distribution networks, microgrids may operate in a decentralised manner to manage regional operations in emergency conditions. However, the capacity and functionality of a single microgrid are limited to achieve effective resilience enhancement of the distribution network, since the other microgrids may not be capable of being restored by themselves [80].
3. Routing MPSs to boost resilience requires coordination of the energy system and the transportation system. Although significant research has been carried out on the integration of energy and transportation sectors [82], the models and interactions become more complex when a large population of MPSs behave routing and scheduling in the couple energy and transportation networks, making the problem highly dynamic and stochastic.
4. Moving towards decarbonisation is expecting an increasing penetration of RESs. However, integrating intermittent RES becomes a serious challenge due to their limited-controllable variability and partial predictability. The stochastic programming and robust optimization have been widely used to handle the uncertainties of RES [83]. However, a large number of scenarios generated may cause severe computational

burdens. Meanwhile, modelling the probability distribution for the uncertain parameters is even more challenging.

3.2.2.2 Innovation provided

Cascading Analysis and Quantification:

So far, the identification of critical components has been primarily performed through the analysis of graph and topological features or by extracting trends from data using explanatory data analysis. While these approaches have yielded valuable insights, they often prove to be time-consuming and impractical, particularly when dealing with high-dimensional datasets. However, the identification of critical components is of utmost importance, as these components are more susceptible to failure and can potentially lead to significant load shedding within a network.

Event simulator of a progressing wildfire and assessment of its impact on distribution system:

Distribution line faults can provoke wildfires, particularly in regions with high temperatures and winds and low humidity. In order to address this hazard, a comprehensive assessment of wildfires' potential impact on distribution system is required.

In the premises of this sub-task, a tool is going to be developed, aiming at determining the optimal scheduling of the distribution system operation and resources to significantly enhance its resilience, considering the varying conditions during the spread of a progressing wildfire and its impact on the system. By using close coordination between all engaged actors (DGs and ESSs, if any) it will enhance the defense of the grid against these extreme events, providing a list of emergency operational measures for the DSO.

The tool will use a stochastic programming approach to determine the operation of a resilient distribution system exposed in an approaching wildfire. A wildfire is able to cause a direct damage to distribution system components or to decrease thermal rating of the lines due to the increase of the conductor's surface temperature [84]. Dynamic Line Rating (DLR) is employed to capture the influence of the wildfire on the conductor's temperature for overhead lines. The calculation of conductor temperature for changing weather conditions over the time horizon is based on the application of the non-steady-state heat balance. The main contributions of this sub-task in the overall C3PO features are summarized as follows:

- The tool will be able to effectively model wildfire events and to assess their spatial and temporal impact on distribution system (such as line outages, lines capacity reduction, spatiotemporal load shedding).
- The DLR of overhead lines is integrated in distribution system operation, in order to enhance resilience against an approaching wildfire.
- The impact of the wildfire on the line's functionality is considered, not only on conductor's temperature. This provides a better appraisal of the wildfire effects.
- The non-steady-state heat balance equation is used to take into account the influence of the wildfire on the conductor's temperature.
- It will introduce a stochastic programming approach to capture the uncertainties of load demand, weather conditions (wind speed and direction, solar radiation) and RES generation.

Resilience Driven Planning:

This task introduces optimization tools based on a stochastic mixed integer linear programming model for optimal line hardening, and placement of switches/ DGs to improve DS's resiliency under extreme events. A key component of this task will be to develop integrated decision-making frameworks for resilience-driven investment and operational planning strategies. As part of this project, optimization techniques will be applied to determine network investment strategies. In addition, operational planning strategies will be integrated in the model to enhance power system resilience with reduced investment costs. Furthermore, general algebraic formulations will be designed to measure overall DS resiliency while considering post-disaster restoration operation to be used in the resilience-driven planning studies. These metrics are integrated into resilience-driven planning models. It is expected that integrated optimization of infrastructure solutions and flexible resources will eventually reduce the need for bulk infrastructure enhancements or expansions, thereby reducing the cost of infrastructure investment. The main contributions of this task are summarized as follows:

- Developing a set of linear formulations for evaluating the nodal- and system-oriented resiliency metrics of complex distribution systems while considering possible interruptions following a cascading extreme event.
- Integrating the developed resilience metrics in the infrastructure and operational planning problems considering flexibility strategies.
- Introducing effective two-stage stochastic optimization programming to deal with the complexity and stochastic nature of the planning problems.
- Multiobjective approaches are introduced to deal with conflicting objectives, i.e., investment cost and resilience improvement metrics to facilitate decision-making for system operators and planners.

Post-disruption distribution system operation and restoration based on flexible microgrid formation and scheduling:

This task aims to enhance distribution system resilience by determining the optimal operation and restoration activities after the occurrence of catastrophic events. After the occurrence of a major disruption, a pragmatic and effective way is to separate the system into multiple microgrids to maintain the electrical connection between DGs and critical loads (CLs). Forming microgrids is a dynamic process requiring a set of sequential switch operations to develop and extend the faulted distribution system. Subsequently, the formed microgrids should be sustainably scheduled to energize as many CLs as possible. In the microgrid scheduling scheme, a key task is to handle the stochastic power of DGs and loads in a robust and non-conservative manner to achieve a reasonable trade-off between system security and outage cost reduction. While the microgrids are operating, a tailored restoration scheme should be implemented to clear the existing faults and restore the system back to the normal operating state. During the restoration process, the repair crews should be dispatched in coordination with load peak to reduce system interruption time and accelerate load energization. Considering the potential strategies (microgrid formation, scheduling, and restoration) for distribution system resilience enhancement, this task proposes an integrated operation and restoration strategy for distribution systems subject to catastrophic events. The main contributions of this task are summarized as follows.

1) Proposing a two-stage dynamic microgrid formation model for post-disruption distribution systems. The first stage determines the final and optimal microgrid topology to be formed, and the second stage searches for a set of sequential switch operations toward the desirable microgrids.
2) Proposing a real-time microgrid scheduling model considering source-load stochasticity. The uncertain power of DGs and loads is formulated with the joint chance constraint to develop a non-conservative scheduling scheme that guarantees the overall violation of system states under a desirable probability. Furthermore, the proposed scheduling scheme is implemented with model predictive control to provide real-time dispatch values for DGs and loads in the distribution system.
3) Proposing a dynamic distribution system restoration model by coordinated repair crew dispatch and cold load pickup. The repair crew dispatch is formulated with chance constraints to incorporate the stochastic repair time, which is updated dynamically according to the fault knowledge acquisition. After a fault is cleared, cold loads are selected to be picked up so that the secure frequency condition is met.

Operation and planning for resilient multi-energy microgrid:

The aim of this task is to develop a tri-level defender-attacker-defender (DAD) planning model as well as a series of model-free smart control algorithms to optimally operate DERs and mobile sources under the concept of MGs for resilience enhancement with a cost-efficient solution. The objectives can be listed as follows:

1. To develop resilience-driven planning strategies for the optimal sizing of mobile power sources (MPSs) in the context of microgrids, including mobile energy storage systems (MESSs) and mobile emergency generators (MEGs). Specifically, the capacities and locations of these MPSs can be optimally decided for resilience-driven microgrid operations, where the routing and scheduling behaviours of these MPSs are also considered in the planning strategy towards realistic decision making.
2. To develop resilience-driven operation strategies for microgrids under the concept of networked-microgrid (NMG), where the system resilience can be enhanced by switching tie-lines and sharing energy resources among NMGs.
3. To develop real-time smart control strategies for MPSs and repair crews (RCs) to enhance microgrid resilience given their mobility and flexibility compared to static energy resources. Specifically, MPSs can route to the damaged locations in the transportation network and then provide energy supplies to the energy network. Furthermore, RCs as one of the critical mobile sources can also route to the damaged locations and make the repair decisions to recover the damaged components back to the normal operations. The microgrid resilience is consequently enhanced by the joint routing and scheduling behaviours of mobile sources in the coupled transportation-energy network.

3.3 RELEVANT USE CASES AND ACTORS

C3PO product is composed by the following tasks, developed in the premises of WP3:

- T3.1 Security assessment through advanced IT technologies – Cyber Risk Assessment Tool
- T3.2 Dynamic Cyber-Risk Status Evaluation
- T3.3 Spatial and Temporal Modelling and Quantification of Cascading Physical Events
    - T3.3.1 Spatial and temporal event and fragility modelling
    - T3.3.2 Cascading modelling and quantification
- T3.4 Resilience-driven investment and operational planning to mitigate or prevent cascading effects
- T3.5 Operation and Planning of Advanced Multi-Energy micro-grids for Enhancement of Resilience
    - T3.5.1 Advanced control of mobile power sources in enhancing micro-grids resilience
    - T3.5.2 Resilience-driven optimal design of micro-grids
- T3.6 Knowledge sharing – Cyber Threat Intelligence and cascading events

Each of these tools encompass a set of Use Cases that describe the proposed technical solutions in detail, its functionalities and services. A comprehensive analysis of the Use Cases that will be developed within the R^2D^2 project, covering the functionalities, requirements and step by step analysis for all the tools can be found in the D2.1 document. The Use Cases developed within the C3PO product - WP3, are listed below (extract from D2.1 document):

Security assessment though advanced IT technologies – Cyber Risk Assessment Tool

This task will be performed through the following use-cases:

- UC ID and title: **UC24 - Cyber Security Risk assessment on EPES infrastructure**
    - Related business cases: BC3
    - Short description: The aim of this use case is to demonstrate the use of the developed C3PO Cyber Risk Assessment Tool (T3.1), and its capability to identify and assess risks, measure risks levels and assess the security posture of the target environment, propose risk mitigation measures, including the developed R^2D^2 components.
    - Demonstration pilot site: Greece
    - Actors: System Operator, Cyber Security Experts, C3PO Cyber Risk Assessment Tool

Dynamic Cyber-Risk Status Evaluation

This task will be performed through the following use-cases:

- UC ID and title: **UC25 - Dynamic Cyber-Risk Status Evaluation considering existing technical vulnerabilities**
    - Related business cases: BC3

- Short description: The C3PO Dynamic Cyber Risk Evaluation Tool will facilitate the dynamic and close to real-time threat detection and mitigation as well as vulnerability management in the targeted IT/OT environment, by (proactively) assessing associated risks for the organization's target environment.
- Demonstration pilot site: Greece
- Actors: System Operator, Deep Learning Data Analytics Software, Cyber Threat Intelligence Collection/Sharing System, Vulnerability Assessment Tool, Cyber Security Experts

Spatial and Temporal Modelling and Quantification of Cascading Physical Events

This task will be performed through the following use-cases:

- UC ID and title: **UC22 – Prevention and mitigation of cascading effects in case of extreme weather events**
  - Related business cases: BC1, BC2
  - Short description: This Use Case focuses on the enhancement of the grid's resilience under extreme weather events. The analysis of the network's current state, along with potential cascading effect indicators calculation that derive from a possible extreme weather event, are necessary for the R^2D^2 tools to propose the optimal corrective actions for the minimization of potential major outages. A series of actions, like network flexibility capability and reconfiguration actions are utilised for the grid's resilience enhancement. Finally, a faster restoration of outages can be achieved, through the optimal workforce allocation in the critical parts of the network.
  - Demonstration pilot site: Greece
  - Actors: EMMA GIMAN, C3PO Cascading simulators, operational network planning modules, DSO, Weather service provider, SCADA/DMS

- UC ID and title: **UC29 – Event simulator of a progressing wildfire and assessment of its impact on Distribution System**
  - Related business cases: BC1
  - Short description: The purpose of this Use Case is to expand T3.3 event simulator which is mainly focused at windstorms and fragility-based modelling to also include the modelling of wildfire events. The presented scheme will assess the impact of wildfire events on distribution system (such as line outages, spatiotemporal load shedding, wildfire's trajectory assessment, etc.) by using a stochastic programming structure to capture the uncertainties. The goal of this Use Case is to provide an optimal operational scheme and corrective actions for enhancing distribution system resilience considering the varying conditions during the spread of a progressing wildfire.
  - Demonstration pilot site: Greece

- Actors: System Operator, C3PO, External Weather Service Provider, Fire Station, SCADA-DMS

Resilience-driven investment and operational planning to mitigate or prevent cascading effects

This task will be performed through the following use-cases:

- UC ID and title: **UC23 - Cooperative crisis handling in case of cascading event**
  - Related business cases: BC1, BC2, BC4
  - Short description: This Use Case focuses on the upward or downward signal/alert that must be exchanged between the system and the network operator, in order to prevent a potential cascading effect caused by a failure in the interconnection point between system and network.
  - Demonstration pilot site: Greece
  - Actors: C3PO Cascading simulators, operational network planning modules, TSO, DSO
- UC ID and title: **UC30 - Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling**
  - Related business cases: BC1, BC2
  - Short description: The use case aims to enhance distribution system resilience by determining the optimal operation and restoration activities after the occurrence of catastrophic events. The integrated operation and restoration solution provided by the use case includes a flexible microgrid formation scheme to separate the faulted system into multiple microgrids, a sustainable microgrid scheduling scheme to dispatch the stochastic power of distributed generators and electrical loads, and a frequency-aware restoration scheme to dispatch repair crews and pick up loads.
  - Demonstration pilot site: Greece
  - Actors: System Operator, C3PO, Energy Service Company, Repair crews, SCADA-DMS

Operation and Planning of Advanced Multi-Energy Micro-grids for Enhancement of Resilience

This task will be performed through the following use-cases:

- **UC ID and title: UC 32 - Planning and operation for a resilient multi-energy micro grid**
  - Related business cases: BC1, BC2, BC5
  - Short description: The use case aims to enhance the system resilience of a multi-energy micro grid by planning and operating the mobile sources. Specifically, a three-level defender-attacker-defender model is developed to plan the optimal sizing and pre-positioning of mobile sources in

networked micro grids with decentralized control; an advanced learning-based algorithm is developed to control the routing and scheduling of mobile sources in a coupled energy-transportation network to maximize the load restorations of a multi-energy micro grid.

- Demonstration pilot site: Greece
- Actors: Micro grid central controller, Multi-energy micro grid, Mobile power source, Mobile energy storage system, Mobile emergency generator, Electric vehicle, Repair crew, Distributed energy resources, Transportation operator

Knowledge sharing – Cyber Threat Intelligence and cascading events

This task will be performed through the following use-cases:

- UC ID and title: **UC26 - Cyber Threat Intelligence knowledge collection/sharing with external sources**
  - Related business cases: BC4
  - Short description: The aim of this use case is to demonstrate the capabilities of the Cyber Threat Intelligence CTI Tool in collecting, correlating, producing added-value data ready to be ingested by security appliances and further disseminating CTI.
  - Demonstration pilot site: Greece
  - Actors: System Operator, C3PO CTI Tool (Cyber Threat Intelligence Collection/Sharing System), R^2D^2 Defence Mechanisms, CTI Community (e.g., EE-ISAC), CTI Sources

Each of these Use Cases will be integrated in the C3PO product using a common interface, developed in T3.7 premises. Table 2 summarizes the C3PO-WP3 Use Cases and their correlation with the product's tasks.

Table 2. WP3 Use Cases and related actors

ID	Title	Tool/Task	Actors
22	Prevention and mitigation of cascading effects in case of extreme weather events	T3.3, T3.4	EMMA GIMAN, C3PO Cascading simulators, operational network planning modules, DSO, Weather service provider, SCADA/DMS
23	Cooperative crisis handling in case of cascading effects	T3.3, T3.4	C3PO Cascading simulators, operational network planning modules, TSO, DSO
24	Cyber Security Risk assessment on EPES infrastructure	T3.1	System Operator, Cyber Security Experts, C3PO Cyber Risk Assessment Tool
25	Dynamic Cyber-Risk Status Evaluation considering existing technical vulnerabilities	T3.2	System Operator, Deep Learning Data Analytics Software, Cyber Threat Intelligence Collection/Sharing System, Vulnerability Assessment Tool, Cyber Security Experts
26	Cyber Threat Intelligence knowledge collection/sharing with external sources	T3.6	System Operator, C3PO CTI Tool (Cyber Threat Intelligence Collection/Sharing System), R^2D^2 Defence Mechanisms, CTI Community (e.g., EE-ISAC), CTI Sources

29	Event simulator of a progressing wildfire and assessment of its impact on distribution system	T3.3	System Operator, C3PO, External Weather Service Provider, Fire Station, SCADA-DMS
30	Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling	T3.4	System Operator, C3PO, Energy Service Company, Repair crews, SCADA-DMS
32	Operation and planning for resilient multi-energy microgrid	T3.5	Micro grid central controller, Multi-energy micro grid, Mobile power source, Mobile energy storage system, Mobile emergency generator, Electric vehicle, Repair crew, Distributed energy resources, Transportation operator

At this point it must be stressed that Use cases 22 and 23 are not software tools and therefore they are not presented in Section 4, however a short description of their features is employed at this section. These use cases are correlated to both C3PO and EMMA products and describe preventive activities against cascading effects in case of extreme weather events and cooperative crisis handling in case of cascading effects, from the DSO's (HEDNO) perspective.

The objective of use case 22 is to both assess and enhance the resilience of the grid against potential cascading effects from extreme weather events. Such an event can cause severe damages in the network infrastructure (e.g., several MV lines fed by a HV/MV substation, primary and secondary substations) and as a consequence, a major outage to several customers may occur. Initially, the module of 'spatial and temporal event and fragility modelling' (T3.3.1) will be used, in order to assess the system resilience, taking into account the existing network infrastructure and thus calculating fragility curves. Furthermore, the 'cascading modelling and quantification' module (T3.3.2) will be used to provide some crucial indications, related to the impact of the event. Based on this assessment, resilience enhancement measures to mitigate the impact in case of an imminent extreme weather event will be examined. Finally, the EMMA module developed in the 'resource management' Task (T6.3), will be the one to determine and allocate the available workforce and human resources in an optimal way, in order to achieve the fastest possible power restoration. The aforementioned mechanisms will include:

- Forecast of weather events that could potentially threaten the grid.
- Modelling of extreme weather impact on the network.
- Optimal schedule of demand response and energy storage systems to minimize load shedding.
- The application of further mitigation actions (isolation of faulted sections of a feeder, etc.)
- Automatic generation, assignment, and tracking of the necessary works to mitigate the identified problem

On the other hand, the goal of use case 23 is to examine the necessary signal that can be sent in case of a failure in the interconnection point between system and network, which may lead to a potential cascading effect. The cause of such an event could either be an extreme weather event or a cyber-attack. An extreme weather event as described in UC36, can cause severe damage to the grid infrastructure, and may lead to a possible outage.

Furthermore, in case of a cyber-attack, which may come from a possible malicious attack to the databases of the HV/MV substation control systems (e.g., SCADA) or from software/firmware distortion of the controllers of protection relays of MV lines, major parts of the network can be cut off. Considering that according to the HEDNO manual the loss of more than 50 MVA for more than half an hour is considered as emergency and IPTO (Greek TSO) should be notified, this UC focuses on the signals and alerts that must be exchanged between the system and network either upstream or downstream, so that a cooperative crisis handling between the operators can follow. In case either of an incident in the HV/MV substation (interconnection point between system-network) or an event, which may affect large part of the MV distribution network, a cascading event may occur. A possible result could be the HV/MV substation isolation and the grid operator must inform the TSO by sending a signal-alert, so that the latter can proceed to its necessary proactive actions. Furthermore, R^2D^2 C3PO tools could also be utilized from the DSO, in order to mitigate such an event, as described in UC36 (for physical events). If an incident (physical or cyber) has occurred in the system, which may affect the distribution network by leading to a loss of multiple MV lines, a signal must be sent to the grid operator, in order for the latter to take proactive measures for the mitigation of the event.

Each Task leader or participant defined several requirements for tool development. WP3 encloses 35 requirements in total, defined in the "Volere" tool. Table 3 depicts the mapping of C3PO/WP3 requirements to each of the described tools:

Table 3. WP3 requirements

ID	Requirement Description	Tool/Task
C3P_016, C3P_017, C3P_018, C3P_019, C3P_020	• C3PO Static Risk Assessment Tool should allow users (TSO/DSO operators) to define existing assets, assets criticality, and security controls to create an accurate representation of the system's security posture. • C3PO Static Risk Assessment Tool should assess risk considering asset criticality, threats likelihood and identified vulnerabilities criticality. • C3PO Static Risk Assessment Tool should provide guidance and recommendations (including countermeasures) for mitigating identified risks and vulnerabilities. • C3PO Static Risk Assessment Tool should provide access control to ensure that only authorized users have access to the system. • C3PO Static Risk Assessment Tool should be accessible through standard web browsers and compatible with different devices, such as desktops, tablets, and smartphones.	Security assessment through advanced IT technologies – Cyber Risk Assessment (T3.1)
C3P_021, C3P_022, C3P_023, C3P_024, C3P_025, C3P_026	• C3PO Dynamic CyberRisk Evaluation tool shall evaluate dynamically the EPES' Cyber-Risk Status considering assets' criticality, identified existing and emerging cyber threats as well as existing technical vulnerabilities. • C3PO Dynamic CyberRisk Evaluation tool should consume threat related information and technical vulnerabilities from the Cyber Threat Intelligence tool. • C3PO Dynamic CyberRisk Evaluation tool should consider DSO/TSO's assets' criticality, controls and their topology to assess risk values. • C3PO Dynamic CyberRisk Evaluation tool should provide near real-time alerts / notifications to experts when new technical vulnerabilities are identified, allowing for timely response and mitigation.	Dynamic Cyber Risk Status Evaluation (T3.2)

	• C3PO Dynamic CyberRisk Evaluation tool should evaluate risks utilizing T5.4 Deep Learning Data Analytics Module. • Access to Dynamic CyberRisk Evaluation tool will be authenticated and web-based.	
C3P_001, C3P_002, C3P_003, C3P_004, C3P_006, C3P_007, C3P_008, C3P_009, C3P_010	• Data of historical experiences with extreme weather. • Switches available in the feeders must be controllable • The topology of the grid at pilot sites must be known in advance. • Pilot sites must identify critical nodes of the grid. • C3PO must have access to weather forecast of the pilot site locations. • The topologies of pilot site networks must be well known and modelled. • In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the dispatchable DGs, RES and ESS units. • The location and technical characteristics of DERs must be known. • The characteristics of distribution lines must be known.	Spatial and Temporal Modelling and Quantification of Cascading Physical Events (T3.3)
C3P_001, C3P_002, C3P_003, C3P_004, C3P_006, C3P_007, C3P_008, C3P_009, C3P_010	• Ideally some historical weather data to better calibrate the wildfire event generation. • Data of historical experiences with extreme weather. • Switches available in the feeders must be controllable. • The topology of the grid at pilot sites must be known in advance. • Pilot sites must identify critical nodes of the grid. • C3PO must have access to weather forecast of the pilot site locations. • The topologies of pilot site networks must be well known and modelled. • In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the dispatchable DGs, RES and ESS units. • The location and technical characteristics of DERs must be known. • The characteristics of distribution lines must be known.	Resilience-driven investment and operational planning to mitigate or prevent cascading effects (T3.4)
C3P_008, C3P_009, C3P_010	• In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the dispatchable DGs, RES and ESS units. • The location and technical characteristics of DERs must be known. • The characteristics of distribution lines must be known.	Operation and Planning of Advanced Multi-Energy Microgrids for Enhancement of Resilience (T3.5)
C3P_027, C3P_028, C3P_029, C3P_030, C3P_031	• The Cyber Threat Intelligence Tool should collect cyber threat information from external sources to share with R^2D^2 components. • The Cyber Threat Intelligence Tool should disseminate sanitized indicators of compromise identified by R^2D^2 components, to the CTI community. • The Cyber Threat Intelligence Tool should enforce a sharing policy abiding to the DSO/TSO's information classification policies. • The Cyber Threat Intelligence Tool should support widely accepted formats of cyber threat information sharing.	Knowledge Sharing – Cyber Threat Intelligence (T3.6)

- The Cyber Threat Intelligence Tool should be able to generate alerts and notifications based on predefined rules.

-	-	Integration and UI (T3.7)

4. Product Description

The C3PO product is developed within the WP3 of the R²D² project and comprises an advanced toolkit designed to offer a comprehensive set of innovative solutions for stakeholders, encompassing cybersecurity and resilience assessment and enhancement tools. Section 4 provides a detailed description of the architectural design, functionalities, data exchanges and required resources of each C3PO tool.

C3PO will provide valuable practices and insights, offering static and dynamic frameworks for assessing and enhancing cybersecurity and resilience-oriented planning, preventive and restorative strategies, enabling stakeholders to efficiently evaluate and improve the overall defense of the grid against a growing number of hazards and threats across the energy value chain. These tools and data exchanges among them will be integrated in the C3PO Platform, utilizing two applications developed within WP3 to address the cybersecurity and the resilience tools separately, using a cohesive User Interface, thereby realizing the C3PO Suite.

C3PO encloses 6 technical tasks, 10 tools and 8 Use Cases. The Use Cases are engaged to the Greek pilot site of the R²D² project. The architecture of the whole product is shown in Fig. 1, where the various Use cases are classified to cybersecurity, resilience or knowledge sharing tasks. Specifically, tasks 3.1 and 3.2 address cybersecurity, while tasks 3.3, 3.4 and 3.5 refer to resilience frameworks and T3.6 is related to the development of the two aforementioned knowledge sharing databases. Use Cases 24 and 25 are corresponding to cybersecurity, Use Cases 29, 30 and 32 are correlated to resilience and Use Case 26 addresses the knowledge sharing tasks, respectively.

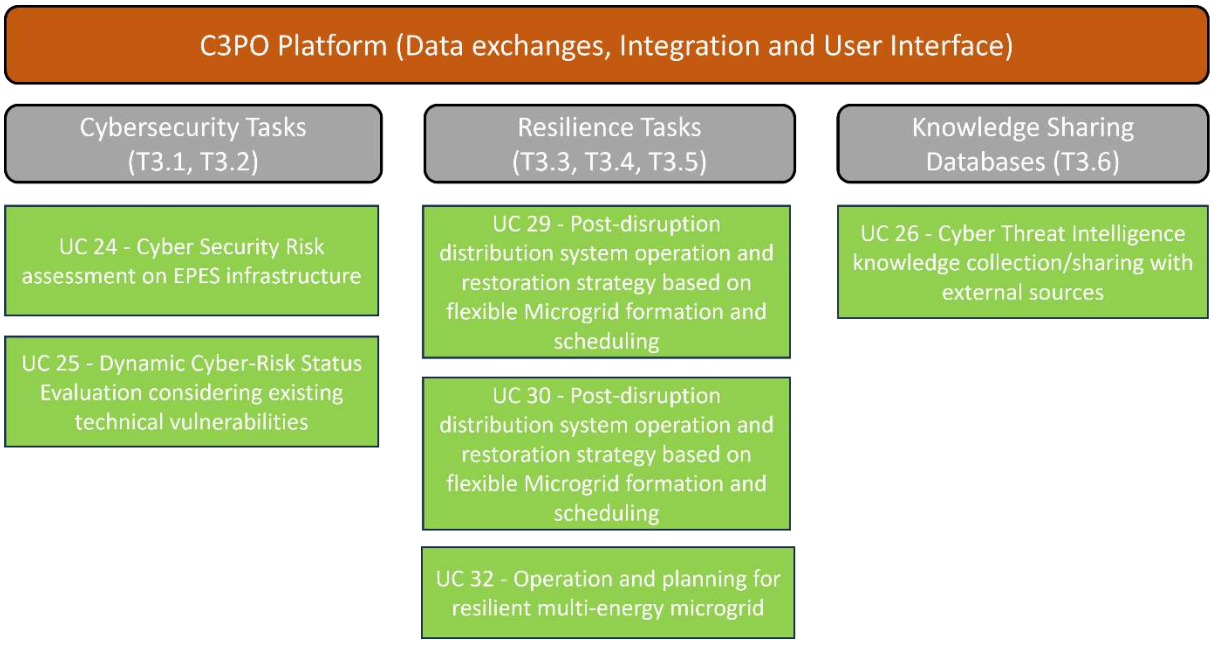


Figure 1. High Level Architecture of C3PO Suite

Fig.2 depicts the interconnections and data exchanges between C3PO tools as well as the communication with other R²D² products. As can be seen, the C3PO product communicates at a certain level with both the PRECOG and the EMMA tool. Task 3.1 will provide 3.2 with asset information, topology and asset criticality data, while the Cyber Threat Intelligence (CTI) tool will exchange information with both internal and external components. More specifically, it will consume information from external sources to feed internal R²D² tools, like the R²D² T3.2 Dynamic Risk Evaluation Tool and the R²D² T5.3 PRECOG SIEM, but will also share malicious activities identified by the R²D² Tools, with the community, thus contributing to the protection of the energy community against cyber actors. Use Cases 22 and 23, which refer to the DSO's (HEDNO) emergency actions against extreme weather events, are designed for both C3PO and EMMA products, hence the communication between the two products must be assured. With regard to the resilience frameworks, the advanced modular event simulator of task 3.3 will provide inputs of windstorm-related outages scenarios as initiating events to all sub-modules of tasks 3.4 and 3.5. Moreover, tasks 3.1-3.5 will provide relevant information and results data to the knowledge sharing databases of task 3.6.

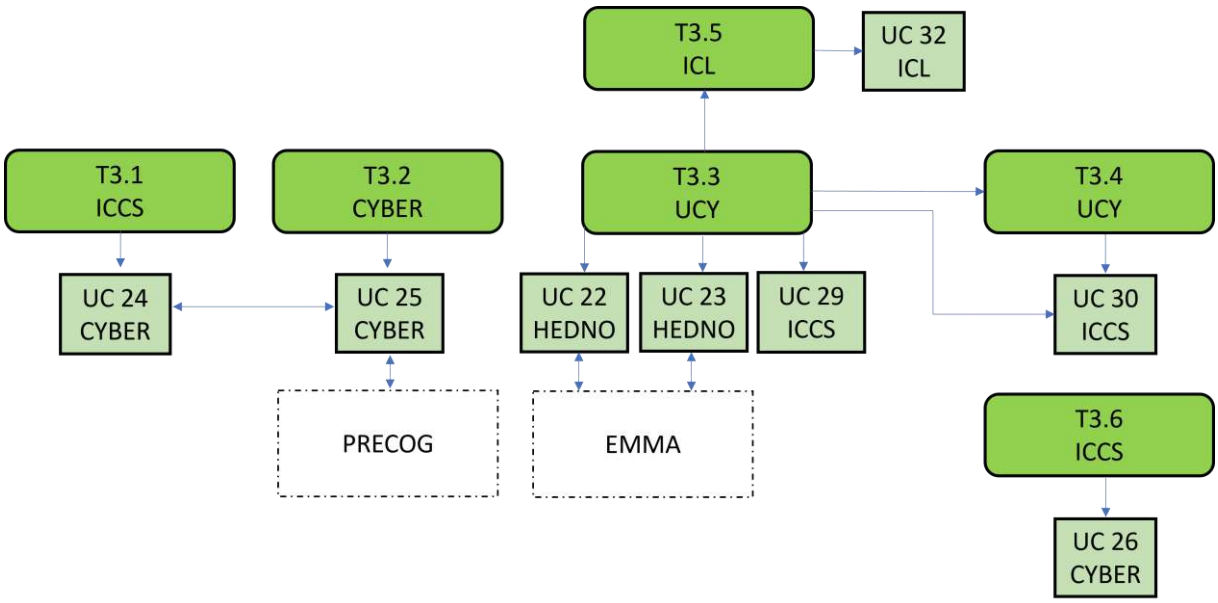


Figure 2. Interconnections between C3PO components and other tools

4.1 SECURITY ASSESSMENT THROUGH ADVANCED IT TECHNOLOGIES – CYBER RISK ASSESSMENT TOOL (TASK 3.1)

4.1.1 Internal Architecture of the Tool

4.1.1.1 Aim of the tool

A well-managed, underlying compliance base is essential for any cyber security program. This can only be achieved through a systematic, disciplined, and repeatable approach for evaluating an EPES security posture. The C3PO Cyber Risk Assessment tool will provide EPES operators the means to evaluate their operational technology (OT) and information technology (IT) security practices through a multifaceted and guided process. Operators will be able to evaluate their cybersecurity stance using EU regulatory requirements and many recognized industry standards and best practices like the NIS (2) Directive, ISO/IEC 27000 series, IEC62443, IEC62351, NIST Special Publication 800-82, Guide to Industrial Control Systems Security and NIST Cybersecurity Framework. Among the objectives of the Cybersecurity Risk Assessment Tool are the deployment of a common approach to assess and manage risks that will allow EPES operators to use as a reference tool to compare their security posture and risk levels with values provided by third parties in the same sector, to ensure that the community has a common understanding on the acceptable risk levels.

4.1.1.2 Detailed Architecture

The Cyber Risk Assessment Tool will have the following characteristics and provide the corresponding functionality that satisfies the typical cyber risk assessment process, but also elaborates risk management practices to provide advanced functionality that will give EPES the ability to more efficiently assess and manage risks:

- Import Assets identified in the target environment, to the C3PO Cyber Risk Assessment tool.
- Import Controls deployed in the target environment, including their maturity as a control's attribute.
- Define Asset criticality: Valuate and/or assess Asset Criticality / Impact (using EPES specific impact scales).
- Select Cyber Risk Scenarios for TSO/DSO infrastructure (using pre-defined risk scenarios).
- Automatically calculate Threat likelihood for each risk scenario.
- Automatically calculate vulnerabilities' criticality (considering applicable controls maturity and assets topology).
- Export defined assets – together with impact values - to be imported to MONARC as well as vulnerabilities' levels.
- Provide comprehensive Reporting and Visualization for the assessed risk levels through:
    - Dashboard / User Interface
    - Data Visualization Tools
    - GAP Analysis Reports
- Provide Risk Treatment Plan/ Capabilities to support and monitor the implementation of the controls.

The tool, and more specifically the interfaces to the users will be web-based, while access to the software functionality will be available to authenticated, using 2FA, users.

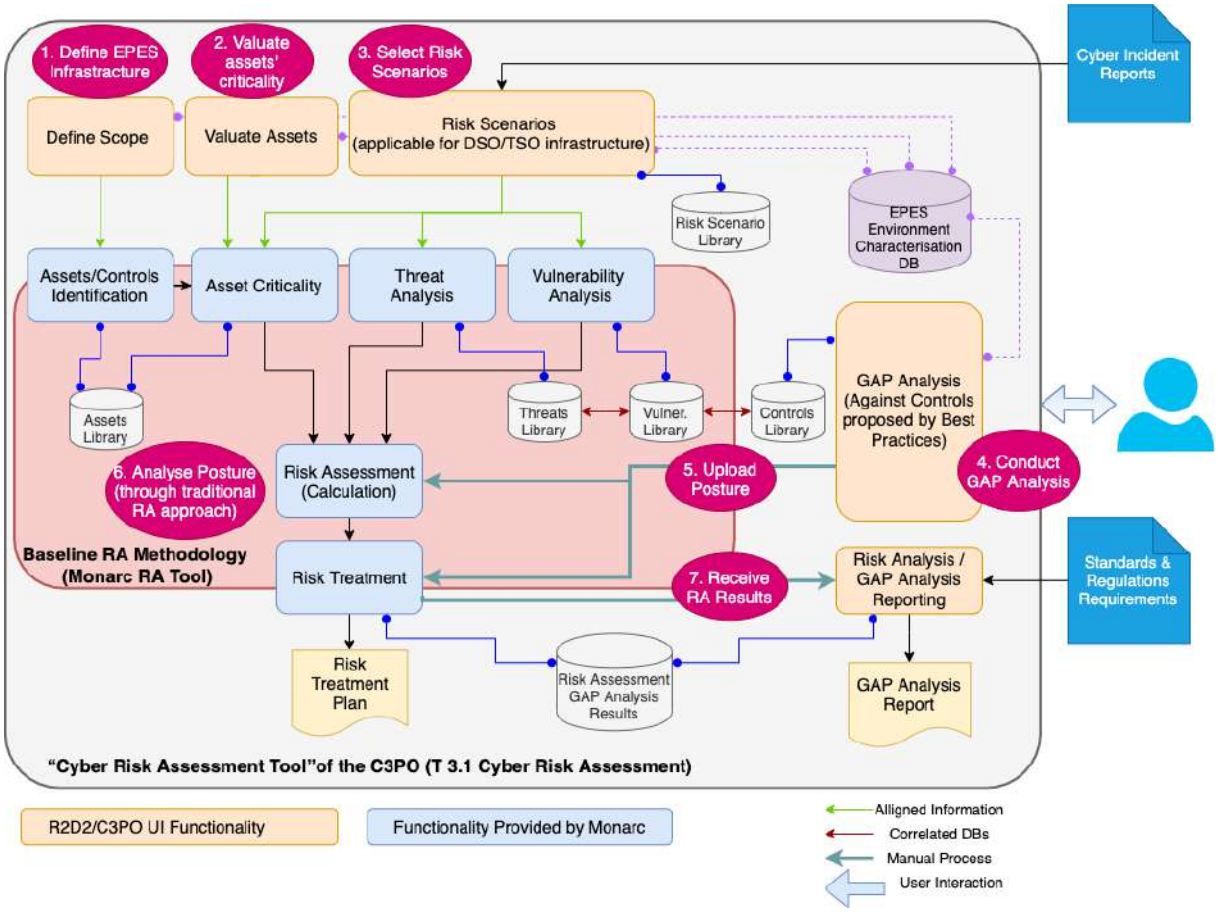


Figure 3. C3PO Cyber Risk Assessment Flow

Fig.3 depicts the C3PO Cyber Risk Assessment Tool and outlines the steps undertaken to conduct cybersecurity risk assessment using the provided tool. More specifically, the Cyber Risk Assessment process involves the following steps:

1. Define EPES infrastructure: the EPES operator populates the C3PO Cyber Risk Assessment Tool with information about the assets deployed in the target environment. The collected information will be stored on the EPES Environment Characterization DB.
2. Valuate assets' criticality: the EPES operator assesses the value of the target environment's assets using the provided scales regarding the impact to the organisation if a security dimension (confidentiality, integrity, and/or availability) of the asset is lost.
3. Select Risk scenarios: the EPES operator will have the capability to choose specific pre-defined risk scenarios related to well-known analysed security incidents.
4. Conduct GAP Analysis: the target environment is analysed in respect of well-established cybersecurity standards, regulations and/or best practices and gaps regarding the required deployed security controls are identified. Moreover, the criticality of the identified vulnerabilities is assessed for the chosen assets.

5. Upload EPES Environment Cyber Security Posture (assets, impact, vulnerability levels etc.): the details of the target environment, together with the assessed values about the vulnerability levels are uploaded to MONARC.

6. Analyse EPES Environment Cyber Security Posture

   Cybersecurity posture analysis is the core functionality of the Cyber Risk Assessment Tool. Based on the well-established MONARC methodology, the component will interact through the UI to get all the necessary information about the target environment and the customized assessment that the EPES operator wishes to conduct, to perform the assessment and the requested GAP analysis, based on the chosen standards and frameworks and for the chosen risk scenarios and provide the results and the reports back to the user. To accomplish the risk assessment, this component complements the typical process that MONARC provides towards a comprehensive security posture and gap analysis. It comprises the following sub-components:

   - **Assets Identification**: It is responsible for populating the Cyber Risk Assessment Tool with information about the target environment's assets and controls, as this is provided by the EPES operator, through the dedicated UI. The provided information will be collected from the Target Environment Characterisation DB and stored on the Assets Database.
   - **Assets Library**. This database will accommodate information about the target environment, such as the Assets and Controls, and the Assets criticality.
   - **Asset Criticality**: It allows the EPES operator to assess the assets' values by considering the provided EPES-oriented impact scales that will be developed for the needs of the tool. The information will be collected from the Target Environment Characterisation DB and stored on the MONARC's Assets Database.
   - **Threats Analysis**: It handles the set of threats that will be used for the risk assessment, based on the selected risk scenarios or the applicable to the target environment threats, selected from the Threats Library. which will accommodate all threats that will be defined for the target environment.
   - **Vulnerability Analysis**: It handles all vulnerabilities that are identified in the target environment and can be selected form the vulnerabilities libraries. Moreover, it is responsible for the (optionally) automated calculation of the vulnerabilities and criticalities considering the deployed security controls. This information will be collected from the Target Environment Characterisation DB and it will be calculated based on GAP analysis results.
   - **Risk Assessment**: Having established the context for the target environment, having identified the related threats and their likelihood, as well as the target environment's vulnerabilities and their criticality, this component can calculate the risk levels for all the requested risk scenarios.
   - **Risk Treatment**: For the risk scenarios whose assessed levels exceed the organisation's threshold, appropriate security controls can be suggested to mitigate them considering the already deployed controls, and their maturity. As a result, a risk treatment plan will be developed to be handed to the EPES operator for further consideration.

7. The risk assessment algorithm will be applied by using the MONARC risk management software tool.

4.1.1.3 Description of Components

The Cyber Risk Assessment Tool comprises three main components responsible for instantiating the tool and populating information about the target environment (assets, criticality and controls), as well as providing results and reports (Risk Treatment Plan, GAP Analysis Report) through a dedicated UI, a library of Risk Scenarios for TSO/DSO infrastructures, and the core component responsible for assessing risks. The overall architecture of the tool is presented in Fig.3.

4.1.1.3.1 Information about the target environment

Define Scope

The scope definition process plays a crucial role in setting the boundaries and context for the cyber risk assessment. This initial step helps establish the framework within which the assessment will be conducted and ensures that the assessment focuses on the most relevant and significant aspects of the EPES. Having said that, this component provides all the necessary functionality to an EPES operator for populating information about the target environment, i.e., asset information so that GAP analysis can be performed considering specific standards of the operator's choice. The information is stored on the EPES Environment Characterisation DB.

Valuate Assets

The assessment of asset value in an EPES environment during cybersecurity risk evaluation is facilitated by the Valuate Assets component. This component accomplishes this assessment by employing customized impact scales tailored to the unique characteristics of the energy sector. These specialized impact scales ensure precise evaluation of energy-related assets, encompassing both cyber and cyber-physical aspects from the IT and OT environments, along with their associated impacts. This meticulous process guarantees that the most vital energy assets are assessed and prioritized appropriately, ultimately contributing to a comprehensive grasp of asset criticality within the EPES environment.

Risk Scenarios

This library will accommodate risk scenarios that will be developed specifically for the needs of the EPES environment and will be used to assess operators' risks associated with specific attack scenarios. Their development will be based on published reports and analyses of known cyber-attacks. It comprises the following components:

- **Definition of Risk Scenarios for TSO/DSO infrastructure**. This component implements the off-line process of preparing risk scenarios to be stored on the Risk Scenarios Library and consumed by the Risk Assessment components for assessing associated risks.

- **Risk scenarios library**. A database that will host all the defined Risk Scenarios for the EPES environment.
    - Attack Steps
    - Assets
    - Impacts (security Dimension)
    - Threats
    - Vulnerabilities
    - Controls

Cyber Incident Reports. This is an external source of information that will provide valuable insights about reported and analysed cyber-security incidents to be used in the development of risk scenarios. Well-known sources, like CISA Advisories will be part of this list of sources.

4.1.1.3.2 Baseline Risk Assessment (MONARC)

The heart of the C3PO Cyber Risk Assessment Tool is based on the well-established risk assessment method MONARC (Optimized Risk Analysis Method). It serves as both a tool and a method, enabling organizations to conduct optimized, precise, and repeatable risk assessments. The MONARC method provides a systematic and structured approach to risk analysis, focusing on understanding the context, evaluating risks, and implementing effective risk treatment measures. By capitalizing on previous risk analysis efforts and continually optimizing security measures, organizations can enhance their overall resilience against potential threats and vulnerabilities.

The key advantage of MONARC lies in its ability to capitalize on existing risk analyses conducted in similar business contexts. As many businesses in a sector, like the energy sector, encounter the same threats and vulnerabilities when dealing with common assets in the IT and OT environment, such as servers, smartphones, and IoT components, risk scenarios can be generalized for these assets based on context and business specifics. This ensures that risk management becomes more streamlined and adaptable across different organizations, as they can leverage insights from similar risk assessments. MONARC has the following phases:

- **Context Establishment**: The initial phase involves gaining a comprehensive understanding of the company or organization's context, challenges, and priorities to guide the risk analysis process effectively. This phase lays the foundation for the risk analysis by identifying the most vital elements that could impact the organization's operations.
- **Context Modelling**: In this phase, the identified assets from the previous step are detailed and formalized in a diagram that illustrates their interdependencies. The primary assets, such as critical processes or sensitive information, have impacts defined based on the information gathered in the context establishment phase. Secondary assets inherit the impact of the primary asset to which they are linked (object tree). The impact level of secondary assets can be manually adjusted to reflect their specific importance and relationship to primary assets.
- **Evaluation and Treatment of Risks:** The evaluation phase involves quantifying threats, vulnerabilities, and impacts to calculate the overall risks. This requires high-quality

information on the likelihood of threats, ease of exploiting vulnerabilities, and potential consequences, which is obtained using metrics validated by experts. The risk assessment process determines if any risks exceed the acceptable risk level as defined in the risk acceptance grid. If unacceptable risks are identified, risk treatment measures are developed and implemented to reduce these risks to an acceptable level.

- **Implementation and Monitoring:** After implementing the initial risk treatment measures, the process enters an ongoing management and monitoring phase. Security measures are continuously monitored, and recurring controls are conducted to ensure their effectiveness and sustainability. This phase aims to improve security measures continually and enhance risk management in a dynamic environment. It involves increasing the detail of objects used in the risk analysis and expanding the scope of the analysis to cover a broader range of assets and processes. Note that this phase is out of the scope of the Tool's functionality.

Having the above as the basis for conducting risk assessment on an EPES environment, the C3PO Cyber Risk Assessment Tool will complement it with the following key capabilities, thus providing a comprehensive solution designed to streamline and optimize the risk assessment process for EPES Pilots' specific infrastructure:

- **Data Import and Infrastructure Configuration**: provides a user-friendly interface that allows EPES Pilots to import their infrastructure data seamlessly. This includes details about
  - primary i.e., data and services,
  - supporting assets i.e., software, hardware, communications, premises, that are used to manage the primary assets, and
  - controls or security measures

  that are in scope for the risk assessment. Users can organize and categorize these assets and controls for easy management.
- **Asset Criticality Valuation**: It enables the application of EPES' specific impact models to valuate the criticality of assets. By considering the potential consequences of asset failure or compromise, with respect to at least the three security dimensions i.e., confidentiality, integrity and availability, EPES Pilots operators can inform the tool about the assets values.
- **Vulnerabilities Scoring Calculation**: The tool leverages its advanced algorithms to calculate vulnerabilities scoring for each asset and control in the infrastructure. It takes into account factors such as the potential impact of a vulnerability being exploited and the likelihood of such an event occurring. These scores provide valuable insights into the areas of highest risk within the infrastructure.
- **Risk Scenario Selection and Execution**: The tool allows users to choose and customize risk scenarios based on various threat vectors and operational contexts, but also on pre-defined scenarios available in the Risk Scenarios library. Risk analysts can execute risk assessments for specific scenarios, which helps them target their risk management efforts precisely.
- **GAP Analysis Against Controls:** The tool facilitates conducting GAP analysis through a comprehensive questionnaire tailored to EPES's unique requirements. This feature

enables a detailed comparison of existing controls against industry best practices and regulatory standards, highlighting areas where additional measures are needed.

- **Data Communication to MONARC**: The tool facilitates smooth data communication to the MONARC platform, ensuring that all the collected and calculated risk assessment data is accurately and securely transferred for further analysis and reporting.

Remediation Proposals and Reporting: The tool goes beyond risk assessment by offering support for implementing remediation proposals. It generates detailed reports that highlight risk exposure, recommended controls, and the potential impact of proposed risk treatments. These reports help EPES Pilots make well-informed decisions to enhance their security posture.

4.1.1.3.3 GAP Analysis & Reporting

Conduct GAP Analysis

The GAP Analysis component provides a solution designed to meticulously evaluate the alignment of deployed security controls with various well-established cyber-security standards, regulations, and industry best practices. In today's complex cybersecurity landscape, it is imperative for organizations to ensure that their security measures not only meet regulatory requirements but also adhere to the highest industry standards. The tool provides a holistic assessment, offering a detailed comparison of the existing security controls registered to the tool by the EPES operator, against the chosen standards.

The GAP Analysis tool goes beyond the conventional assessment against applicable best practices. It takes into account the identified vulnerabilities and the details of the target environment, including assets, controls and their topology, to automatically assess the criticalities of vulnerabilities. By doing so, it delivers a contextualized evaluation that reflects the actual risk landscape of the EPES environment. This means that the EPES operator, will not only gain insights into the compliance posture, but will also receive a tailored understanding of the vulnerabilities that pose the most significant threats to the reported assets.

Critical role in the GAP Analysis process and in the functionality of the C3PO Cyber Risk Assessment tool has the EPES Environment Characterisation Database, which accommodates all the information about the target environment, and which includes the Assets, deployed Controls, and related Vulnerabilities.

The Controls Library is another important source of information for the GAP Analysis process as it will accommodate the controls required or recommended by the adopted standards/best practices (at least 2 of them). These controls will be related to vulnerabilities to ease the integration with MONARC and the automated assessment of the vulnerability criticality, as in MONARC the vulnerability criticality level has a strong dependency on the deployment of appropriate security controls, as well as their maturity and strength. Equally important in this process is the mapping among the different sets of security measures/controls as each methodology, standard, or recommendation adopts its own controls library and terminology which is not directly mapped to the rest of the standards/recommendations.

The results obtained for each control area assessed evaluated according to the following evaluation scheme which is represented in Table 4:

Table 4. GAP Analysis Evaluation Scheme

Value	Description
Not Implemented	This value is selected if the corresponding security controls (for a particular objective of the standard) are not addressed or are not implemented.
Partially Implemented	This value is selected if the corresponding security controls (for a particular objective of the standard) are implemented partially (e.g. policies, procedures, standards) or pending approvals.
Implemented	This value is selected if the corresponding security controls (for a policy of the standard) are fully implemented.
Not Applicable	This value is selected if the corresponding security controls (for an objective of the standard) are not applicable to the Organisation.
Not Implemented	This value is selected if the corresponding security controls (for a particular objective of the standard) are not addressed or are not implemented.
Partially Implemented	This value is selected if the corresponding security controls (for a particular objective of the standard) are implemented partially (e.g. policies, procedures, standards) or pending approvals.
Implemented	This value is selected if the corresponding security controls (for a policy of the standard) are fully implemented.
Not Applicable	This value is selected if the corresponding security controls (for an objective of the standard) are not applicable to the Organisation.

GAP Analysis/Risk Analysis Reporting

The reports produced by the C3PO Cyber Risk Assessment tool will summarize the results of the GAP Analysis conducted by EPES operator and will present current level of compliance with the selected standards/best practices (e.g., ISO/IEC 27001). The reports will provide EPES operator's Top Management a better indication of where the organisation stands in terms of the standard/best practice and roughly what effort is required to be fully compliant. More specifically, in the produced reports not only security gaps against requirements will be listed but also specific recommendations and corrective actions for each identified security gap will be provided.

The GAP Analysis reports will include diagrams to depict the overall level of compliance of the Organisation, against selected standards/requirements. More specifically, these diagrams will illustrate issues like the overall level of compliance, including all controls listed in a specific baseline standard (in the form of pie-chart), the level of compliance per control area (in the form of Bar-charts) etc.

Furthermore, the C3PO Cyber Risk Assessment tool, using the Risk Assessment results produced by MONARC, will formulate a **Risk Treatment Plan (RTP)** identifying the appropriate management actions, resources, responsibilities, and priorities for dealing with its information security risks. The RTP should be set within the context of the organization's information security policy and should clearly identify the approach to risk and the criteria for accepting risk.

4.1.1.4 Techniques & Algorithms

The baseline risk assessment process that will be used by the C3PO Cyber Risk Assessment tool, will be based on the well-established MONARC risk assessment method. The sub-stages provided by the method are also in line with ISO/IEC 27005:

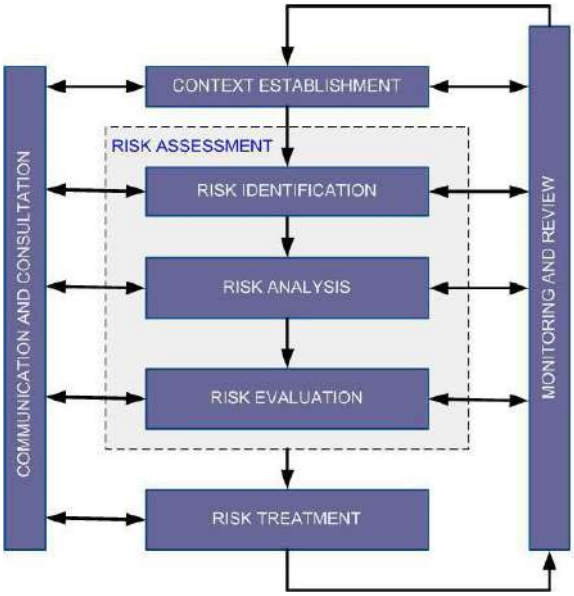


Figure 4. ISO 27005 - Information Security Risk Management Methodology

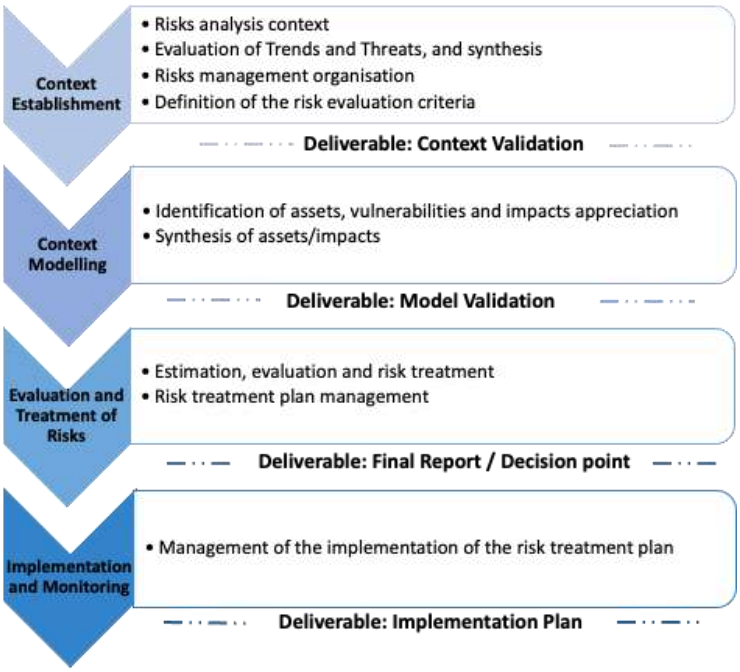


Figure 5. MONARC risk assessment process

MONARC is based on a library of risk models offering objects made of risk scenarios by assets or groups of assets (Fig.6). This approach facilitates the management of the most common risks and allows for benefits in objectivity as well as efficiency. As MONARC is completely repeatable, these results can be intensified and adjusted to the maturity of each organisation by increasing the depth of risk scenarios.

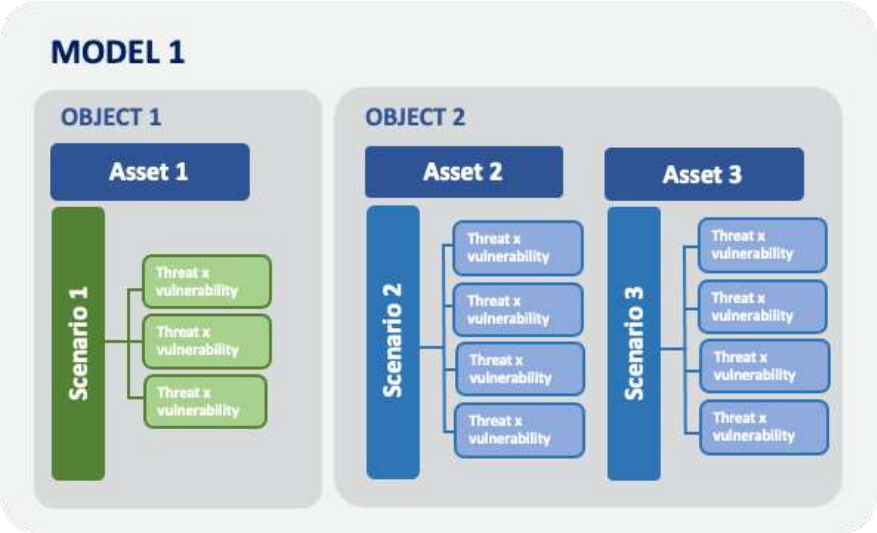


Figure 6. Objects, assets and risk scenarios in MONARC.

The risk analysis is made by describing the primary assets (business or information process according to ISO/IEC 27005:2011) and by associating objects modelling the predefined risks in a cascade mode, that is to say, by building a tree of objects. The impact is defined at the highest level and inherited downwards to all the risk objects in order to calculate cybercity risks.

4.1.1.5 Data Exchanges & Interfaces

Data exchanges, communication with other tools and/or products (data flows and protocols)

- The Gap analysis tool exports the identified assets and their corresponding criticality to be imported in MONARC.

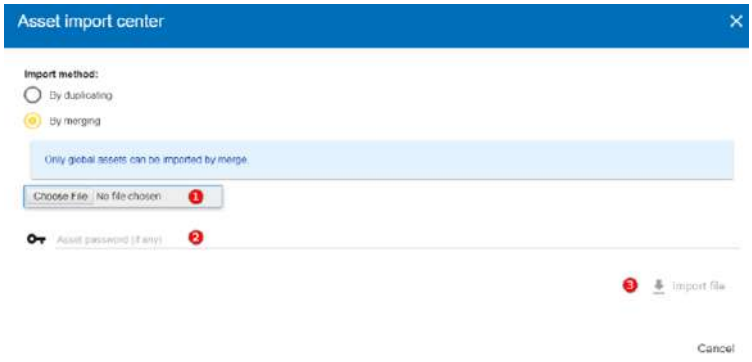


Figure 7. MONARC's assets import centre

There are two types of assets:

a. Primary or business assets: They generally represent, but are not limited to, internal or external services, processes or information. They are the ones that are at the root of the analysis and that will decline their impact on other assets. The containers used to organize the analysis visually are declared as a primary asset (e.g., Back Office).
b. Secondary or supporting assets: These are the assets on which risks are associated, they are using to describe the risk profile of the primary assets.

- The Gap analysis tool exports the selected control along with identified assets and their corresponding criticality to be imported in MONARC.
- Gap analysis (Controls Maturity) -> MONARC (file)
- Gap analysis exports the identified Vulnerabilities and their corresponding score to be imported in MONARC.

Vulnerabilities describe the risk context in a negative way. The greater the vulnerability, the less existing or effective measures are. Vulnerability is inverse to maturity. Example: "Absence of identification of sensitive assets": Low vulnerability if the sensitive assets are identified and vice versa, the vulnerability is great if they are not. The description of the vulnerability is very important because it appears in the risk table as an additional description that helps the security specialist to refine his questionnaire or the precise points that are sought in relation to a risk.

4.1.2 User Interface

In this section we provide preliminary user interfaces, including dashboards and mock up that will be implemented for the needs of the C3PO Cyber Risk Assessment tool.

4.1.2.1 MONARC

4.1.2.1.1 Risk identification

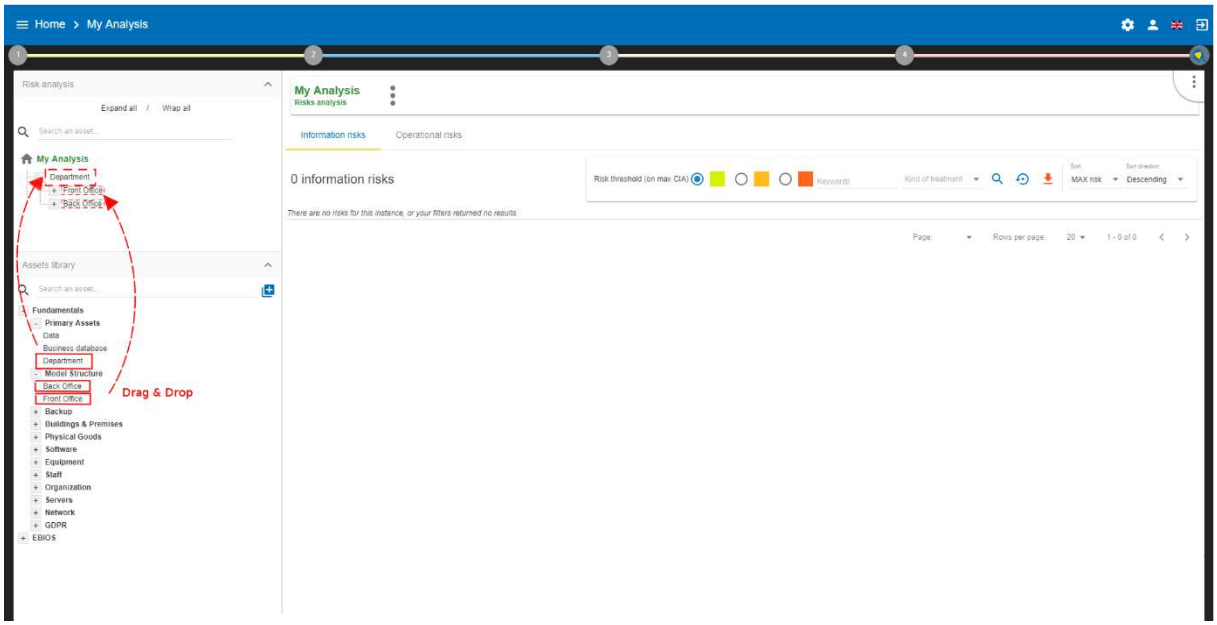


Figure 8. MONARC's scope definition environment

4.1.2.1.2 Edit impacts and consequences

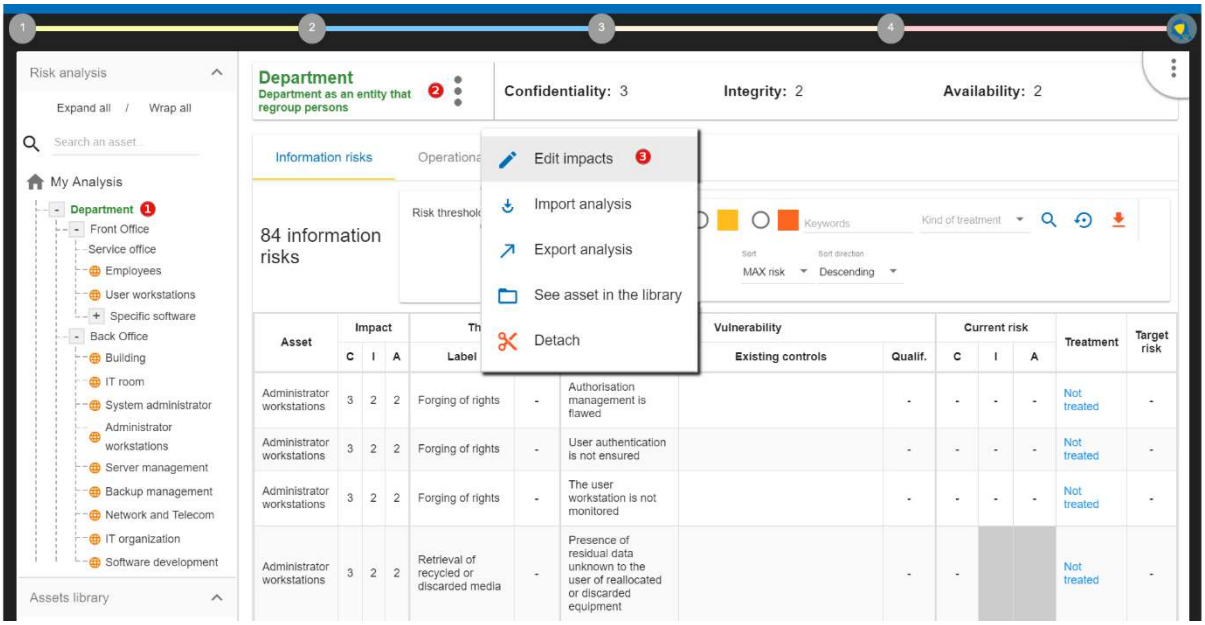


Figure 9. MONARC's assets impact assessment environment

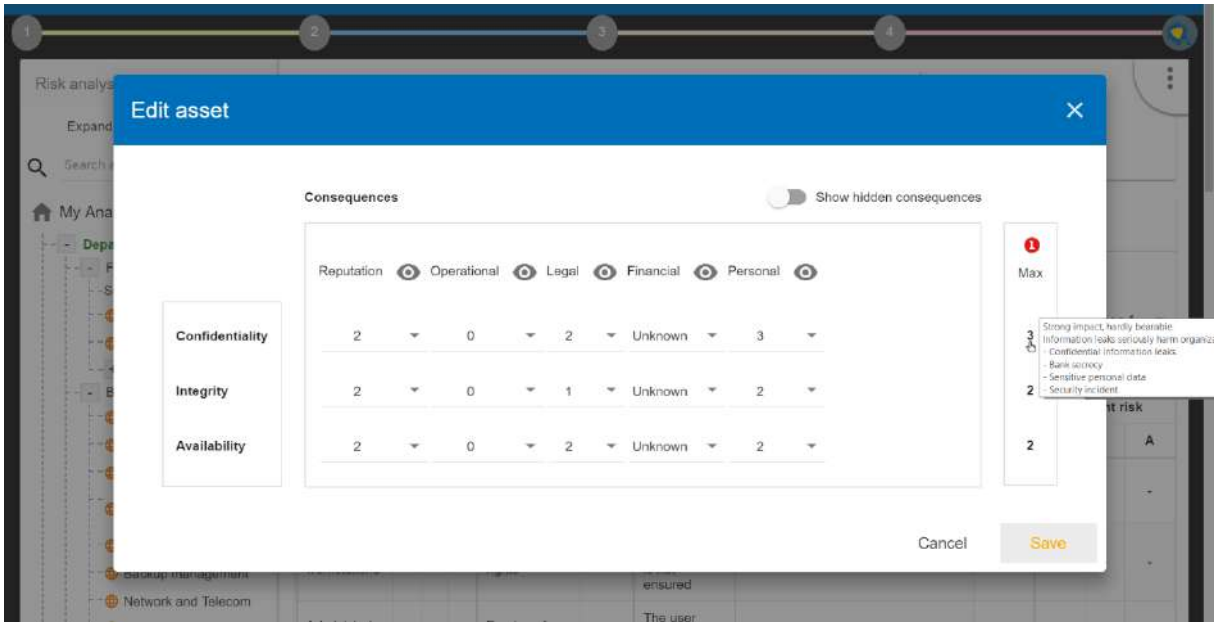


Figure 10. MONARC's assets impact levels

4.1.2.1.3 Risk Assessment

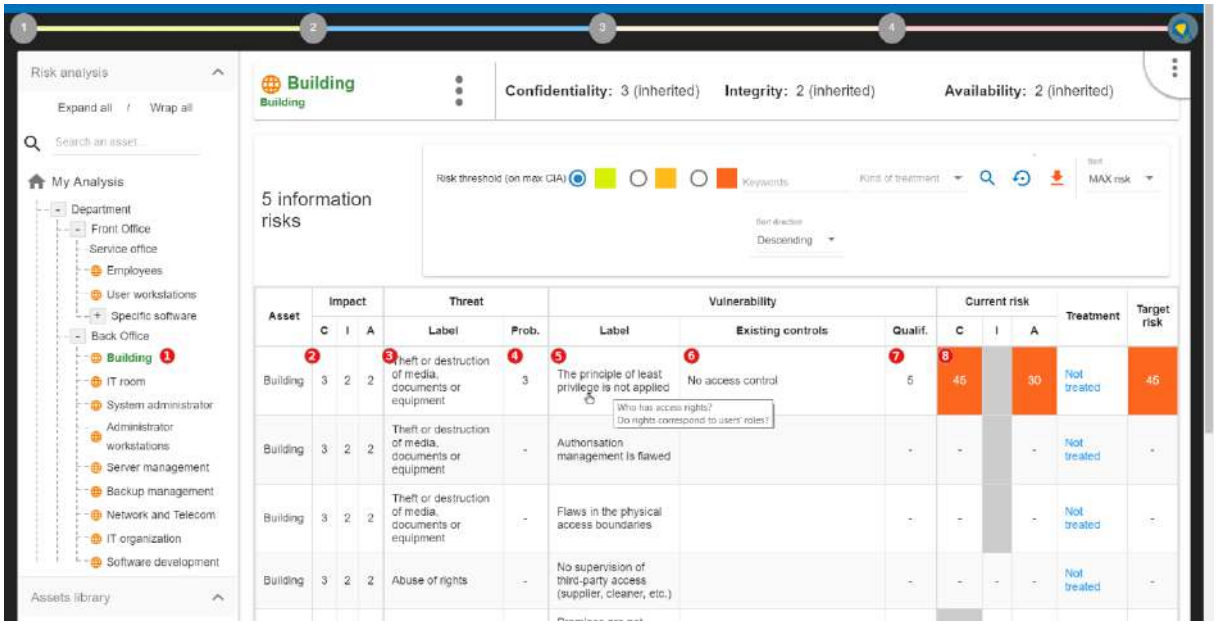


Figure 11. MONARC's risk assessment steps

4.1.2.1.4 Risk Treatment

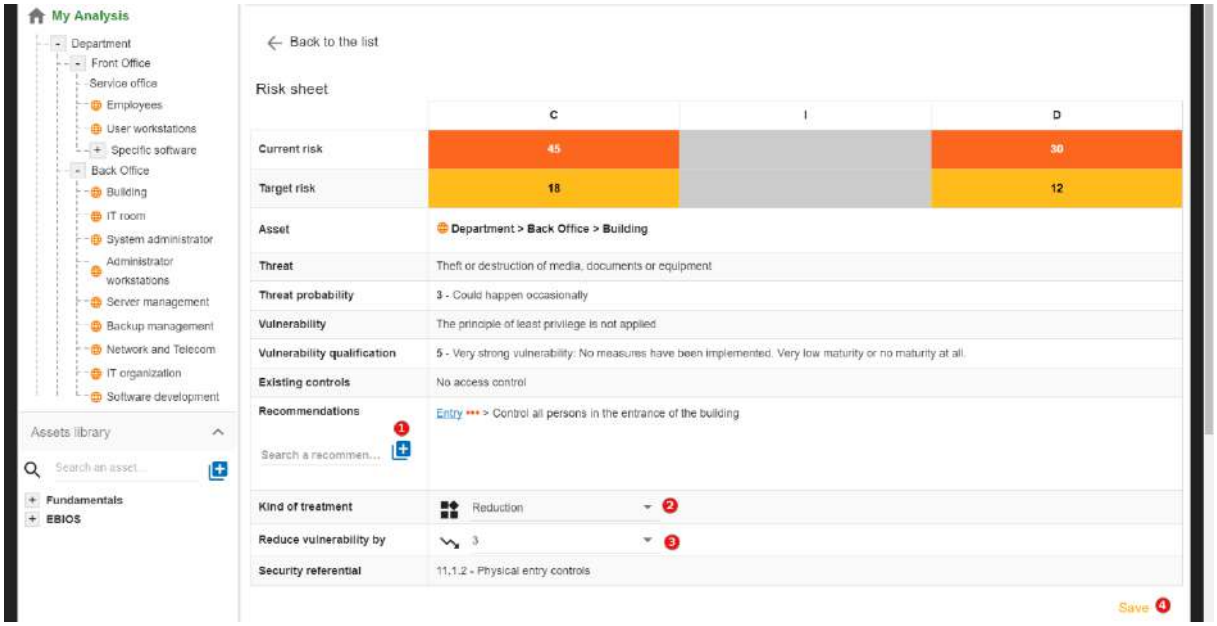


Figure 12. MONARC's risk treatment options

4.1.2.2 R²D² GAP Analysis Tool

The following mock-up depicts the Cyber Risk Assessment tool log-in page.

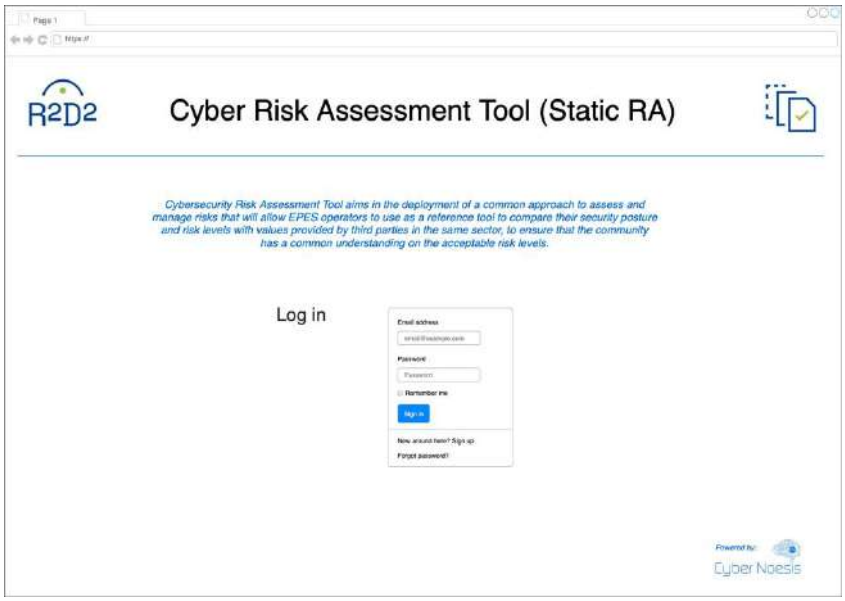


Figure 13. Cyber Risk Assessment – Log-in mock-up

4.1.2.2.1 Import identified Assets

The following mock-up depicts the scope definition environment for the Cyber Risk Assessment Tool.

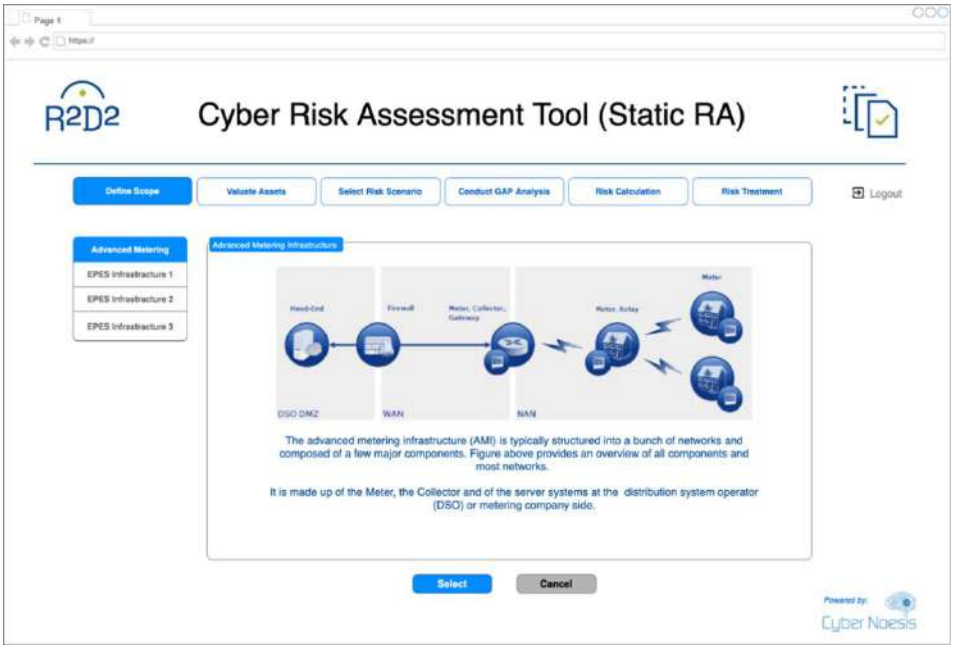


Figure 14. Cyber Risk Assessment – Scope Definition- mock-up

4.1.2.2.2 Define Asset Criticality

The following mock-up depicts the environment for the valuation of assets identified in the target environment.

Figure 15. Cyber Risk Assessment – Asset Valuation- mock-up

4.1.2.2.3 Select Risk Scenarios for TSO/DSO Infrastructure

The following mock-up depicts the environment for selecting cyber risk scenarios to be used for assessing the risk levels at the target environment.

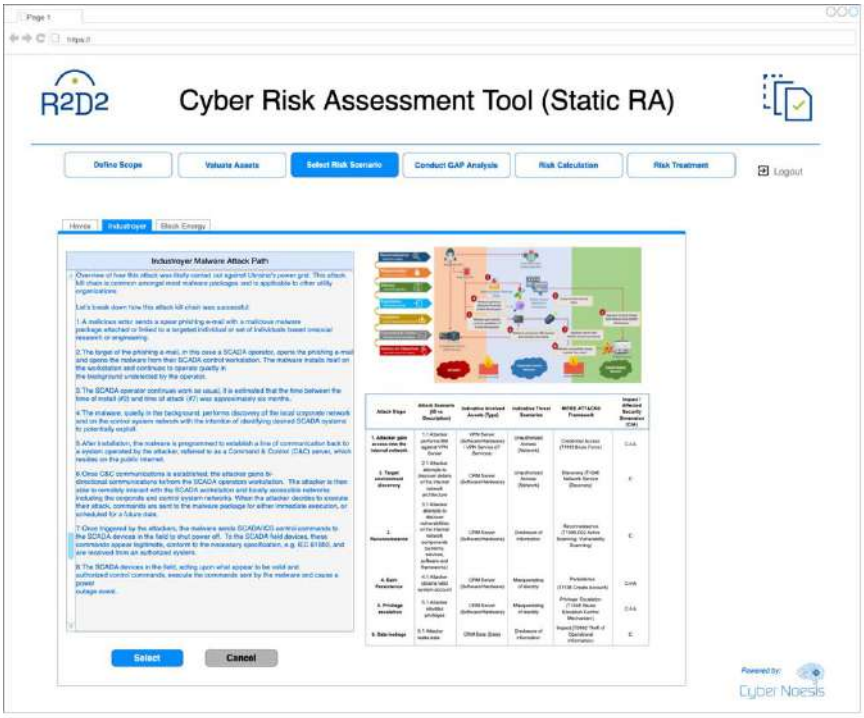


Figure 16. Cyber Risk Assessment – Scenario Selection- mock-up

4.1.2.2.4 Conduct GAP Analysis

The following mock-up depicts the way that the existing in the target environment controls are selected, including their maturity as a control's attribute.

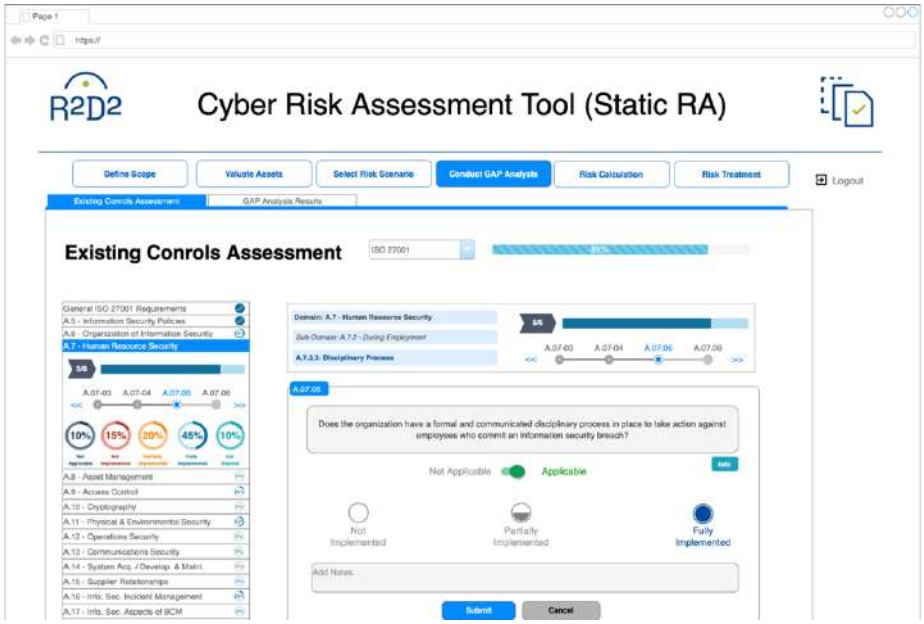


Figure 17. Cyber Risk Assessment – GAP Analysis / Assessment- mock-up

The following mock-up depicts the way that the results of the GAP Analysis are presented to user.

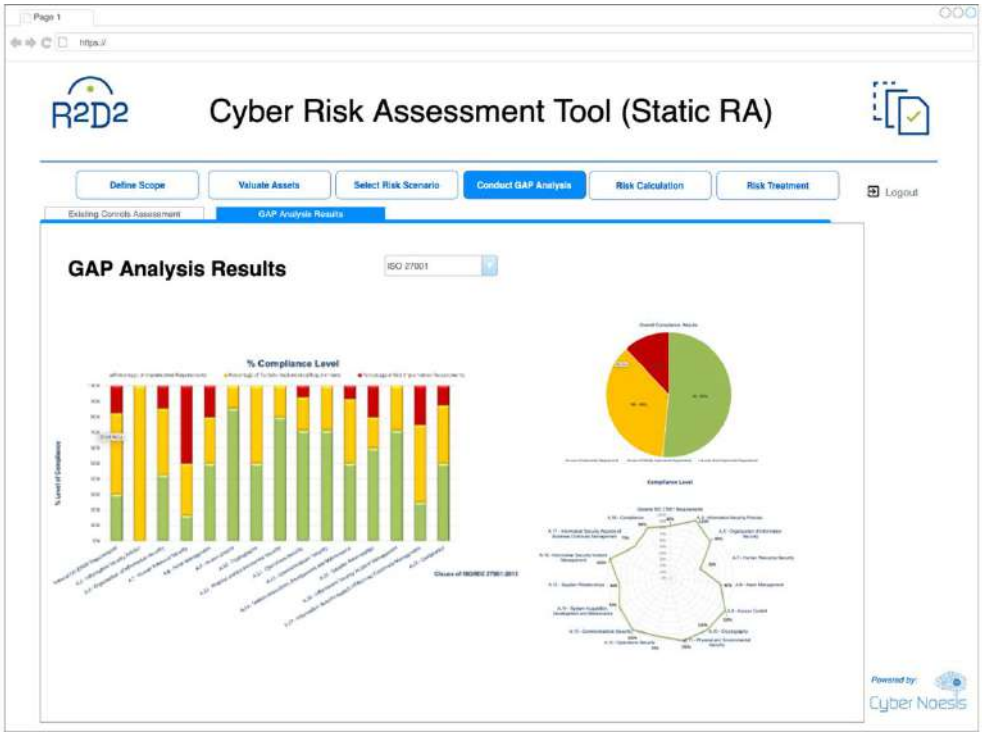


Figure 18. Cyber Risk Assessment – GAP Analysis / Results- mock-up

4.1.2.2.5 Risk Calculation & Reporting

The following mock-up depicts the way that the results of the cyber risk analysis are presented.

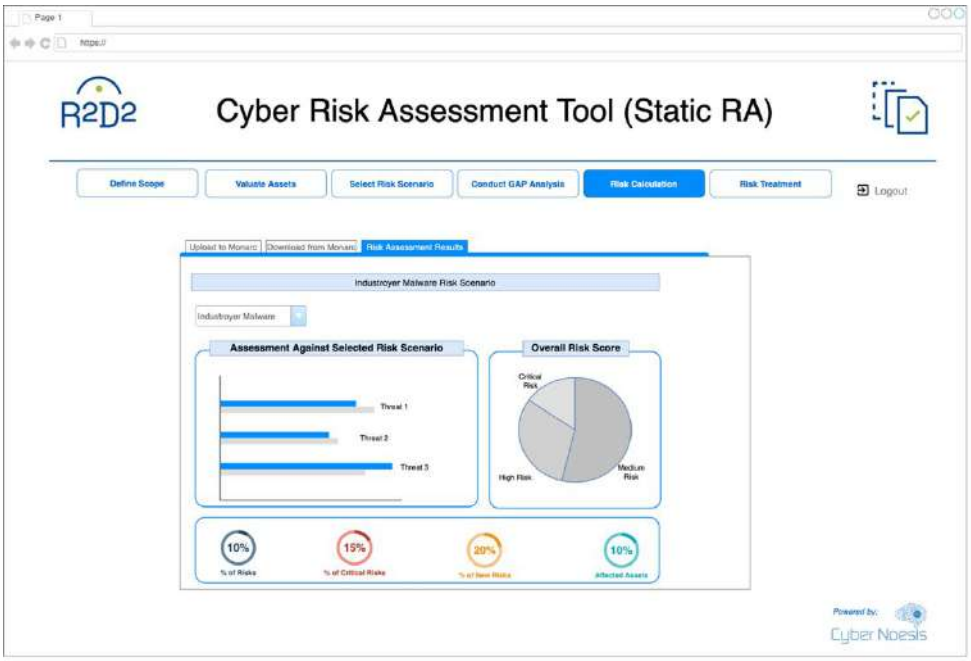


Figure 19. Cyber Risk Assessment – Risk Calculation- mock-up

4.1.2.2.6 Risk Treatment Plan

- Present Risk Treatment Plan

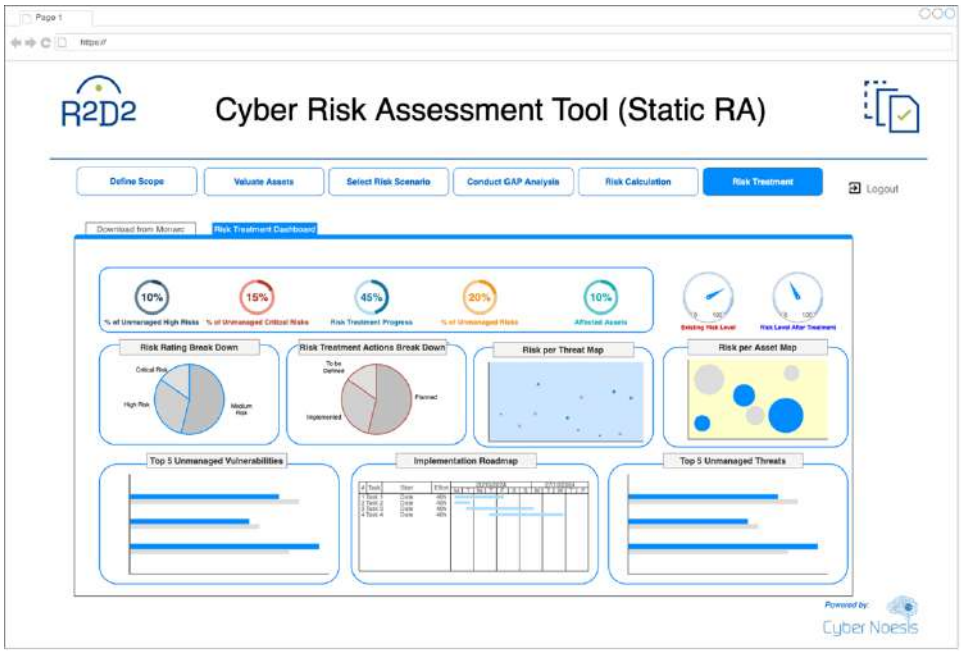


Figure 20. Cyber Risk Assessment – Risk Treatment- mock-up

4.1.3 Resources

The Dynamic Cyber Risk Assessment tool will utilize the following techniques, incorporating and deploying them.

- Deployment model

  The deployment model outlines the location for installing the solution, whether it's on physical server(s), virtual machine(s), or in a public cloud. The Cyber Risk Assessment tool can be deployed on Virtual Machine (VM). The components MySQL, web server and other development tools of the application can be installed on a Docker, running on the VM.

  While Docker excels in creating and managing containers or components, it doesn't scale effectively. Kubernetes provides a solution to address this scaling issue. Kubernetes possesses the capability to deploy containers across clusters and automatically replace containers that fail. Additionally, Kubernetes can offer load balancing, which is a valuable feature.

  Both Docker and Kubernetes will be installed on a VM hosted within CYBER's infrastructure. Furthermore, Docker will house the application server and the web server components.
- Operating System

  The operating system options include CentOS Linux 7.0 and Ubuntu Linux. CentOS may be favoured for its potential to deliver enhanced stability as an operating system.
- Web server

  The web server of choice is Apache HTTP Server 2.4.57.
- Database management system

  The Database Management System options consist of MySQL Community Server 8.0.34 or PostgreSQL.
- Development language

  Our development will primarily rely on Python and HTML5, some JavaScript code might be applied.
- Software Libraries

  Python Django and Bootstrap CSS will serve as the key software libraries in this project.
- Visualization.

  Tools like Kibana, Chart.js or D3.js can be used in order to visualize charts.

4.2 DYNAMIC CYBER-RISK STATUS EVALUATION (TASK 3.2)

4.2.1 Internal Architecture of the tool

4.2.1.1 Aim of the tool

The Dynamic Cyber-Risk Status Evaluation component will help in dynamic cyber threat detection and mitigation by providing a comprehensive solution that will involve asset tracking, cyber threat likelihood and vulnerability criticality evaluation for critical assets in the EPES environment. The asset inventory will provide a comprehensive up-to-date detailed list of all deployed network-connected assets, including Workstations, Servers, HMIs, Historians, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), IEDs and network devices. The Dynamic Cyber-Risk Status Evaluation Tool will be able to collect information from well-known technical Vulnerability Assessment tools (e.g. Nessus, OpenVAS) and well-established vulnerabilities databases (e.g. NIST NVD) using the "Cyber Threat Intelligence" tool (T3.6)", as well as cyber threat likelihood assessments from the "Deep learning data analytics for security" tool (T5.4) to generate risk scoring for critical assets along with mitigation suggestions. The aim is to develop a tool which will be able to dynamically maintain a logical model of IT/OT infrastructure, existing assets, security controls in place, existing vulnerabilities, risk scoring, as well as risk treatment plans based on realistic scenarios.

The Dynamic Cyber-Risk Status Evaluation component is set to furnish our system with dynamic and (near) real-time risk assessment capabilities. It will make use of data provided by a variety of sources, which encompass other R^2D^2 components. Through analysis and correlation with the help of "Deep Learning data analytics for security" tool (T5.4), it will enable the perpetual detection of threats. This dataset will undergo further enhancement through the incorporation of Cyber Threat Intelligence (CTI) knowledge, thereby imbuing our model with not only reactive, but also proactive, capabilities. This proactive facet within our Dynamic Cyber-Risk Evaluation component will equip our model with the capability to pre-emptively mitigate threats that are directed towards the EPES architecture in (near) real-time, even before they materialize within our system.

4.2.1.2 Detailed Architecture

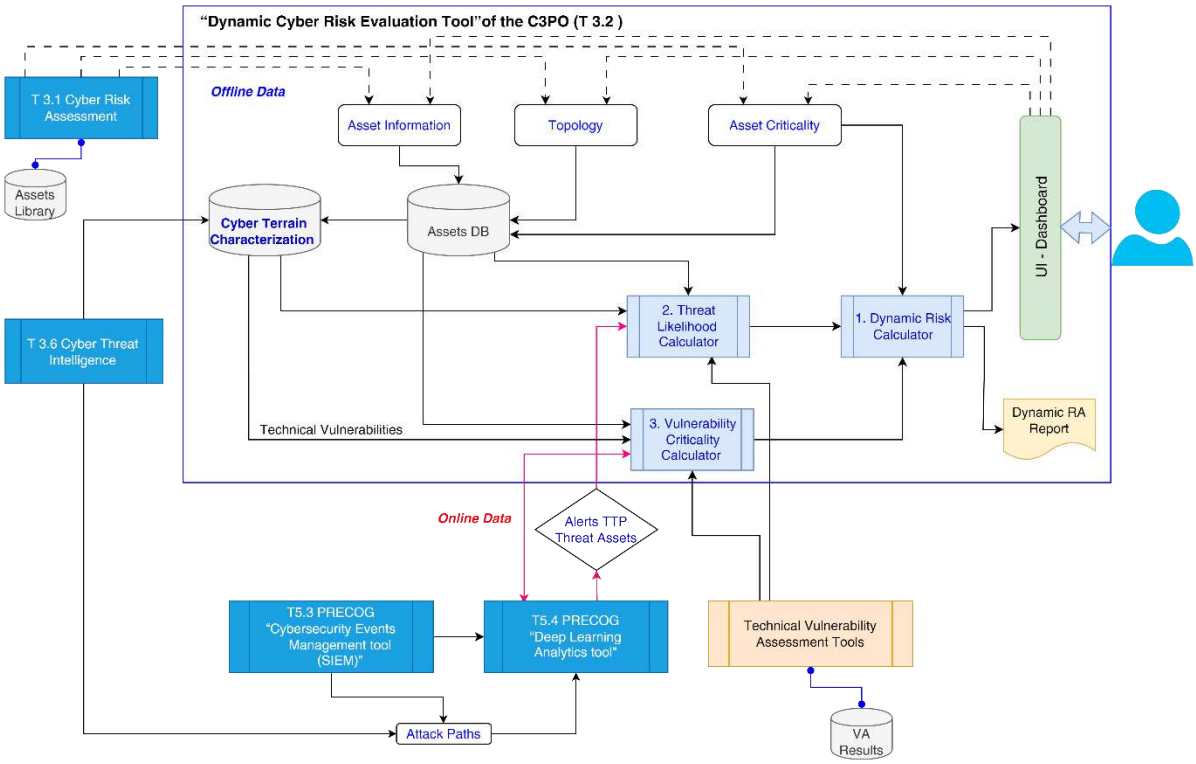


Figure 21. The Dynamic Risk Evaluation Tool and its interfaces with other R2D2 and external components

The Dynamic Risk Evaluation Status Evaluation component comprises the components that are used for managing information about the target environment (Asset information, Topology, Asset criticality, Cyber Terrain characterisation), key components used for dynamically assessing risks (Threat Likelihood calculator, Vulnerability criticality calculator, Dynamic Risk Calculator), the UI and Dashboard, and other R^2D^2 and third-party components that contribute to the tool's functionality.

4.2.1.2.1 Target environment

It comprises the following components:

- **Asset information**: this component is used for managing information about assets and existing controls of the target environment, provided by the user through the UI-Dashboard component. Other methods that will be used for the collection of asset information include excel/csv files. The collected information is stored on the tool's Assets Database.
- **Topology**: this component is used for managing information about the topology of assets at the target environment, also collected through the UI-Dashboard component. and stored on the tool's Assets Database. In addition, it contains relative information about security controls in place and how these are connected to assets.
- **Asset criticality**: this component is used for assessing the criticality of the managed assets, based on energy sector-oriented impact scales. The collected information is stored on the tool's Assets Database.

- **Assets Database (DB)**: this database is used for storing and collectively managing information about the target environment.
- **Cyber Terrain Characterisation**: this component is used for correlating the information about the target environment with the information provided by the CTI Tool, to filter CTIs and use only the ones that are applicable to the target environment.

4.2.1.2.2 Dynamic risk assessment

It comprises the following components:

- **Threat Likelihood calculator**: this component is used to dynamically assess the likelihood of threats considering security incidents reported by the R²D² T5.3 PRECOG SIEM, the CTI and the target environment, assessed by the R²D² T5.4 PRECOG Deep Learning Analytics Tool.
- **Vulnerability criticality calculator**: this component evaluates the criticality of a vulnerability found in the target environment by the VA Tool, but also of newly published vulnerabilities, communicated by the CTI tool, that are related to the assets of the target environment, considering the target environment's characteristics, like assets, their topology, but also existing controls,
- **Dynamic Risk Calculator**: this component calculates the risks associated with newly identified threats and/or vulnerabilities, considering the threat likelihood and/or the vulnerability criticality provided by the corresponding components, but also the associated assets' impacts to the target environment. The T5.3 PRECOG SIEM, is the CARMEN tool, provided by S2 Grupo, a Security Information and Event Management (SIEM) tool enhanced with data acquisition and aggregation, as well as with threat detection and threat modelling capabilities within the scope of tasks T5.3 and T5.4 of the project.

4.2.1.2.3 UI and Dashboards

It is the component responsible for receiving information about the target environment but also for providing the user the results of the dynamic risk assessment and situational awareness about the target environment, including risk levels and applicable threats.

4.2.1.2.4 Other R²D² and third-party components

It comprises the following components:

- Technical Vulnerability Assessment (VA) Tool: this component is used for identifying existing vulnerabilities in the target environment.
- R²D² T5.3 PRECOG SIEM: this component is used for identifying and reporting malicious activities in the target environment.
- R²D² T5.4 PRECOG Deep Learning Analytics Tool: this component is used for evaluating potential follow-up malicious activities, considering the identified by the R²D² T5.3 PRECOG SIEM reported incidents, the target environment, and the CTI provided by the R²D² T3.6 Cyber Threat Intelligence tool.

- R²D² T3.6 Cyber Threat Intelligence; this tool is used for managing Cyber Threat Intelligence from external sources but also, for sharing malicious activities found in the target environment, with the community.

4.2.1.3 Description of Components

In this section we provide a detailed description of the components, their functionality and interfaces.

4.2.1.3.1 Target environment

Asset Information

The asset information component is an integral part of the Assets DB system. Its primary purpose is to manage crucial information pertaining to assets within the target environment including deployed security controls. This component handles the identification of assets by maintaining a proper categorisation of assets found in an EPES environments and by utilizing their corresponding CVE identifier. Additionally, it encompasses the recording of implemented security controls and other pertinent asset-specific details.

Considering that numerous assets within the EPES environment might lack CVE identifiers, the use of a vulnerability scanner becomes essential for conducting the initial vulnerability assessment across all assets in the environment. The asset information component stores this information in Excel or CSV files, and then stored on the asset database.

Through the effective management of asset information, the system ensures comprehensive documentation and evaluation of assets and security controls/policies.

Topology

The asset topology component plays a critical role in storing vital information pertaining to the asset topology within the target environment, specifically within the EPES environment. This component is responsible for mapping and documenting the dependencies among assets in the target environment, ensuring that crucial functions and interconnections among assets are accurately recorded. The information regarding the asset topology can be derived from network monitoring tools, enabling a comprehensive view of the system. In addition, this component takes into consideration the security controls in place and how these are connected to, or contribute to the protection of cyber or cyber-physical assets. This process results to the establishment of an association between each asset and its corresponding control(s), if any, thereby formulating a tailored approach specific to the system.

By incorporating the asset topology component, we ensure that the evaluation of risk encompasses the entire system rather than focusing solely on the isolated risks associated with individual assets. This approach enables a holistic understanding of the system's vulnerabilities and potential impact on overall system security while also considering the security mechanisms in place. Consequently, the asset topology component serves as an integral part of the Assets database component, facilitating a comprehensive and interconnected view of the asset landscape within the EPES environment.

Asset Criticality

The asset criticality evaluation component, an integral part of the Asset Database component, is specifically designed for assessing the criticality of assets within the EPES environment. This evaluation is carried out based on impact scales that are tailored to the energy sector. By utilizing these energy sector-oriented impact scales, the component ensures accurate assessment of highly valuable energy assets, both cyber and cyber-physical, and their corresponding impact. Through this process, we guarantee that the most crucial energy-related assets are evaluated and prioritized accordingly, contributing to a comprehensive understanding of asset criticality within the EPES environment.

Assets Database

The central assets repository consists of several components, namely the asset information component, topology component, asset criticality component, and Cyber Terrain Characterization component. These components collectively contribute to the asset database, which serves as a central repository for managing assets within the EPES infrastructure. The asset database effectively correlates and stores information from these components, facilitating comprehensive asset management.

The information contained within the asset database is utilized by both the T3.1 Cyber Risk Assessment component and the T3.2 Cyber Risk Status Evaluation component. This information plays a crucial role in these components, as it serves as input for generating the expected risk-related outputs. The integration of asset information, topology data, asset criticality assessments, and Cyber Terrain Characterization within the asset database ensures a holistic and informed approach to asset management and risk evaluation within the EPES infrastructure.

Cyber Terrain Characterization

The characterization of the cyber terrain [8] depends on the strategic objective determined in the planning phase. This is why the achievement of this objective is done through a kill chain model. These phases are carried out on specific assets. The objective of cyber terrain characterisation is to provide the dimension of where an attacker's actions take place.

This cyber terrain characterization will rely on a database in where the different types of threats are stored, together with their associated Tactics, Techniques and Procedures (TTPs). This data will be correlated with asset information, so that each asset will be assigned a type of terrain.

Each generated, by the PRECOG SIEM, alert will be assigned to an actor and a TTP. Information on each generated alert will be correlated with the database and, as a result, each alert will be assigned to a kill chain phase, providing a dynamic assessment of the state of threats. The organisation's assets will be modelled based on the classification of terrain according to the cyberspace-based OCOKA model (key terrain, observation and firing terrain, concealment terrain and approach path terrain). Based on the information provided by Course of Actions (COAs), it will be possible to determine which type of asset will be in each phase and therefore, which type of asset is more likely to be attacked by that tactic.

[8] The Cyber Terrain is defined as “the systems, devices, protocols, data, software, processes, cyber personas, and other networked entities that comprise, supervise, and control cyberspace” (https://ccdcoe.org/uploads/2018/10/d2r1s8_raymondcross.pdf)

Cyber terrain can be represented in every plane of cyberspace. The two planes that apply in this section are the physical plane and the logical plane.

- On the one hand, the physical plane corresponds to the physical layer of the OSI (Open Systems Interconnection) model and encompasses all the tangible components of a computer system, as well as the interconnected hardware. This level includes all physical devices, such as computers, servers, routers, switches and other network devices.
- On the other hand, the logical plane is composed of the software and the configuration that governs the behaviour of each of the elements present in the physical plane. This category includes the operating system that runs on each device, the software that runs on them and all of the configurations and settings that determine their operation.

To properly characterize these planes of cyber terrain, a system known as Common Platform Enumeration (CPE), which assigns a unique name to each system, platform and software present in cyberspace, is used. These identifiers facilitate the management and classification of the different elements present in cyberspace, which is essential for maintaining a clear picture of its infrastructure and configuration. After this identifier assignment, each element will be related to their respective CVSS to calculate the criticality of the vulnerability.

4.2.1.3.2 Dynamic risk assessment

Threat Likelihood Calculator

This module analyses potential threats detected by CARMEN analysers and measures the similarity of these potential threats to already known APTs, attending to both tactical and operational intelligence. This analysis is carried out combining different ML algorithms.

As explained, the threat intelligence basis on which similarity will be calculated can belong to two different types:

- Tactical Intelligence: This type of threat intelligence is related to atomic and behavioural Indicators of Compromise (IoCs). These atomic indicators will be obtained from external sources, such as MISP (https://www.misp-project.org/).
- Operational Intelligence: This type of intelligence is extracted from the high-level description of the TTPs.

Both types of intelligence are normalized and mapped to an n-dimensional space, so that data is comparable and suitable to be used for training a ML algorithm. Combining different normalization and ML algorithms, this intelligence is clustered and different groups of APTs are generated.

After that, when a potential threat is detected by CARMEN, it is normalized and mapped to the above-mentioned n-dimensional space and, as a result, it is possible to identify to which already known APTs is that activity similar.

Results of the similarity analysis, along with the threat likelihood, will include the following information:

- Percentage of resemblance
- Linked APT group

- TTP

Threat Likelihood Calculator

The Vulnerability Criticality Calculator component plays a pivotal role in dynamically evaluating vulnerabilities within the EPES environment, utilizing data from various sources. These data originate from the Asset Database component, the Cyber Threat Intelligence tool (vulnerabilities databases), the Cyber Terrain Characterization Component, and the Technical Vulnerability Analysis tool. By leveraging these inputs and` employing dynamic vulnerability assessment, the Vulnerability Calculator Component contributes to the comprehensive and real-time evaluation of vulnerabilities, enhancing the overall security of the EPES infrastructure.

In addition, the Vulnerability Criticality Calculator component establishes continuous communication with the Deep Learning Analytics tool to effectively analyze the provided data using advanced deep learning techniques. The Cyber Terrain Characterization will provide the vulnerability criticality calculator information relating the target environment assets with those involved in the killchain of different APT groups in order to allow the identification of assets that might be in the attack path. Furthermore, the Cyber Terrain Characterization will furnish dynamic criticality calculator values (CVSS – Common Vulnerability Scoring System) pertaining to the assets within the EPES environment.

The output generated by the Vulnerability Criticality Calculator component serves as input to the Dynamic Risk Calculator, enabling the latter to deliver real-time estimations about the risk levels in the target EPES environment. This integration ensures that the risk assessment process remains dynamic and up-to-date, enhancing the accuracy and timeliness of risk evaluations for the EPES infrastructure.

Dynamic Risk Calculator

The Dynamic Risk Calculator component fulfils the critical role of delivering continuous, close to real-time, assessments pertaining to the current risk status within the EPES environment. To accomplish this, the component relies on input data derived from the Threat Likelihood Calculator, Vulnerability Criticality Calculator, and Asset Criticality components. In addition, the dynamic risk calculation will involve interpreting the kill chain of each actor and assessing the outputs of the Machine Learning engines. Each of the inputs will be associated with the killchain of the actor in question, then correlated with the cyber-terrain information. With this correlation, a drawing of the organization's assets will be obtained, showing the different attack paths that an APT group could follow By integrating this information, the Dynamic Risk Calculator estimates the current risk level effectively. The output of this component is then utilized in the UI-Dashboard, providing users with valuable real-time information concerning the status of risk. This information will encompass details related to the kill chain, including APT group involvement, the percentage of attack evolution, assets engaged in this kill chain, probabilities associated with the next asset in the kill chain, as well as the likelihood of kill chain interruption and remediation. Moreover, the component produces analytical reports that provide in-depth information concerning the ongoing risk assessment. and comprehensive insights to stakeholders.

The dynamic risk calculation will be carried out by interpreting the killchain of each actor and evaluating the outputs of the Machine Learning engines. Each of the inputs will be associated to the killchain and, consequently, its evolution within the cyber-terrain will be compared.

The assets involved will allow the association with the cyber-terrain, drawing the possible lines of succession in the evolution of the attack of the same APT group.

The output of the engine will be as follows:

- Killchain
- APT group
- Percentage of evolution
- Assets involved in the killchain
- Probability of next asset in the killchain
- Possibility of killchain blocking and remediation

4.2.1.4 Techniques & Algorithms

The techniques and algorithms that will be described here will be about the three main components of the Dynamic Cyber-Risk Status Evaluation component.

4.2.1.4.1 Threat Likelihood Calculator

In order for the different ML algorithms to operate on the discussed threat information, there will be a microservice in charge of applying various natural language processing (**NLP**) techniques that convert the text of their descriptions into numeric variables. NLP techniques focus on transforming natural language into a formal, programming-like language that computers can process. Several NLP algorithms will be considered for this preprocessing, such as Word2vect, Bag-of-words or Tfidf (Term frequency – Inverse document frequency), until the one that gives the best results is found.

Once the numerical characterisation of the threats is done, the clustering microservice groups them by similarities and common patterns. It will use the Birch algorithm which, through its "threshold" parameter, allows to be more or less demanding in clustering. The initial calibration of the algorithm parameters for testing will be fine-tuned through several iterations with the security team, but these parameters can be reconfigured to better suit each working dataset. All this process will take place offline, storing the clustering models for the next microservice.

The last microservice is in charge of providing the Threat Likelihood. To achieve this, it starts from the threat clustering provided by the Birch model, against which it compares the information collected from the different sources in real time. In fact, this microservice calculates the distance of the analysed observation to each known group and generates an alert hypothesis when it is too close to any of the malicious groups.

The cosine distance is the metric of choice for measuring the similarity between points in the vector space. It is particularly useful when dealing with high-dimensional data and is commonly employed in various fields such as information retrieval, natural language processing, and recommendation systems. The similarity is determined by the cosine of the angle between the two analysed vectors; the closer the cosine value is to 1, the more similar the vectors are, and the closer it is to -1, the more dissimilar they are.

4.2.1.4.2 Vulnerability Criticality Calculator

The Vulnerability Criticality Calculator serves as a dynamic and real-time vulnerability analysis tool, employing cutting-edge techniques for EPES environments. This component processes vulnerability-related information from diverse sources, utilizing ML techniques for correlation. Subsequently, the calculator receives CVSS scores as input, which are associated with the CPE of assets from Cyber Terrain Characterization. In this process, each asset will be represented by one or more vulnerability values, provided that the asset possesses vulnerabilities.

Moving forward, deployed security mechanisms are taken into consideration in the vulnerability valuation process. After representing each vulnerability to a numeric value using CVSS, adjustments are made based on the effectiveness of the deployed security mechanisms in mitigating the identified vulnerabilities. In addition, because CVSS scoring mechanism is not tailored to the specific EPES environment, additional CVSS factors, and in particular, environmental metrics group will be re-assessed to depict the specific needs of IT/OT infrastructure. The final step of this process requires adjustments to convert the vulnerability-related information into acceptable numerical values, which are vital for the subsequent phases of analysis.

Drawing from the vulnerability-related data, the asset topology and information related to the killchain that identifies which assets are going to be affected by specific attacks, the Vulnerability Criticality component generates a comprehensive map of potential exploitations, illustrating the interconnections among the detected vulnerabilities. This map portrays how an attacker could exploit one vulnerability after exploiting another in a different asset. These paths of exploitation are established using appropriate algorithms for creating attack paths or through the adoption of attack tree methodologies. The primary objective is to identify the most efficient algorithm for detecting and analyzing all conceivable attack paths within the EPES infrastructure.

Once the attack paths are constructed, and each detected vulnerability is appropriately represented by numerical values, the model advances to the next step, which most likely will be based on Fuzzy Cognitive Maps (FCM).

In this approach, the attack paths are converted into an FCM, where each node represents a vulnerability, and each edge symbolizes the associated numerical value. After a specified number of iterations, our system achieves balance and, based on the result, vulnerability values are recalculated. This technique provides invaluable insights into how an attacker could potentially impact a vulnerability at the end of an attack path, often corresponding to a crucial OT asset.

Moreover, this approach aids in estimating the vulnerabilities of OT assets, even in scenarios where limited vulnerability-related information is available. By estimating the connections and vulnerabilities of each asset, the model offers an overall vulnerability estimation for each asset, contributing to an encompassing evaluation of the entire system's security status.

While FCM are recommended, alternative approaches will also be considered to achieve similar outcomes. This integrated approach equips our model with a dynamic and comprehensive understanding of EPES infrastructure vulnerabilities.

4.2.1.4.3 Dynamic Risk Calculator

Research is being conducted for the most appropriate methodology to calculate risks considering the factors such as threat likelihood, vulnerability value, and asset criticality as

provided by the respective components. One methodology currently under consideration for adoption will be based on a widely recognized and publicly accepted mathematical formula used for calculating risk status, as denoted by:

$$R = V * I * T$$

where:

R represents the overall risk level,

V stands for vulnerability criticality,

I signifies the impact, and

T denotes the threat likelihood.

This formula forms the basis of risk assessment and management methodologies, enabling the determination of the level of risk associated with a system, asset, or environment. Conversely, alternative methodologies are also being evaluated to determine the most appropriate approach for addressing the unique and diverse operational environment in which EPES operates.

What sets this component apart is its innovative approach, incorporating dynamic and real-time values that are continually adjusted to the specific context of the EPES environment, particularly regarding vulnerability and threat factors. By employing real-time data and adapting to the changing nature of the EPES environment, the Dynamic Risk Calculator component enhances the accuracy and relevance of risk assessments.

4.2.1.5 Data Exchanges & Interfaces

The Dynamic Cyber Risk Status Evaluation component will provide the following data exchanges and interfaces internally and externally, with other R^2D^2 and third-party components:

- Tactical Intelligence: Retrieval of Atomic and Behavioral Indicators from MISP (HTTPS/443)
- Operational Intelligence: Get entries from MISP (HTTPS/443)
- Risk Calculator: Sending records from ML engine to Dynamic Risk Calculator (HTTPS/9200)
- Collector: Retrieval of log records from the ML module to CARMEN (HTTPS/443).
- The Vulnerability Criticality Calculator: receives data from the Cyber Terrain Characterization, the Assets DB, the Technical Vulnerability Assessment Tool and sends data to the Dynamic Risk Calculator. In addition, it exchanges data with T.5.4 (Deep Learning Analytics Tool).
- Dynamic Risk Calculator: receives data from Vulnerability Criticality Calculator, Threat Likelihood, Asset Criticality, and send data to UI – Dashboard (HTTPS/443) and Dynamic RA Report (HTTPS/443).

4.2.2 User Interface

In this section we provide preliminary mock up, dashboards, and charts for the Dynamic Cyber-Risk Status Evaluation Tool.

4.2.2.1 User Log in Topology

The following mock-up depicts the Dynamic Cyber-Risk Status Evaluation Tool log-in page.

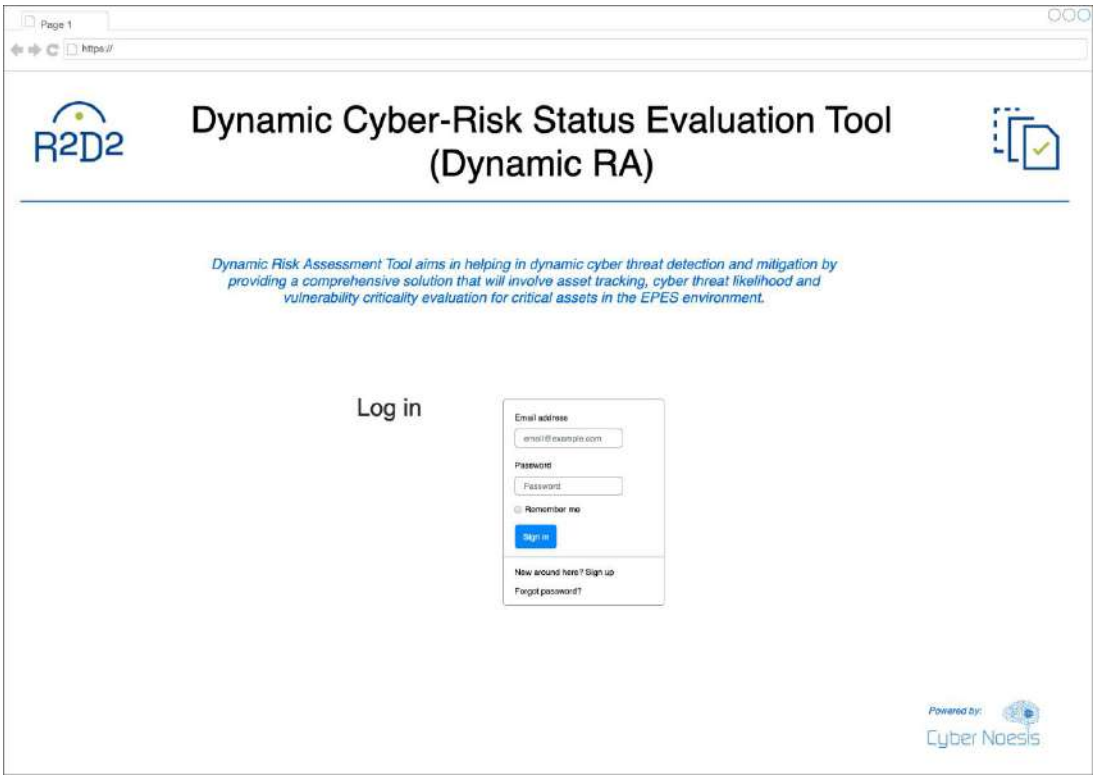


Figure 22. Dynamic Cyber-Risk Status Evaluation – Log-in mock-up

4.2.2.2 Network Topology

The following mock-up depicts the way that topology of the target environment will be displayed to the user.

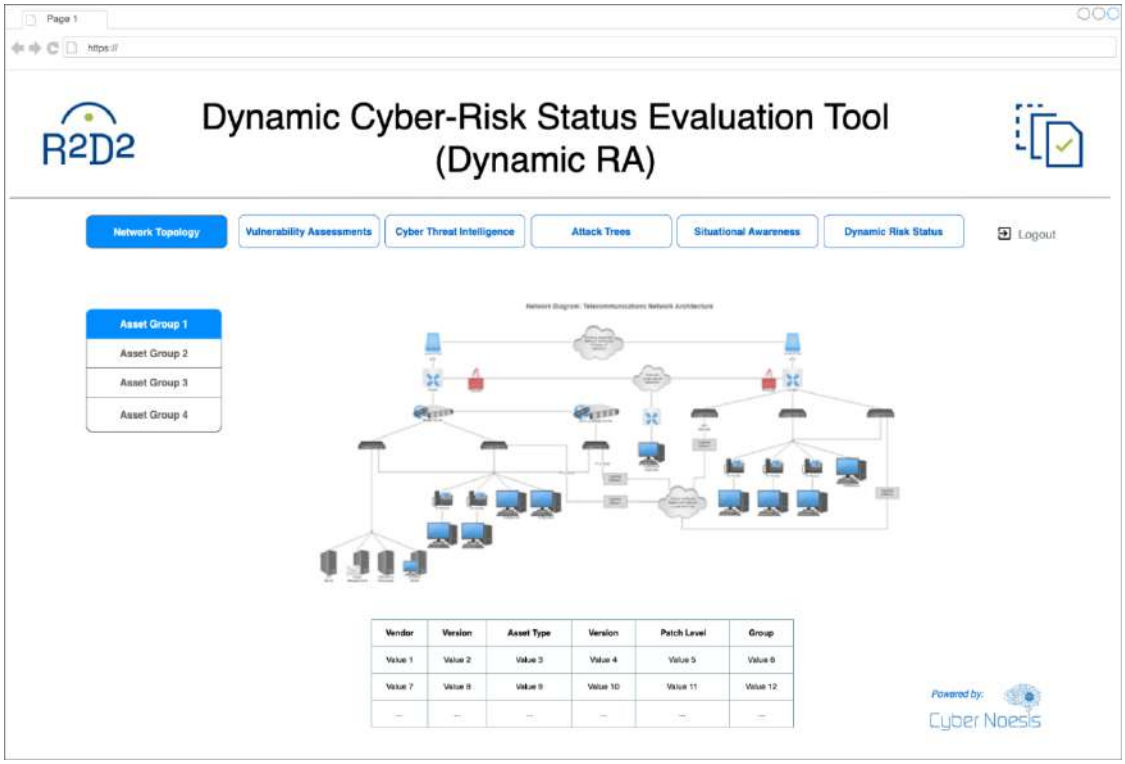


Figure 23. Dynamic Cyber-Risk Status Evaluation – Network topology mock-up

4.2.2.3 Vulnerability Assessments

The following mock-up depicts the way that the output of the vulnerability assessment for the target environment will be displayed to the user.

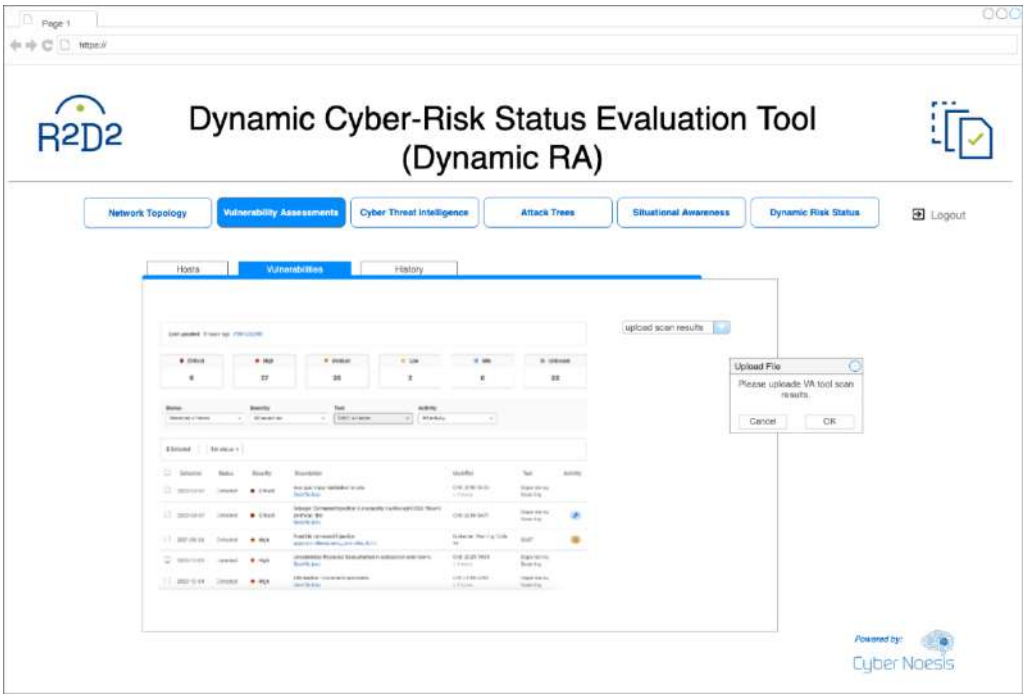


Figure 24. Dynamic Cyber-Risk Status Evaluation – Vulnerabilities reported for the target environment

4.2.2.4 Cyber Treat Intelligence

The following mock-up depicts the way that cyber threat intelligence related to the target environment will be displayed to the user.

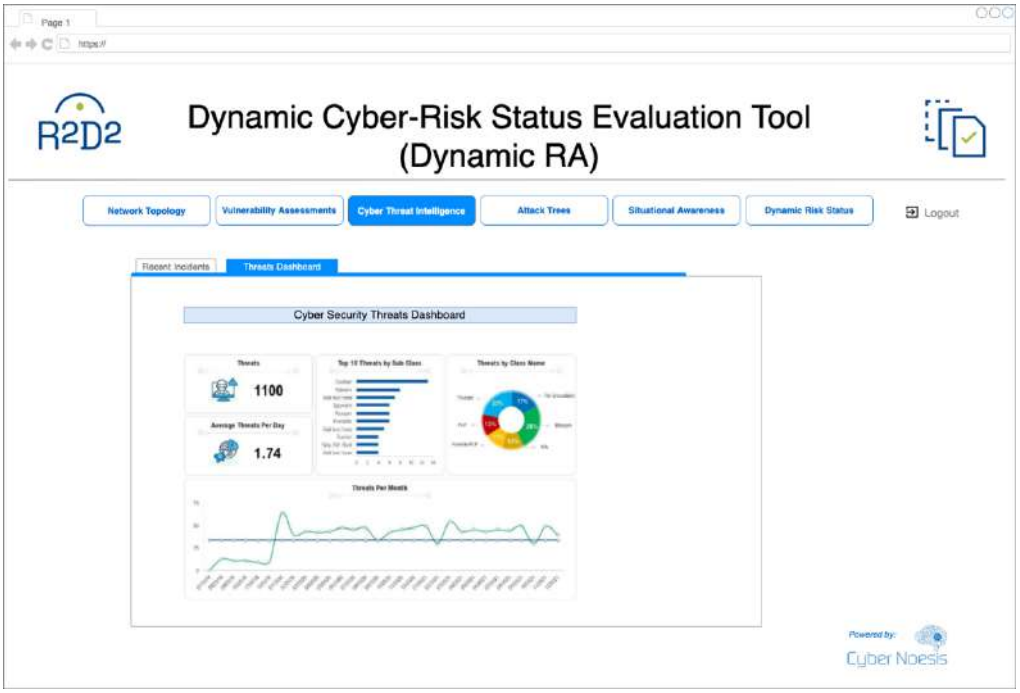


Figure 25. Dynamic Cyber-Risk Status Evaluation – Cyber Threat Intelligence related to the target environment.

4.2.2.5 Attack Trees

The following mock-up depicts the way that formulated attack trees/graphs used for the dynamic calculation of risks for the target environment, will be displayed to the user.

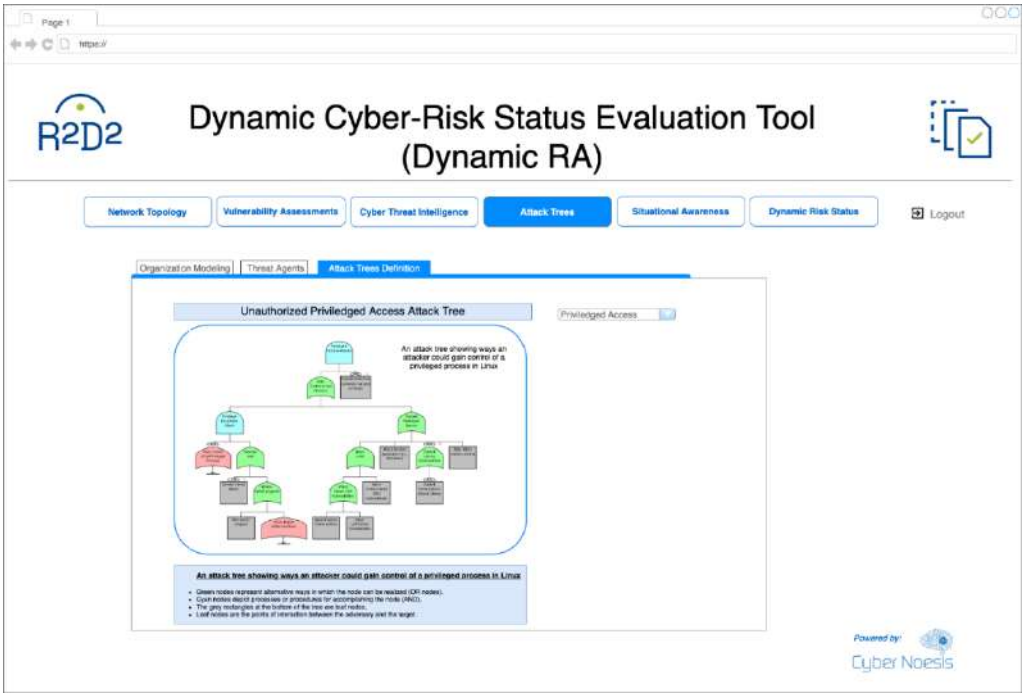


Figure 26. Dynamic Cyber-Risk Status Evaluation – Cyber Threat Intelligence related to the target environment

4.2.2.6 Situational Awareness

The following mock-up depicts the way that information about recalculated vulnerabilities identified on the target environment, based on the vulnerability criticality calculator analysis, will be displayed to the user.

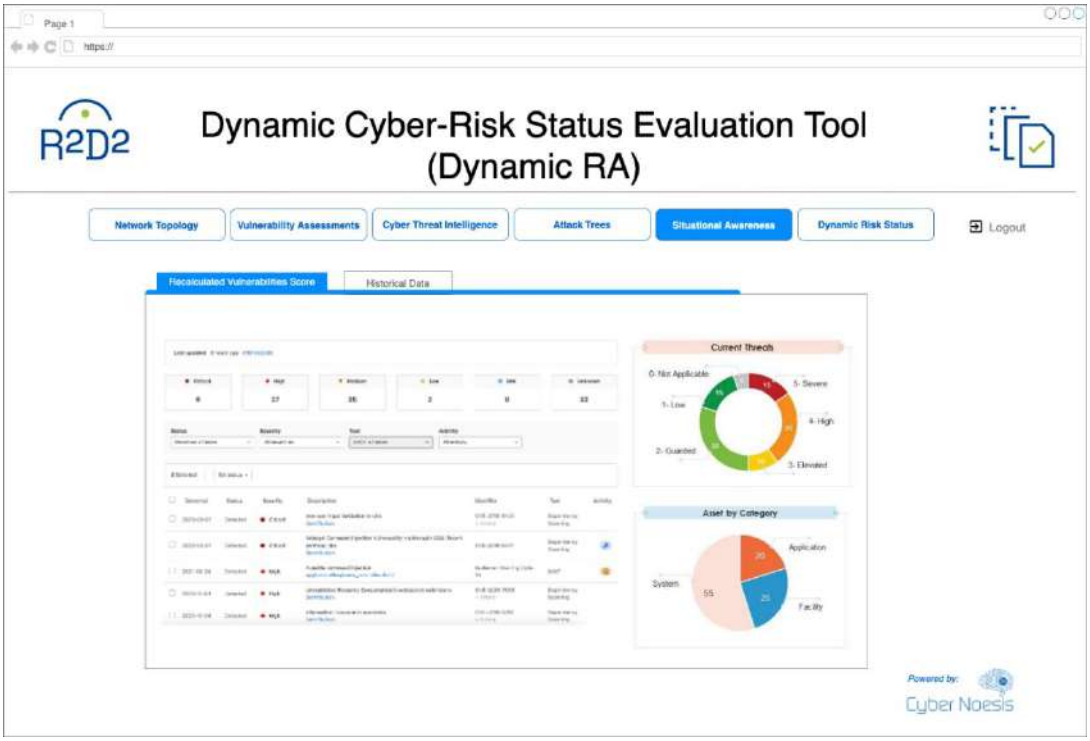


Figure 27. Dynamic Cyber-Risk Status Evaluation – Situational awareness

4.2.2.7 Dynamic Risk Status

The following mock-up depicts the way that the results of the dynamic risk status evaluation activities, will be displayed to the user, including:

- Phase of the Killchain
- APT group(s) involved
- Percentage of evolution
- Assets involved in the Killchain

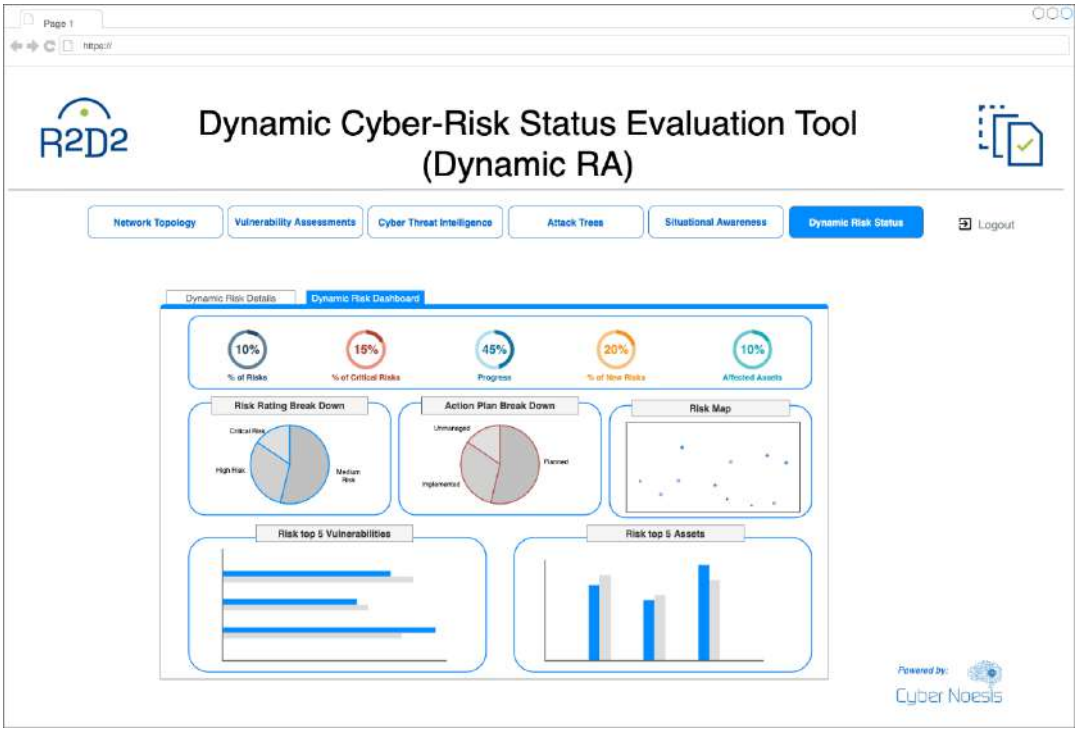


Figure 28. Dynamic Cyber-Risk Status Evaluation – Situational awareness

4.2.3 Resources

The Dynamic Cyber-Risk Status Evaluation utilizing the following techniques, the tool will employ them.

- Deployment model

  The deployment model outlines the location for installing the solution, whether it's on physical server(s), virtual machine(s), or in a public cloud. The Dynamic Cyber-Risk Status Evaluation tool can be deployed on VM. The components MySQL, web server and other development tools of the application can be installed on a Docker, running on the VM.

  While Docker excels in creating and managing containers or components, it doesn't scale effectively. Kubernetes provides a solution to address this scaling issue. Kubernetes possesses the capability to deploy containers across clusters and automatically replace containers that fail. Additionally, Kubernetes can offer load balancing, which is a valuable feature.

  Both Docker and Kubernetes will be installed on a VM hosted within CYBER's infrastructure. Furthermore, Docker will house the application server and the web server components.

- Operating System

  The operating system options include CentOS Linux 7.0 and Ubuntu Linux. CentOS may be favored for its potential to deliver enhanced stability as an operating system.

- Web server

The web server of choice is Apache HTTP Server 2.4.57.

- Database management system

  The Database Management System options consist of MySQL Community Server 8.0.34 or PostgreSQL.

- Development language

  Our development will primarily rely on Python and HTML5, some JavaScript code might be applied.

- Software Libraries

  Python Django and Bootstrap CSS will serve as the key software libraries in this project.

- Visualization.

  Tools like Kibana, Chart.js or D3.js can be used in order to visualize charts.

4.3 SPATIAL AND TEMPORAL MODELLING AND QUANTIFICATION OF CASCADING PHYSICAL EVENTS (TASK 3.3)

4.3.1 Event Spatial and Temporal Modelling

Fig. 29 displays the plan we developed in this project to examine how the network responds to a natural disaster. The plan consists of three parts. Initially, we manage the input data. Following that, we create a simulation of the disaster event. Lastly, we evaluate the impact on the network to understand the condition of its various connections. The details of each part are discussed in the following subsections.

4.3.1.1 Input Data

The first stage of the proposed framework initializes the simulation process by preparing the required input data which includes network data, fragility curve, and historical event data.

4.3.1.1.1 Network Data

The network data mainly includes the following:

- Substation data
  - Active and reactive power demand connected (MW & MVAr).
  - Time-based demand profiles of the active and reactive power demand.
  - Voltage level of the substation and its permissible limits.
  - Parameters of shunt elements connected (if any).
  - Substation coordinates (if available; if not, a virtual geographical coordinate will be generated for any location of interest).
- Lines and transformer data
  - To and from nodes of each line or transformer.

  - Electrical parameters include resistance, reactance, and line charging susceptance (if any) of each line or transformer.
  - MVA ratings.
  - Status of each line or transformer.
- Generator data
  - Location of the generator (i.e., to which bus it is connected)
  - Active and reactive power limits
  - Voltage magnitude
  - MVA base
  - Status of the generator
  - Marginal costs of each generator

The above-mentioned network data are either converted into MATPOWER test case format or PyPower test case format that is given as an input file to the model.

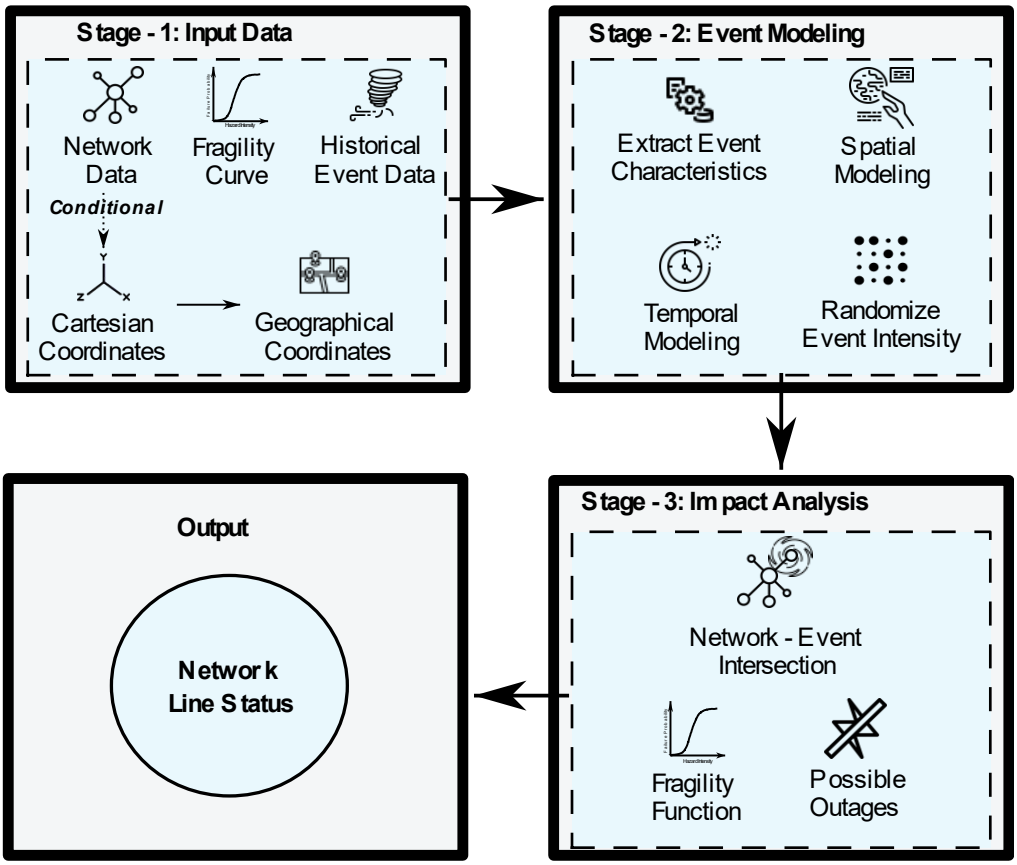


Figure 29. Proposed Fragility Modelling Framework

4.3.1.1.2 Fragility Curve

Fragility curves, broadly employed in resilience research, serve to define the probability of malfunction for power system infrastructures. These fragility curves can be derived: (i) using statistical models built from an extensive failure record database, (ii) using the empirical or simulation-driven characterization of specific equipment subjected to a series of disturbances with various intensities, (iii) using expert's judgment, and (iv) through a combination of these methods. The conclusions from experts could be highly uncertain as

there might be very few experiences to gather. Empirical curves for distribution network lines can be derived from the failure records. However, specifically deriving the wind-related failure of distribution lines from the database is quite challenging. Therefore, this project utilizes the wind fragility curve shown in Fig. 30 which is a result of the Resilient Electricity Networks for Great Britain (RESNET) project led by The University of Manchester [87]. The wind fragility curve shown in Fig. 30 is mathematically expressed as follows:

$$P_L^{hw}(w) = \int_0^w \frac{1}{x\sigma\sqrt{2\pi}} e^{-\frac{(\ln x-\mu)^2}{2\sigma^2}} dx$$

where, w is the wind gust speed, σ and μ represent the standard deviation and expectation for the underlying logarithmic normal distribution.

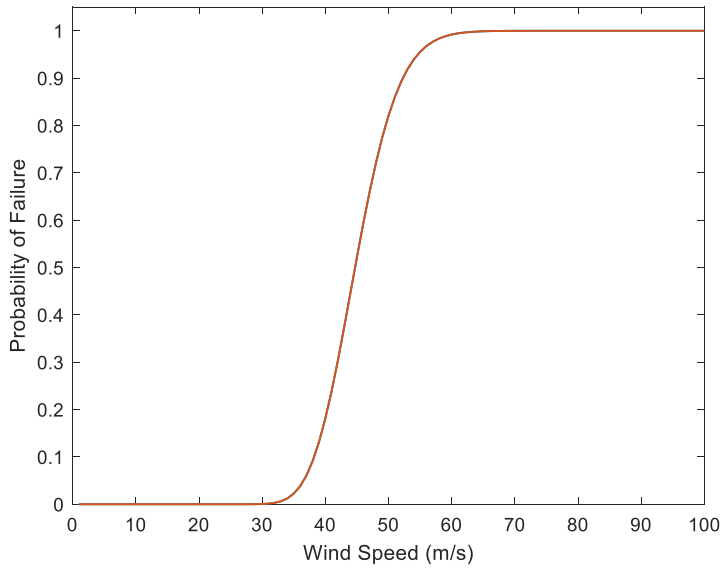


Figure 30. Fragility Curve for Overhead Lines

The wind-dependent failure probability of the distribution line can be expressed as:

$$P_L(w) = \begin{cases} 0 & \text{if } w \le w_{critical} \\ P_L^{hw}(w) & \text{if } w_{critical} \le w \le w_{collapse} \\ 1 & \text{if } w \ge w_{collapse} \end{cases}$$

where, $w_{critical}$ is the wind speed at which the failure probability of the distribution line starts to increase and $w_{collapse}$ is the wind speed at which the distribution line is expected to fail.

4.3.1.1.3 Historical Event Data

The historical event data relates to the weather event data across the region in which the distribution network is located for a specified period. This data mainly includes:

- Period of historical data (e.g., past N number of years)
- Duration of the wind event (in hrs).
- Wind speed of the windstorm epicenter crossing the region.
- Geographical coordinates of the starting point of the wind event.
- Spatial trajectories of the wind event across the region.

- Variation of the wind event intensity (in m/s or km/hr for every period).

4.3.1.2 Event Modelling

The event modelling is the second stage of the proposed framework in which the attributes of the event are extracted, and the corresponding spatial and temporal model of the event is developed. The following subsections elaborate on the modules under this stage.

4.3.1.2.1 Extraction of Event Characteristics

The range of the following parameters is derived from the historical data to represent the characteristics of the wind event of the region.

- Wind gust speed (in m/s or km/hr).
- Windstorm headings (in degrees).
- Windstorm radius (in km).

The heading of the wind event specifies the direction in which the wind is traveling, and its value is calculated clockwise in degrees by taking the reference from North. The wind gust speed provides the intensity of the storm and the windstorm radius provides insight into the spread area of the wind storm that is affected.

4.3.1.2.2 Spatial and Temporal Modelling of the Event

The spatial modelling of the event defines the starting coordinates of the windstorm. This starting coordinate is randomly defined in the each simulation step throughout the area and is considered to move further according to the heading characteristics of the event. Meanwhile, there is a possibility of simulating the event that does not cover the chosen region of interest, therefore, the starting coordinates are chosen accordingly such that it covers the region for evaluation and optimizes the computational efficiency of the algorithm. In general, the intensity of the windstorm decreases with the increase in the roughness factor introduced by the elements through which it travels. For instance, the intensity of the windstorm diminishes upon entering a land mass from sea or ocean. Here, the velocity of the windstorm entering into a high roughness factor region is decreased linearly.
Once the starting point has been defined, the next step is to simulate the spatial trajectory of the wind event across the network. The temporal modelling of the event defines the duration of the event, the movement of the windstorm epicenter that reflects the speed at which the wind gust is moving across the network, and the radius of the windstorm. In this project, the duration of the wind event is randomly set within the bounds of 3 and 12 hours following a uniform distribution. Fig.31 illustrates an example of a wind event, where it can be observed that the windstorm is heading from the North Atlantic toward the mainland of Portugal with a decreasing windstorm radius (in km) as the event progresses.

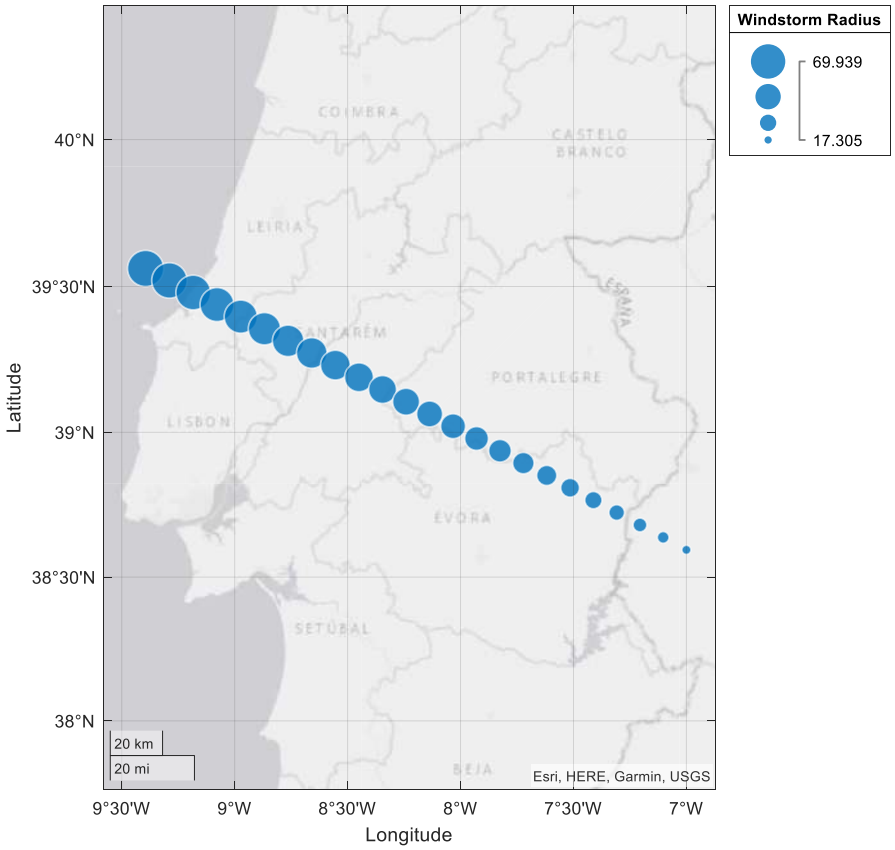


Figure 31. Example of windstorm movement

The combination of the event characteristics is of the most importance to the model as they define the extent of the network that is affected by the wind event. This model is developed with maximum flexibility for the user to adjust the event characteristics as desired.

4.3.1.2.3 Random Generation of Event Intensity

In this project, the windstorm hitting an electrical infrastructure and its corresponding restoration time is assumed to be within 24-hour window. To represent the complete range of historical wind events, 1000 Monte-Carlo-based windstorm scenarios are generated with 100 samples for each scenario. Fig.32 shows some examples of the thousands of wind event scenarios generated in this project.

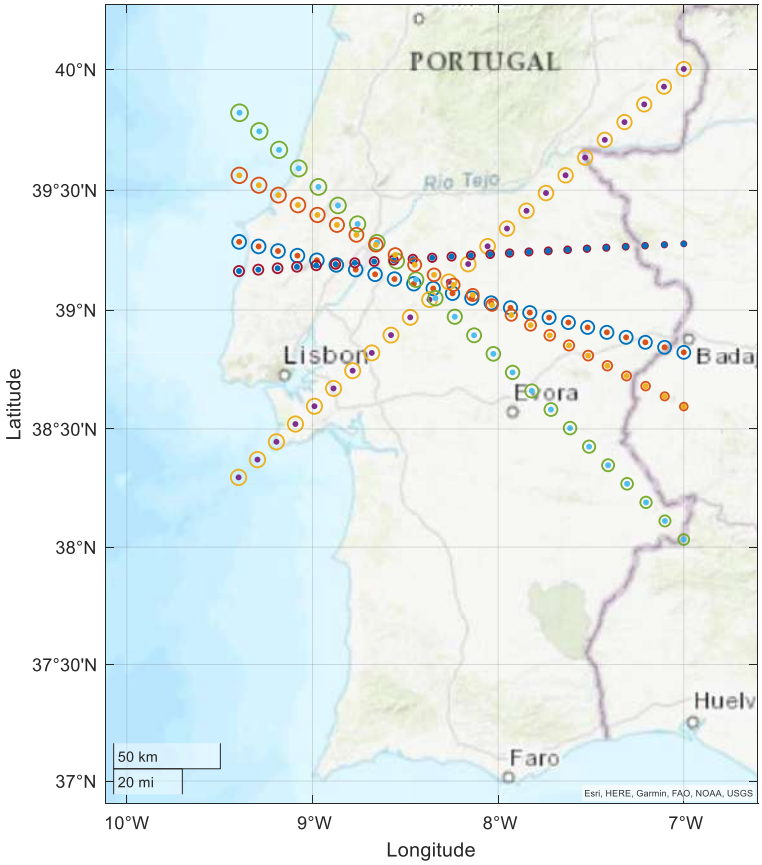


Figure 32. Examples of wind event scenarios across the Portugal distribution network

4.3.1.3 Impact Analysis

The impact analysis is the final stage of the proposed framework which delivers the network line status as an output resulting due to the effect of the wind event. To evaluate the impact of the wind event on the distribution network, an advanced function is developed in this project to identify the intersection points of the wind events and the distribution network lines. This function utilizes the spatial and temporal coordinates of the wind event, and the coordinates of the distribution network lines (developed using coordinates of the from-and-to buses), to identify these intersection points. Specifically, an impact zone is created which contains the distribution lines that lie within the windstorm radius of a wind event. Further, the simulation starts with the identification of the distribution lines that comes under the impact zone and records their wind speed or wind intensity. Subsequently, the operation of the given distribution line is evaluated based on the fragility curve shown in Fig.32. In other words, this fragility function provides the wind-dependent failure probability of the distribution line that comes under the impact zone. Once the failure probability $P_L(w)$ of the distribution line is obtained, it is compared with a uniformly distributed random number $r \sim U(0,1)$ to evaluate the status of the line. These failure probabilities of the distribution lines are dynamically updated at every step of the Monte Carlo simulation. The line status (L_s) of a line L_l in the distribution network at simulation step i is defined as follows:

$$L_s(w_i, L_l) = \begin{cases} 0 & \text{if } P_L(w_i) < r \\ 1 & \text{if } P_L(w_i) > r \end{cases}$$

The above expression represents that, if the wind-dependent failure probability $P_L(w_i)$ is greater than the random number r, then the line will be tripped, and a random restoration time will be generated until which the line status remains zero. This procedure is repeated for all the lines in the network and identifies the affected lines due to wind event in each simulation step. The status of the network lines is updated and stored which is used for further analysis.

4.3.2 AC Cascading failure model

Cascading failure models for resilience analysis are critical in order to simulate cascading events and identify methods to enhance resilience on the power networks. AC Cascading failure model (AC-CFM) [88] 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. AC-CFM uses a recursive approach to handle cascades within each island separately until the cascade comes to a halt as shown in Fig.33.

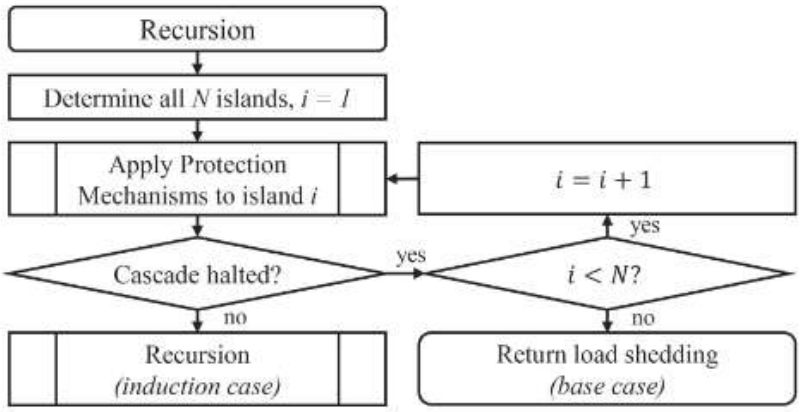


Figure 33. Flowchart illustrating the recursive approach of AC-CFM

Beginning with the initial network, the PF within every island is calculated and protection mechanisms are applied as shown in Fig.34.

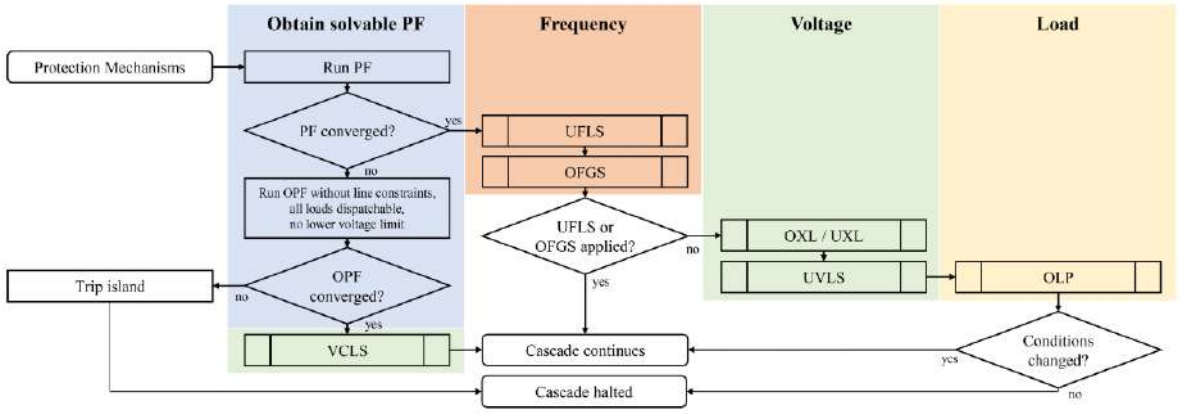


Figure 34. Flowchart illustrating the implementation and succession of protection mechanisms in AC-CFM

If the protection mechanisms have changed the conditions within an island, such as loads, generators, or operating lines, the recursion is applied to the island again (induction case). If the conditions have not changed or are within the specified tolerances, the cascade within the island comes to an end, and the model proceeds with the next island (base case). This implementation is a tree traversal, depth-first search, in which the cascade in one island is handled until its termination before continuing with the next island.

AC-CFM provides a novel way of visualizing cascading failures as a tree-like graph as shown in Fig.35. The graph expresses causalities in cascading failures and helps mitigating the impact of large and wide-spread blackouts. It holds all model output parameters, including the succession of protection mechanisms, the available loads, generators and lines, the disintegration of the network into islands, and the amount of load shedding at each generation.

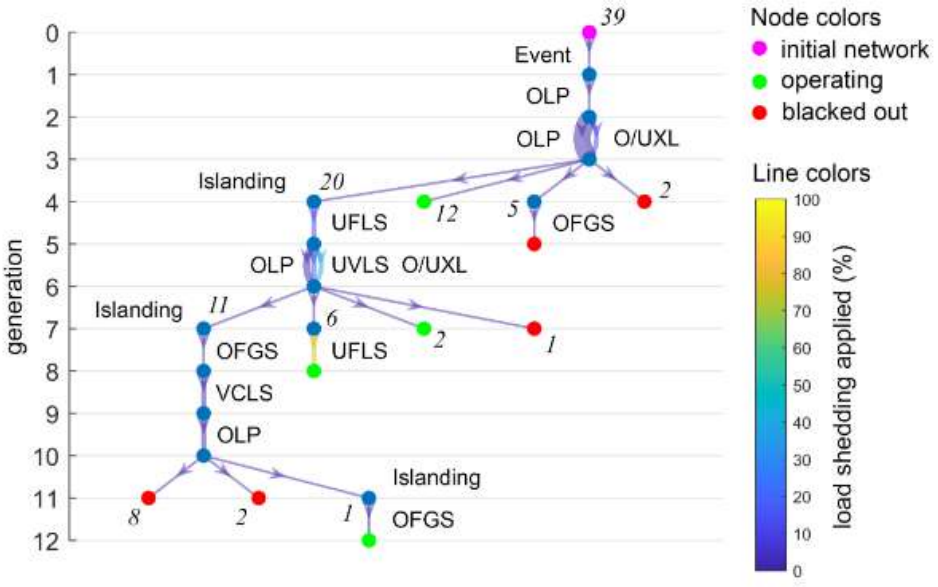


Figure 35. Visualization of a cascade in the IEEE 39-bus network

4.3.3 Machine learning for identification of critical components in power networks

4.3.3.1 Introduction

Analysing vast amount of data to find critical components in power networks is very computationally expensive and, in some cases, impractical. Carrying out such analysis require a lot of different features which means the dimensionality of the problem increases making the analysis even harder. Machine learning models can efficiently learn from vast amount of data and discover underlying patterns to make predictions.

Machine learning algorithms are data-dependent models that learn to recognize patterns using mathematical and statistical process. The construction of a good and representative dataset is the most important process in machine learning. No matter how much data someone has if the dataset and features are not descriptive and illustrative for a specific problem the algorithm will suffer of poor performance. Most machine learning models require huge amount of data to recognize patterns, but this is not always the case. There is no specific number of observations for every problem and there is no such thing as an ideal algorithm for all problems. The amount of data an algorithm needs to address a problem is highly correlated with the complexity of the case and how well the features are selected to represent the case. The more complicated the problem, the more examples an algorithm will need to learn distinguish or predict the classes.

In our case we are using machine learning models along with feature selection techniques to identify critical components in the network. Critical components are the ones more likely to cause bigger load shedding and cascade failures. To do so we construct a dataset of contingencies and run AC-CFM model to calculate the load shedding, then we assign class 0 if the load shedding is equal or over 1MW and class 1 otherwise. Then we are employing 7 feature selection techniques to identify the most critical components. For each set of features selected by the feature selection techniques we train a machine learning classifier to distinguish between class 0 and class 1 and then we evaluate the machine learning classifier performance based on sensitivity and specificity.

Sensitivity refers to the system's ability to correctly identify and react to faults when they occur (true positive rate), while specificity refers to its ability to correctly maintain operations without falsely tripping when no faults are present (true negative rate). (Explanation based on power system protective mechanisms) $Sensitivity = \frac{TP}{TP+FN}$, Specificity = $\frac{TN}{TN+FP}$ where TP the true positive predictions, TN the true negative predictions, FP the false positive predictions and FN the false negative predictions as shown in the confusion matrix of Fig36.

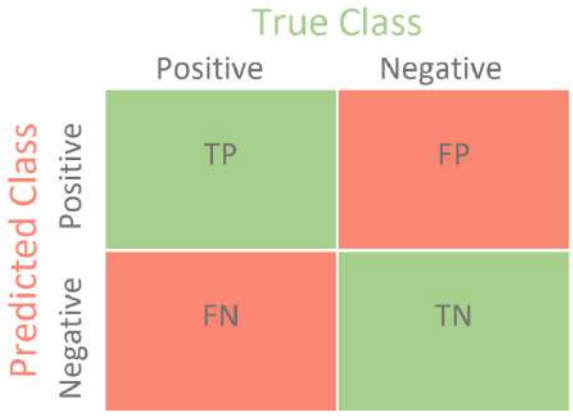


Figure 36. Example of a confusion matrix

The most intuitive metric is accuracy but, in some cases, it can cause misleading results. In most real-world cases we have imbalanced data meaning that we have more data for one class and less for the other class. This is not an issue if there are 60% examples for class 0 and 40% examples for class 1. However, identifying faults results in a lot higher imbalance of at least 1:5 ratio between the classes. Imagine that in this case the model has 80% accuracy, someone could say it's a relatively good model. However, if the model always predicts the majority class as output it would achieves 80% accuracy but in reality, it has 0% accuracy in predicting the minority class. This is known as the accuracy paradox [89]. To overcome this issue, we can use metrics such as sensitivity and specificity that are not sensitive to class ratio.

4.3.3.2 Methodology

4.3.3.2.1 Dataset generation

In our study, we utilize two distinct datasets to enable a multi-tiered analysis. The first dataset, although less comprehensive, provides a fundamental understanding of the prevailing patterns and dynamics. It is instrumental in establishing a broad, contextual understanding of the subject matter.

In contrast, the second dataset is far more comprehensive, encompassing a series of contingencies that represent a variety of scenarios. By using these two datasets in tandem, we can offer an analysis that is both broad in its understanding and detailed in its insight. The following sections will delineate the methodological approach we adopted for compiling these datasets.

For the dataset generation consider a network with n lines. In the first dataset we randomly generated 10660 contingencies. In building the second dataset, we systematically targeted each component in our system across a sequence of 1000 contingencies. In each of these contingencies, the targeted component was set to a 'failed' state. Concurrently, we induced random failure states in 1 to 6 additional components, generating a wide variety of failure combinations for each targeted component. This process was repeated for each component in our system, resulting in a series of 1000-contingency blocks. In each block, a

different component was set as the primary failed component, while the remaining components were subject to secondary, randomized failures. Therefore, the second dataset results in $1000n$ samples. For both datasets the minimum number of failed lines is 2 and the maximum is 7.

Once we have our contingency datasets we run the AC-CFM model for each contingency, and we are getting the load shedding. Then we assign the classes according to the load shedding. In both datasets we have a 1:5 ratio between the classes.

4.3.3.2.2 Feature selection techniques

The next step is to use the feature selection techniques to find the K most critical components, reducing the dataset more than that will cause lack of information and result in a poor performance model. We deploy 7 feature selection methods which are explained below.

1. XGBoost Feature Importance: Feature importance is calculated in XGBoost using a metric called 'F score', which represents the number of times a feature is selected to split the data across all trees. More important features will generally have larger F scores as they will be chosen more frequently for splits. The score is then normalized to sum to 1, creating a percentage-based importance measure.
2. Random Forest Feature Importance: The importance of a feature is computed by averaging the decrease in Gini impurity over all the trees in the forest where that feature is used to split the data. The Gini impurity measures the misclassification rate that would result from assigning a class label randomly according to the class distribution in a subset; a larger decrease means a more important feature.
3. Lasso Regression: Lasso (Least Absolute Shrinkage and Selection Operator) is a regression analysis method that involves penalizing the absolute size of the regression coefficients. By doing this, it effectively reduces the less important features' coefficients to zero, thus performing feature selection.
4. Logistic Regression: logistic regression coefficients assigned to each feature, can be seen as the importance or influence of features. A larger absolute value of a coefficient means a more important feature.
5. Logistic Regression based on P-values: In this approach, we fit a logistic regression model and keep the features with p-values below a certain threshold. The p-value for each term tests the null hypothesis that the coefficient is equal to zero (no effect). A low p-value (< 0.05) indicates that we can reject the null hypothesis, thus the feature is considered significant and selected for the model.
6. Mutual Information: In the context of feature selection, MI is used to quantify the "relevance" of each feature, i.e., the amount of information it gives about the output variable. A higher MI means a higher relevance. This measure is particularly good at capturing non-linear relationships. Note that mutual information is not a good method to find patterns but a good method to find relationships between variables.
7. Chi-Squared: The Chi-Square test is a statistical test that determines whether there is a significant association between categorical variables. In feature selection, it's typically used to test the relationship between each feature and the output variable, both being categorical. Features that are highly dependent on the output variable will return a low p-value (high chi-square statistic), indicating that the feature is relevant and should be selected.

4.3.3.2.3 Machine learning classifier

After testing many machine learning models, we chose eXtreme Gradient Boosting (XGBoost) classifier [90] based on its based on its superior accuracy in predicting class labels. The XGBoost is an ensemble algorithm that combines several decision trees (or weak learners) using the boosting method to generate the desired output prediction. Once the decision trees were trained, ensemble modelling by weighted averaging was performed to pool the results from multiple trees and average them using weights based on accuracy to minimize the error.

The core of XGBoost is to optimize the objective function's value by using gradient descent to create new trees based on the residual errors of previously trees. For a given dataset with n labelled examples and m features, K additive functions are used to predict the class of the examples as follows:

$$\hat{y} = \varphi(X_i) = \sum_{k=1}^{K} f_k(X_i),\ f_k \in F$$

where $F = \{f(x) = w_{q(x)}\}(q: \Re \to T, w \epsilon \Re^T)$ is the space of regression trees, q represents the structure of each terminal node index and T is the number of leaves in the constructed tree. Each f_k corresponds to an independent tree structure (q) and leaf weights (w). To this end, XGBoost minimizes the following regularized objective:

$$L = \sum_i l(\hat{y}_i, y_i) + \sum_k \Omega(f_k)$$

where $\Omega(f) = \gamma T + \frac{1}{2}\lambda\|w\|^2$, l is the loss function of the model based on the training data, and Ω the regularization term which penalize the complexity of the model. To speed up the optimization of the model second order approximation is used:

$$L^{(t)} \approx \sum_{i=1}^{n} [l(y_i, \hat{y}_i{}^{(t-1)} + g_i f_t(x_i) + \frac{1}{2} h_i f_t(x_i)] + \Omega(f_t)$$

where $g_i = \partial_{\hat{y}_i{}^{(t-1)}} l(y_i, \hat{y}_i{}^{(t-1)})$ and $h_i = \partial^2_{\hat{y}_i{}^{(t-1)}} l(y_i, \hat{y}_i{}^{(t-1)})$ is the first and second order gradient statistics on the loss function, respectively.

As discussed before, we are dealing with an imbalanced classification problem of a ratio 1:5. Ideally, we should have balanced class distribution in our data set when we are going to apply machine learning techniques. In most of real-world situations that's not the case, for various reasons our data set may have imbalanced class distribution and can't be fixed with adding more instances that correspond to the minority class. Most of the times, imbalanced ratio occurs from the nature of the problem and therefore sampling only one class can cause biases. Moreover, sampling minority class data maybe cost expensive due to their rarity.

Sampling methods are not used in evaluation dataset, the purpose of these methods is to deal with relative rarity when is trained but continue evaluate the model in real and

representative examples. It is important to separate the dataset into training and testing before applying sampling methods in the training set to avoid any data leakage.

First, the machine learning model is trained and evaluated on the original dataset. Next, we train a model using BorderlineSMOTE as the oversampling technique to address class imbalance. Finally, we train another model by combining the SMOTE oversampling algorithm with the Tomek Links undersampling algorithm, aiming to further enhance the model's performance by both generating synthetic examples for the minority class and removing potentially ambiguous instances near the decision boundary.

BorderlineSMOTE is an extension of the Synthetic Minority Over-sampling Technique (SMOTE) used to address class imbalance in machine learning. It focuses on generating synthetic examples near the decision boundary of the minority class to improve classification performance.

The combination of SMOTE (Synthetic Minority Over-sampling Technique) and Tomek Links is a two-step approach to address class imbalance in machine learning. First, SMOTE generates synthetic examples for the minority class to balance the dataset. Then, Tomek Links are used to identify and remove overlapping instances from both classes, particularly those near the decision boundary.

The methodology as described in this section is shown in Fig.37.

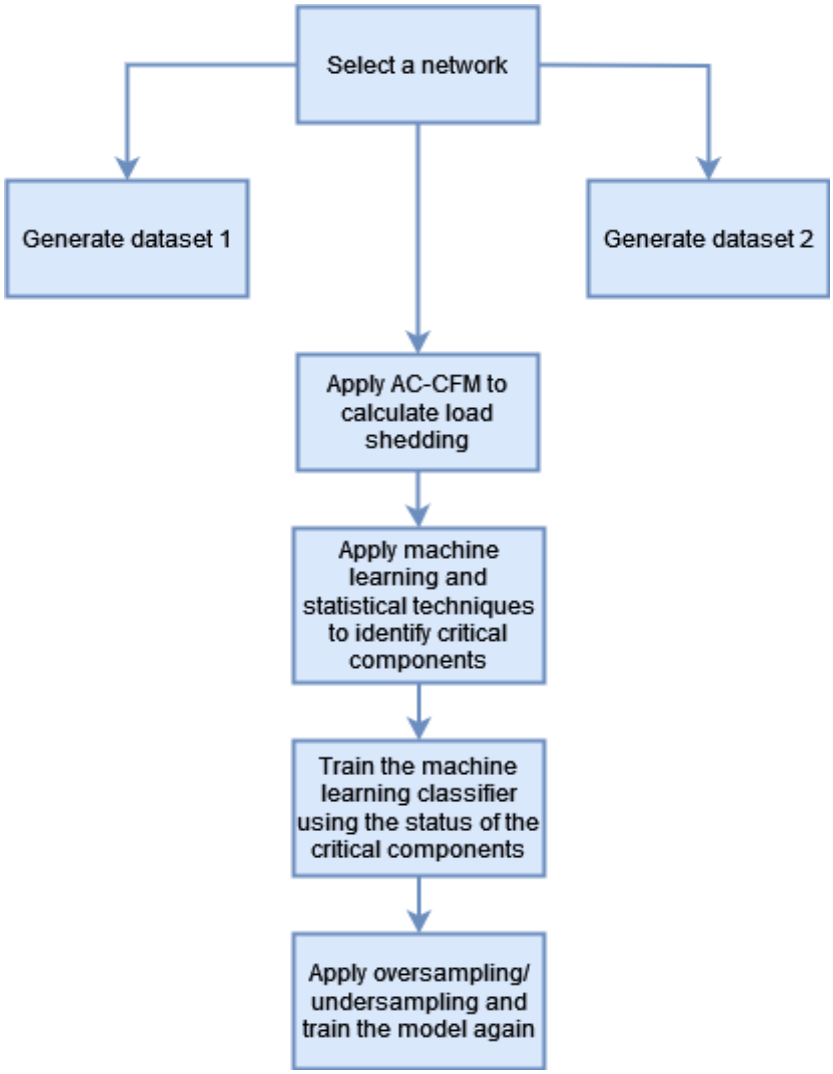


Figure 37. Methodology flowchart

4.3.3.3 Results

The results presented in this section address the research objectives outlined in the previous sections. The selected network for this study is the IEEE-24 Bus Reliability Test System (RTS), which consist of 24 busses and 38 lines (33 transmission lines and 5 transformers modelled as lines). This results in a dataset with 38000 contingencies for the second case. We are choosing the 15 most critical components using the feature selection techniques. The decision to settle at 15 features it provided a balance between model simplicity and performance.

In Fig.38, we illustrate the critical selected components from the first dataset. The figure displays the number of times each component was selected, indicating the level of agreement among the different methods employed. Mutual information was excluded due to its poor performance.

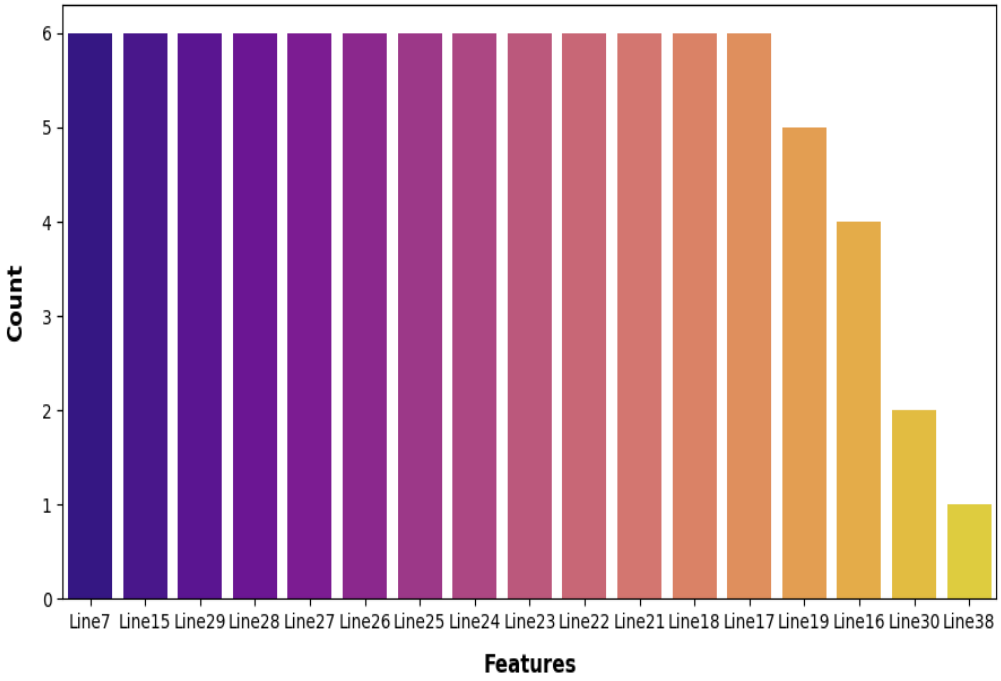


Figure 38. Frequency of critical selected components

Table 6 displays the performance of the classification model under the 3 cases.

Table 5. XGBoost performance

Metric	XGB	XGB OV	XGB OV UN
Sensitivity	79.3%	83.4%	83.2%
Specificity	95.4%	93.6%	92.2%

Where XGB the XGBoost classifier, XGB OV, the case of applying oversampling, and XGB OV UN the case of applying the combination of oversampling and undersampling.
We can clearly observe a trade-off between sensitivity and specificity. The maximization of either of them is up to the user to choose based on their needs.
In the second case, the agreement of the feature selection techniques is even more obvious. As shown in Fig.39, most of the features were commonly selected from all feature selection techniques. Note that mutual information and chi-squared were not included due to poor performance.

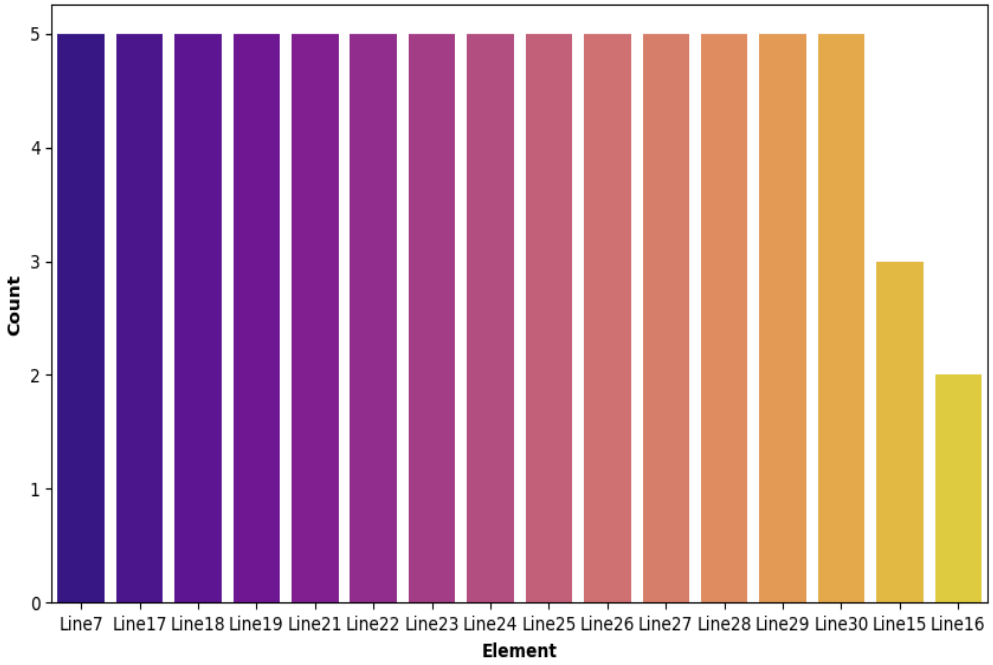


Figure 39. Frequency of critical selected components

Specifically, all the methods chose the same 14 components as critical, and the only disagreement is between lines 15 and 16 that are neighbouring lines in the network. Table 6 displays the performance of the XGBoost under the 3 different cases.

Table 6. XGBoost performance

Metric	XGB	XGB OV	XGB OV UN
Sensitivity	80.6%	90.2%	83.7%
Specificity	92.3%	80.4%	90.3%

We can observe that the sensitivity is increased but the trade-off between sensitivity and specificity is more obvious than before.

4.3.4 User Interface

The user interface platform consists of 5 pages. The first page is just an introduction/welcoming page. The second page requires the user to fill the boxes with the data needed and upload the necessary files for the storm generation model to work. On the third page we can see data regarding the system, the power profile, and the projected network on the map. The fourth page is about the generated storm and its impact on the system regarding line status and load shedding. The user should upload the contingencies dataset along with the load shedding. On the fifth page we have the AC-CFM model where the user can select any hour of the event and run the model. The five mentioned pages are shown in the following figures.

Figure 40. Introduction/Welcoming page

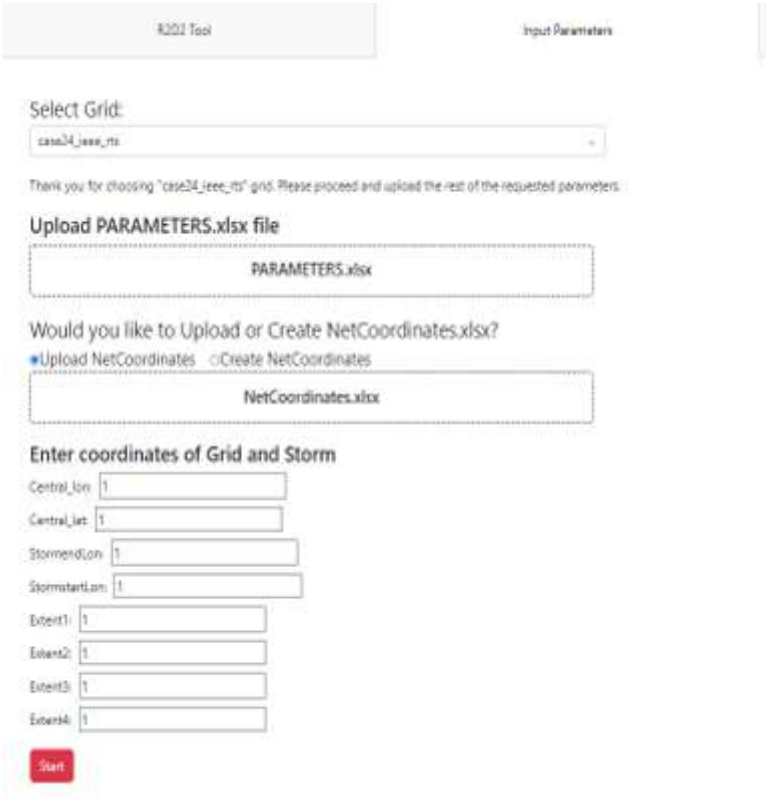


Figure 41 Storm Generation Model Data Page

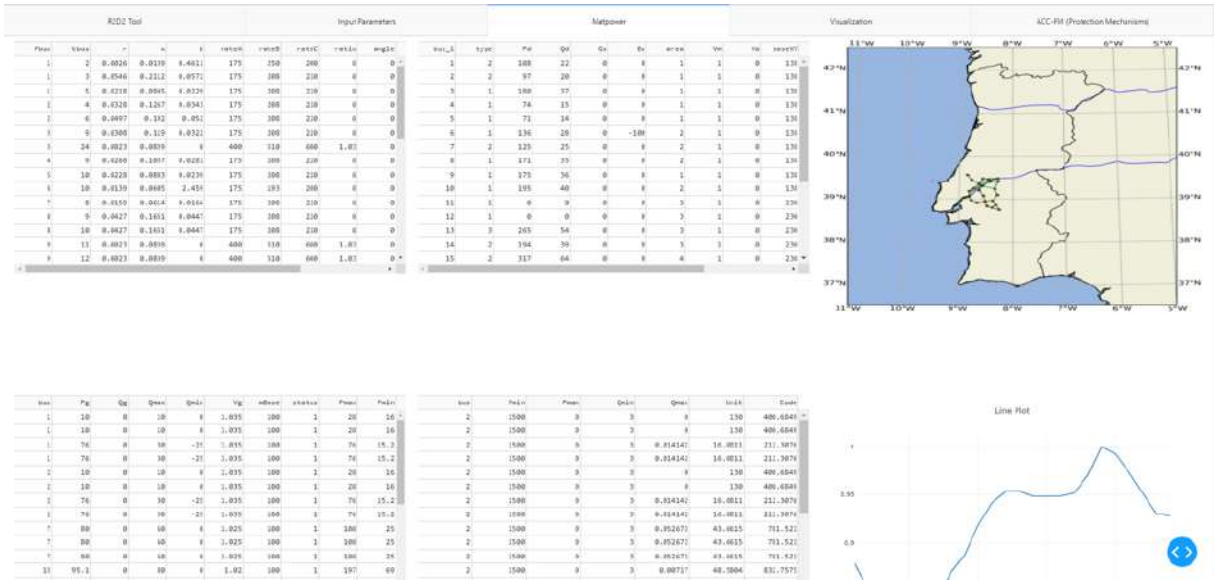


Figure 42. Network data

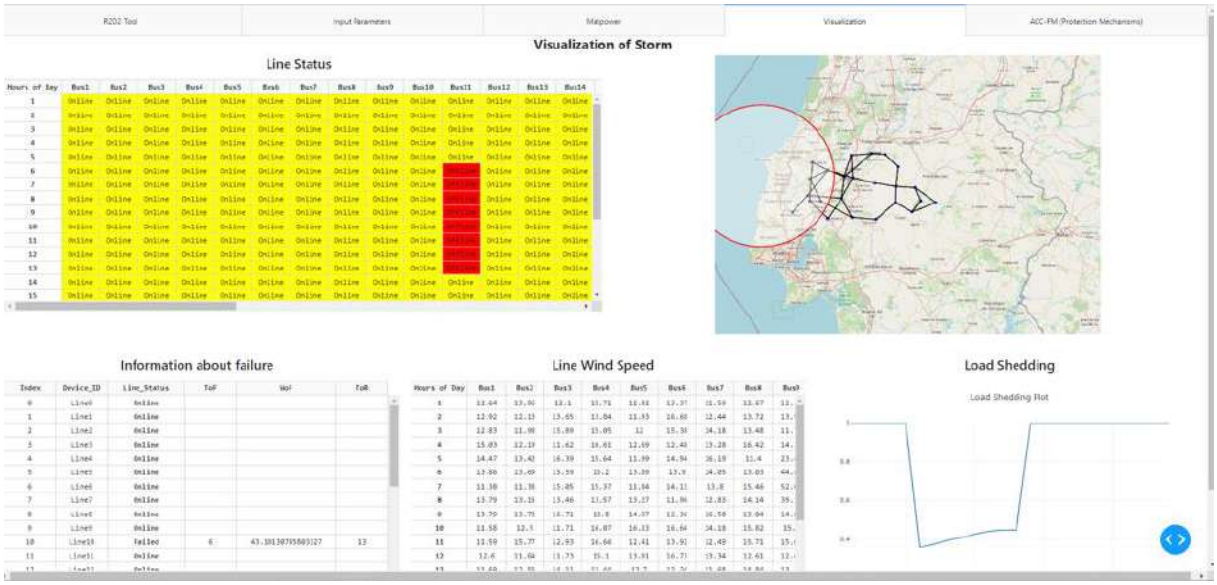


Figure 43. Effects of the generated storm

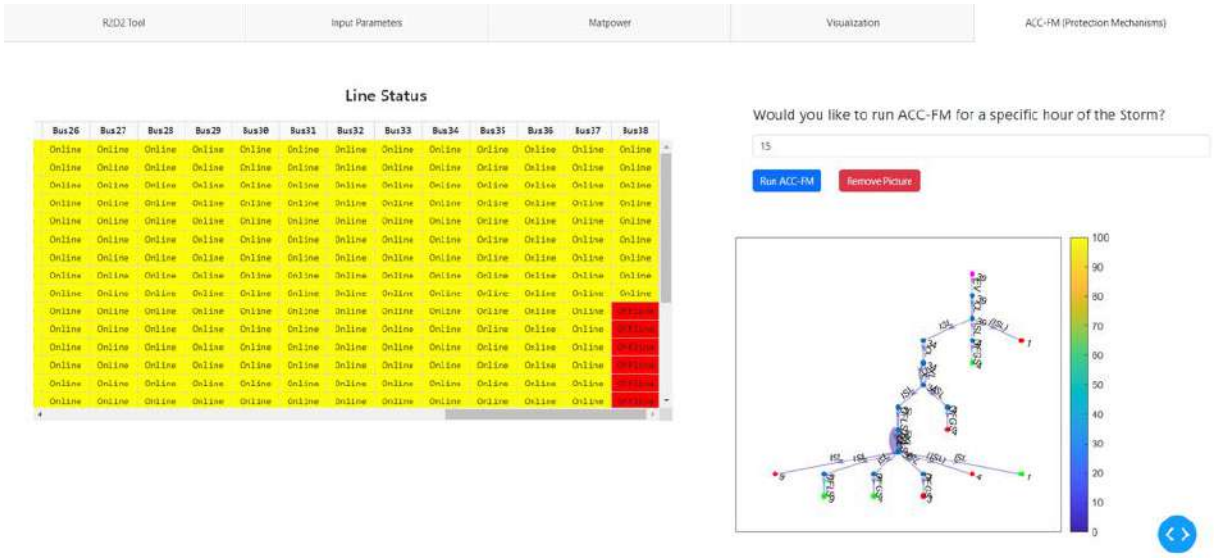


Figure 44. AC-CFM

4.3.5 Resources

1. The fragility modelling framework was coded in Python using the following libraries:
   - Numpy
   - Pandas
   - Math
   - Scipy
   - Matlab engine
   - Cartopy
   - Shapely
   - Geopy
2. The AC-CFM model was coded using MATLAB.
3. The machine learning model was build using Python and the following libraries:
   - Numpy
   - Pandas
   - Scikit-learn
   - Xgboost
   - Imbalanced-learn
   - Statsmodels

4.3.6 Event simulator of a progressing wildfire and assessment of its impact on distribution system

4.3.6.1 Internal Architecture of the tool

Extreme weather events can cause serious damage to power grids. In recent years, the world has witnessed a growing urgency for effective strategies aimed at bolstering the resilience of power grids in the face of such events. Climate change has exacerbated the occurrence and severity of HILF events, including wildfires, floods, and windstorms, which frequently result in power disruptions and infrastructure damage. Any operational framework seeking to enhance the physical resilience of power systems must acknowledge the distinct characteristics of various HILF events. This recognition systems from the fact that each extreme weather event exerts varying spatial and temporal effects on power system infrastructure. Among these natural disasters, wildfires stand out as one of the most dangerous HILF events, capable of imperiling the reliability of power infrastructure. Numerous countries, particularly those such as Greece, Spain, and Portugal, are susceptible to such catastrophic events, particularly during the summer months. In these regions, distribution systems that traverse densely vegetated or forested areas are particularly vulnerable to wildfires. Moreover, incidents involving power lines serving as ignition sources are not uncommon. Distribution line faults can trigger wildfires, especially in areas characterized by high temperatures, strong winds, and low humidity. To mitigate this hazard effectively, a comprehensive evaluation of the potential impact of wildfires on the distribution system is necessary.

The proposed tool is developed in parallel with the T3.3.1 "Spatial and temporal event and fragility modelling". Its purpose is to enrich the HILF events modular simulator tool features of T3.3.1 which mainly focuses at windstorms and fragility-based modelling, to also include wildfire events modelling, expanding the features of the C3PO, as they are described in the DoA. The end users will obtain a tool able to model wildfire events, to assess their spatial and temporal impact on distribution system (such as line outages and lines capacity reduction) and to propose a set of operational measures to enhance its resilience and to mitigate the disruptive effects of a potential wildfire event, supporting DSO's decisions. Therefore, an optimization-based tool is developed aiming at scheduling the distribution system resources operation to minimize load curtailments and the expected socioeconomic (operational) cost during such an emergency situation, using stochastic programming to capture the diverse uncertainties (load demand, solar radiation, wind speed etc.). The described stochastic structure is deployed by utilizing a scenario generation algorithm, based on the uncertain parameters forecasted probability distribution functions (PDFs). By examining a large number of scenarios instead of mean values, the tool provides final results that cover a wide spectrum of different most probable parameter values, including the ones that depict the worst case probable conditions. Afterwards, a scenario reduction algorithm is used to to make the optimization problem tractable and reduce the computational burden, while keeping the stochastic information as intact as possible. Additionally, in order to evaluate the distribution system line outages and to quantify the spatial and temporal load curtailments provoked by the extreme event, this scheme is able to assess the wildfire propagation, taking into account the varying weather-related conditions. The Dynamic Line Rating (DLR) of the overhead lines is considered in order to model the impact of wildfire on conductor temperature and flowing current. By assessing the spatiotemporal propagation of the wildfire (based on network and weather-related data) the tool provides for the DSO an optimal scheduling strategy of power resources to enhance the resilience of the grid, considering the dynamic conditions during the spread of a progressing wildfire. The proposed model comprises a mixed integer problem (MIP) with quadratic constraints and stochastic structure, which effectively provides solution to the distribution system operation against an

approaching wildfire, by optimally scheduling the grid's power resources to enhance its resilient response, taking into account the wildfire propagation. In conclusion, the presented tool aims to deliver a useful toolkit that can contribute to the improvement of the overall security and resiliency in power system, supporting DSO's decisions.

The applicability and practicality of this tool will be tested in Xanthi pilot site (Greek demo). Extreme weather events including high winds, wildfires and heavy snowfall have caused unscheduled power outages at this pilot site in recent years. The presented tool mainly requires the following input data:

- Network data (network topology, asset connections, MVA base)
- Generators data (capacity, minimum generation level, ramping rates, minimum up/ down time, connection to which bus, marginal cost)
- Lines data (resistance, reactance, capacity, diameter, length)
- Weather-related data (ambient temperature, wind speed, wind direction, solar radiation)
- Active and reactive active load demand data (in hourly basis)

In the premises of the R^2D^2 project activities, the presented tool is also correlated with the following requirements:

- C3PO must have access to weather forecast of the pilot site locations
- The topologies of pilot site networks must be well known and modelled
- In case of emergencies, such as extreme weather events, the system operator has the jurisdiction to control the dispatchable DGs, RES and ESS units
- The location and technical characteristics of DERs must be known
- The characteristics of distribution lines must be known
- Ideally some historical data of recorded wildfire events can be used to simulate past events.

The general structure of the proposed tool is presented at Fig.45, depicting the architecture of the described tool.

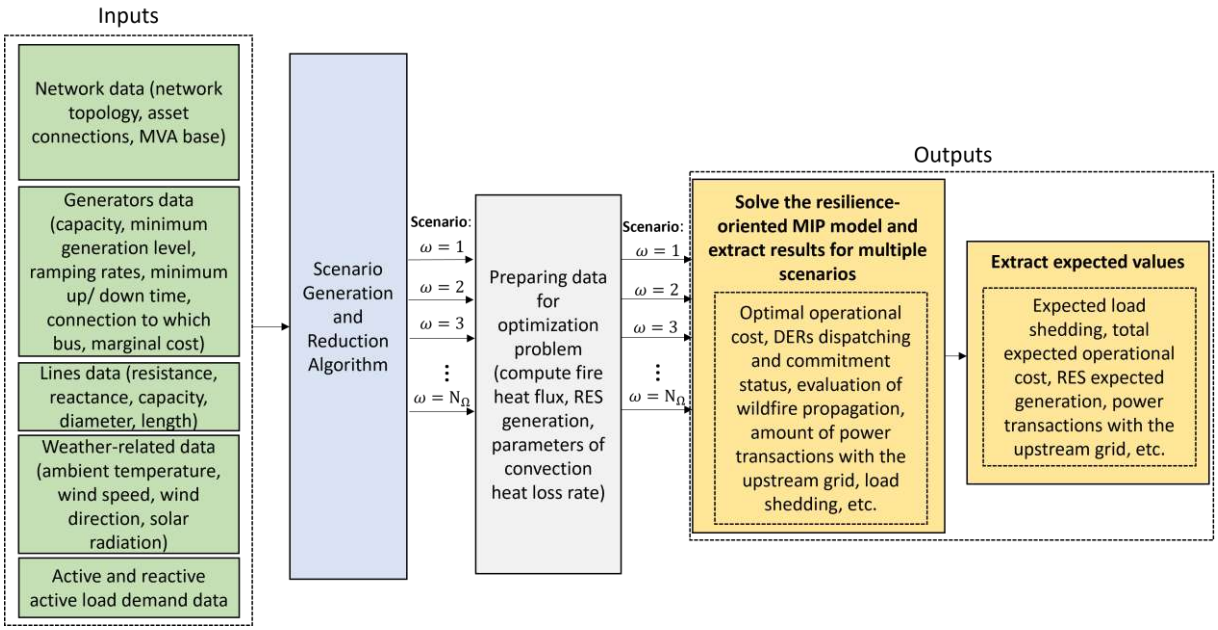


Figure 45. General structure of the tool

In conclusion, this tool provides for the end users a framework which models wildfire events, assesses their impact on distribution system and also delivers an optimal operational strategy to enhance the network resilience against this kind of natural disasters, supporting the DSO's decisions. Regarding C3PO interconnections and features, this tool is available to provide inputs to T3.3.2 as initiating events to the cascading simulators and can also provide wildfire event scenarios inputs for T3.4.2 and T3.5. Although, it is preferable that T3.3.1 provides extreme-weather-events-induced line outages scenarios as inputs for the other C3PO tasks beacause of the extended spatiality of the outages extreme winds can provoke.

4.3.6.2 User Interface

The described tool purpose is to deliver a relevant report for the DSO assessing the disruptive spatial and temporal impact of wildfire events in the grid, evaluating the propagation of the wildfire based on weather-related data and proposing an optimal resilience-oriented scheduling of the DERs for enhancing the resilient response of the grid against such events. The extracted results from the described tool including relevant figures will be illustrated in a web-based application.

4.3.6.3 Resources

The wildfire event simulator is developed in Python programming language environment using the Pyomo package to build the optimization model and the Gurobipy package solvers. In overall, the presented resilience tool utilizes the following packages and libraries:

- Pyomo
- Gurobipy
- Numpy

- Pandas
- Math
- Scipy
- Matplotlib
- Sys

4.4 RESILIENCE-DRIVEN INVESTMENT AND OPERATIONAL PLANNING TO MITIGATE OR PREVENT CASCADING EFFECTS (TASK 3.4)

4.4.1 Aim and objectives

With the occurrence of any extreme event, the network function, as shown in **Error! Reference source not found.**, experiences different states depending on the severity and duration of the extreme events and the fragility of the equipment. So, 5 interruptions may be experienced by any node on the distribution network following an extreme event including progression, fault identification and isolation, restoration, repair, and load shedding (see Table 7).

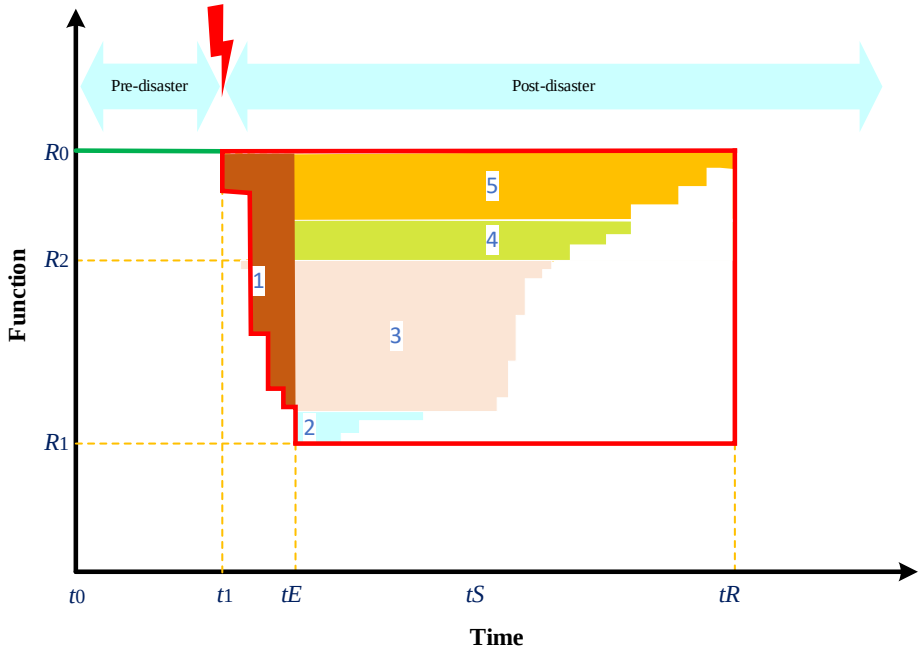


Figure 46. Typical DS resilience curve due to the extreme events

Table 7. Type of extreme events interruptions.

Interruption	Type (c)
Progression	1
Identification and isolation	2

Restoration	3
Repair	4
Load shedding	5

The resilience of DS can be evaluated by the expected duration of the interruption types and the amount of supplied/unsupplied load demand along the resilience curve. The duration of the first type interruption is related to the duration of the disaster, for the second type, this duration is related to the identification and isolation of the faulty parts as well as restoration decision making process of the network after the disaster occurs. The duration of the restoration is related to the time required for post-disaster network reconfiguration (microgrids formation). The period after the restoration, i.e., post-restorative mode, is related to the scheduling and providing the necessary facilities to proceed with the recovery of the damaged infrastructure. The duration of the last mode is mainly associated with the time required for installing and operating the damaged equipment in the network. It is evident that proper planning to reduce each of these time durations, can improve the resilience of the network. On the other hand, the network function in the fault propagation phase is greatly affected by the spatial and temporal characteristics and the severity of the fault and the fragility of the network equipment against the shocks caused by the fault. The amount of network function improvement during the restoration time is greatly affected by the available capacity and the location of existing resources in the network, such as distributed generation resources, switches, energy storage, portable power sources, etc.

Resilience-driven DS operation and planning practices can be used for enhancing DS resilience. The network operation (short-term or operational planning) is employed in two ways, i.e., pre-disaster operation when the imminent fault is predicted, and post-disaster operation. As a means of ensuring rapid response to disasters, early allocation of mobile resources is essential in pre-disaster operational planning. This includes repair crews and mobile power sources that can be deployed within a limited area when an event occurs. Post-disaster operational planning refers to the process of restoring services following extreme events by utilizing a reconfiguration program and forming potentially self-sufficient microgrids. Hence, the optimal allocation of resources can significantly improve network resilience characteristics in the restorative mode. Besides, the long-term planning (infrastructure planning) looks for the optimal allocation of resources (switches, DERs, and MPSs) and network hardening to improve DS resilience from the perspective of duration and system function in the face of possible natural disasters in the future. Therefore, infrastructure planning can be an effective strategy in improving the DS resilience over all modes of the network resilience curve. For example, line hardening can shift the network function in the resilience curve in **Error! Reference source not found.** upwards and reduce the outage time duration of interruption types due to reducing the probability of equipment failures. It's evidence that the first step in the resiliency-driven planning process is to measure the system's resiliency based on the proper metrics.

4.4.2 Methodology

Task 3.4 focuses on long-term planning while considering the possible effects of short-term planning strategies on decision variables and objective functions. The overall procedure of Task 3.4 is outlined in Fig.47. Accordingly, the Tasks' 3.3 tool is used first to generate the hazard scenarios in our proposed methodology. The second step involves calculating and

evaluating resilience indices using the algebraic model developed in the previous step. A resilience-driven planning approach could easily incorporate these metrics into the planning process. Thirdly, objectives, decision variables, and constraints are determined to formulate the planning problem. As a tool for measuring network resilience, the metrics proposed in the second step are also included in the third step. Different approaches are used to solve the planning problem at the final stage.

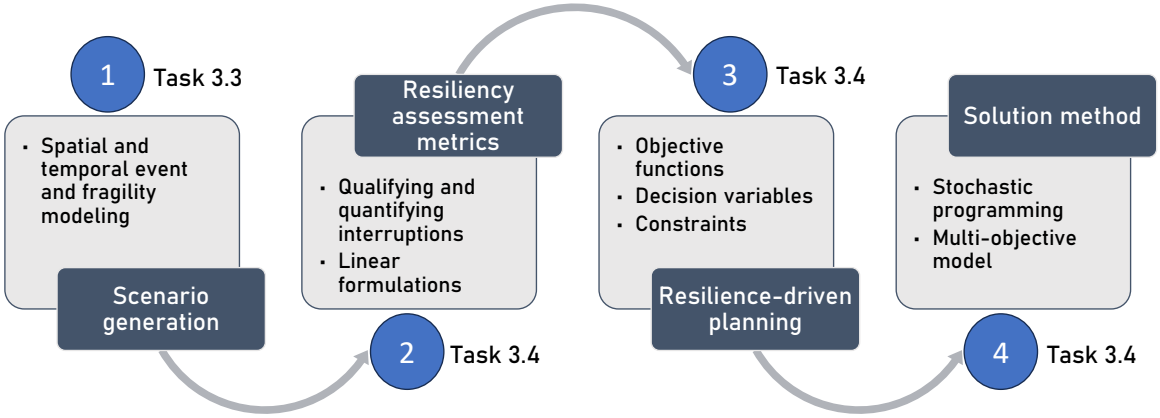


Figure 47. Overall methodology in Task 3.4.

1. Hazard scenario generation. Extreme weather-based events such as floods, earthquakes, hurricanes, typhoon, snowstorm, and other kinds of man-made physical and cyber-attack can leads to disastrous consequences in the operation and planning of electricity networks. Each type of these events has its own impact on the performance of electricity networks. To appropriately develop new operation and planning strategies, it is critical to qualify and quantify these events using sufficiently accurate models. However, estimating, modelling, and predicting such events are very difficult due to the highly uncertain characteristics of these events. For the evaluation and enhancement of power system reliability/resiliency, types and source of events should be properly defined. These events can result in N-1 contingency (in which extreme weather isn't the source of a contingency) and extreme weather-based N-k contingencies. In this work, the hazard scenario generation tools proposed in Task 3.3 is utilized to model the power system components that can potentially fail during an anticipated extreme event.
2. Resiliency assessment model. The power system model needs to incorporate system level failure models to develop the complete system resiliency models. Numerous models will be considered for modelling the power system in resilience-based studies including DS type, enhancement strategies, load flow model, solution method and other technical and operational constraints. Each of these models plays a critical role in developing power system resilience tools. To achieve these goals, a general linear algebraic model of resiliency indices evaluation will be defined based

on nodal-oriented and system-oriented resiliency indices. These indices evaluate rates and durations of possible interruptions caused by predefined set of faults in lines, switches, and other components using novel linear algebraic formulations (see Fig.48). Then, the model extended is used for the resilience assessment of radially operated meshed-designed distribution networks considering the post-disaster service restoration as shown in Fig.49. Additional constraints will be defined in this model to identify radially operation of the networked microgrids in the semi-damaged distribution network. This model defines an optimal re-dispatching of DERs and network reconfiguration of radially operated meshed-designed distribution networks with resiliency improvement goals.

3. Resiliency-driven long-term infrastructure planning. Objectives, and constraints associated to the various kinds of resilience enhancement strategies should be considered in the resiliency assessment model. Then, the developed model is applied to resiliency-driven long-term infrastructure planning. The major objective of this research is to establish a cost-effective optimization tool to be incorporated in various kinds of resiliency-driven planning studies. This model can also be used in disaster preventive scheduling, post-fault scheduling and dynamic restoration, DS expansion planning, DERs integration, DS hardening, switch placement, DS reconfiguration, etc.
4. Solution method. Planning problems usually involve several factors. On the other hand, different scenarios should be considered to model failures, load demand, and production power of photovoltaic systems. Two-stage stochastic programming is introduced to cope this issue. Besides, it is possible to reduce the computational burden of these problems by using decomposition techniques. Additionally, to facilitate decision-making for system operators and planners, multiobjective approaches are introduced to deal with conflicting objectives, i.e., investment cost and resilience improvement metrics.

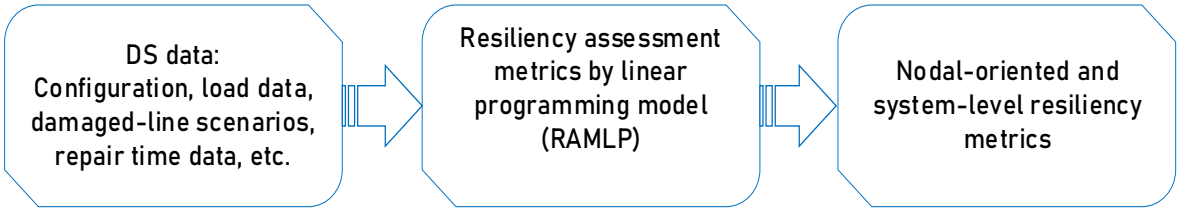


Figure 48. Resiliency assessment performance metrics

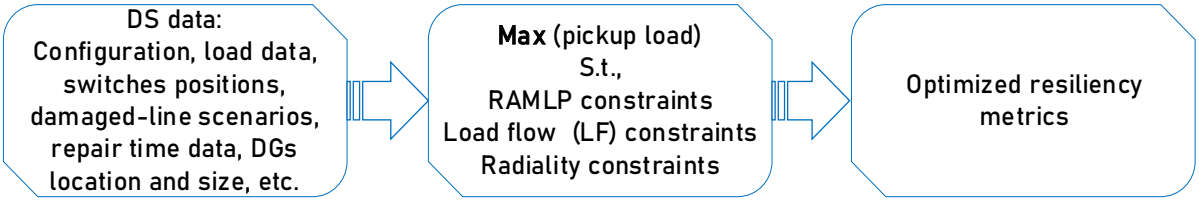


Figure 49. Evaluating the effect of post-disaster restoration on the resiliency metrics

4.4.3 Distribution system interruptions due to the extreme events

Looking at the typical resilience curve, if we ignore post-event restoration, the red curve shows the energy lost. By assuming post-event strategies, it is possible to effectively reduce lost energy, which is the sum of the area of the colored parts.

Each interruption type has different meanings. For example, type 1 interruption shows the network's robustness against cascading extreme events. In contrast, type 2 interruption illustrates the system's ability to identify events and take timely action. This is done to isolate and restore network parts using the main substations. Interruption type 3 shows the level of the resourcefulness of the network and its flexibility to restore the sensitive loads of the network in island mode (in other words, this type of interruption indicates the pick-up loads of the network). Interruption 4 introduces energy lost to repair damaged parts. Interruption type 5 shows the amount of energy lost due to the lack of alternative resources to supply healthy parts of the network. The following interruptions may be experienced by any node on the distribution network following an extreme event.

4.4.3.1 Event progression interruptions

In case of a fault along a feeder, the main breaker at the beginning is tripped. As a result, all buses along the feeder are shut down. The duration of this interruption is equal to the period of the fault and the operation time of the protection system (which is usually negligible and can be ignored). Suppose the extreme event's spatial and temporal nature is considered. In that case, the duration of the interruption of the damaged feeders for the next time step is equal to the period minus the sum of the previous time steps.

4.4.3.2 Identification and isolation interruptions

After the hurricane passes, the network enters the degraded phase. In this phase, the damaged parts are identified by fault indicators and separated from other healthy parts of the network by the nearest sectionalizing switches. In addition, the feeder's main breaker can now be closed so that the substations can reenergize the healthy parts. Consequently, a fault detection, clearing, and reconnection timeout must be included in the switching interruption duration for reenergized buses. Repair crews are dispatched to the damaged sections at this stage, and the repair time begins.

4.4.3.3 Restoration interruptions

For other healthy islands, the restoration program should be implemented. First, the buses fed by existing energy sources and grid reconfiguration should be identified and provided. For these buses, fault identification, isolation, and restoration times must be considered as the interruption time.

4.4.3.4 Repair interruptions

A repair interruption is considered for buses that are located in faulty sections. Repairs must be conducted quickly to minimize disruption to normal bus services. The decision to interrupt repairs is made considering the severity of the fault, the impact on public transport services, and the repair cost.

4.4.3.5 Load shedding interruptions

This type of interruption may occur in two cases: the first is when the bus has experienced a type 2 interruption, and the restoration program cuts off the power supply to the more sensitive loads of the network. The second case is when the load is left without electricity until the restoration program and remains without electricity. These interruptions are assumed to last until the damaged parts are repaired or until an MPS is available.

4.4.4 Distribution system resilience metrics identification and quantification

To assess resilience, we need to identify and quantify these interruptions using appropriate metrics not based on simulations. Towards this end, we have introduced three categories of general indices: node-oriented, feeder-oriented, and system-oriented metrics. Due to cascading extreme events, these metrics are determined based on the expected interruption rates and durations at each load node. The nodal-oriented, feeder-oriented, and system-oriented metrics are defined for network resilience measurement based on the qualification and quantification of interruption types and durations. The metrics are established based on two leading indicators: the frequency and duration of interruptions. This allows for a more accurate assessment of network resilience during unexpected outages.

4.4.5 Resilience-driven investment and operational planning problem

We introduce stochastic mixed integer linear programming model for this optimization problem. The main objective of the problem is to minimize the annual capital cost of line hardening and DG/switch placement as well as minimization of the operation costs in terms of load shedding and damage repair (or expected energy not supplied) in the realized extreme weather events. The post-fault interruptions are also included in the problem to evaluate their potential effects on the planning decision variables and the objective functions.

To facilitate discussion of the proposed resilience-driven planning model, the following compact notation is used:

$$\min_{x} \ \boldsymbol{c}^T\boldsymbol{x} + \sum_{s} \rho(s)\,\varphi(\boldsymbol{x}, s)$$

$$s.t.\ \ \boldsymbol{A}\boldsymbol{x} \leq \boldsymbol{B} \qquad \text{(a-1)}$$

$$\boldsymbol{x} \in \mathbb{Z}_{+}^{\boldsymbol{n}}$$

In the first stage, $\boldsymbol{x}$ represents the binary decision variables of the planning problem, and $\boldsymbol{c}$ represents the cost coefficient vectors. As shown in constraint (a-1) the maximum budget for line hardening, DGs, and line switches is expressed as a vector, i.e., $\boldsymbol{A}\boldsymbol{x} \leq \boldsymbol{B}$.

In addition, for a given scenario s, $\varphi(x,s)$ represents an operational problem as follows:

$$\varphi(\boldsymbol{x},s) = \min\ \boldsymbol{g}^T\boldsymbol{y}$$
$$\boldsymbol{s.t.}\ \ \boldsymbol{F}\boldsymbol{y} \le \boldsymbol{o}(s) - \boldsymbol{n}(s)\boldsymbol{x} \qquad \text{(a-2)}$$
$$\boldsymbol{x} \in \mathbb{Z}_+^{\boldsymbol{n1}} \times \mathbb{R}^{\boldsymbol{n2-n1}}$$

4.4.6 Numerical Results

4.4.6.1 Resiliency assessment

A modified radial network of 37 buses has been evaluated using the proposed resiliency assessment model. Three DG units are considered in buses 3, 23, and 27, and three tie-switches are assumed on lines 3-4, 3-22, and 28-33. Also, a circuit breaker is installed at the beginning of each feeder, and the beginning of all lines is equipped with a sectionalizing switch. Note that, each feeder is defined based on its root node number in this model.

For a set of arbitrary damaged lines caused by an extreme event in the studied case system, the proposed resiliency assessment tool is utilized to identify the type of interruptions at each load node and the result is shown in Fig.50. Note that, all nodes experienced a type 1 interruption due to at least one damaged line per feeder. This is not included here because there is at least one damaged line per feeder. Interruptions of types 2 and 4 are found immediately after identifying fault locations and isolating them using the linear programming model which is proposed in (c2-21) and (c2-22). Other buses can be identified by implementing the third optimization model presented in (c3-26) and (c3-27). As observed, picking up some load nodes by forming an optimal microgrid is possible. Hence, two microgrids have been formed based on the proposed model, as shown in Fig.50.

Using the resilience assessment model, 10,000 possible line failure scenarios were run to obtain nodal-oriented EENS results for each interruption. It can be seen from Fig.51 that most energy is lost because of interruptions of type 1 indicating the weakness of the infrastructure against the simulated extreme event. In addition, Type 3 and 4 interruptions indicate that there are insufficient resources in island mode to restore more loads. The proposed resilience assessment model provides network operators with significant information about the overall state of their networks in the event of a future accidental hurricane. Fig.52 for example, represent nodal-oriented metrics such as interruption rate, interruption duration, and expected lost load per bus. As a result, it is possible to identify which load nodes are at risk of storms. The amount per node is often determined by the degree of destruction caused by the storm, the fragility of the equipment, the length of the lines, and the load demand at each node.

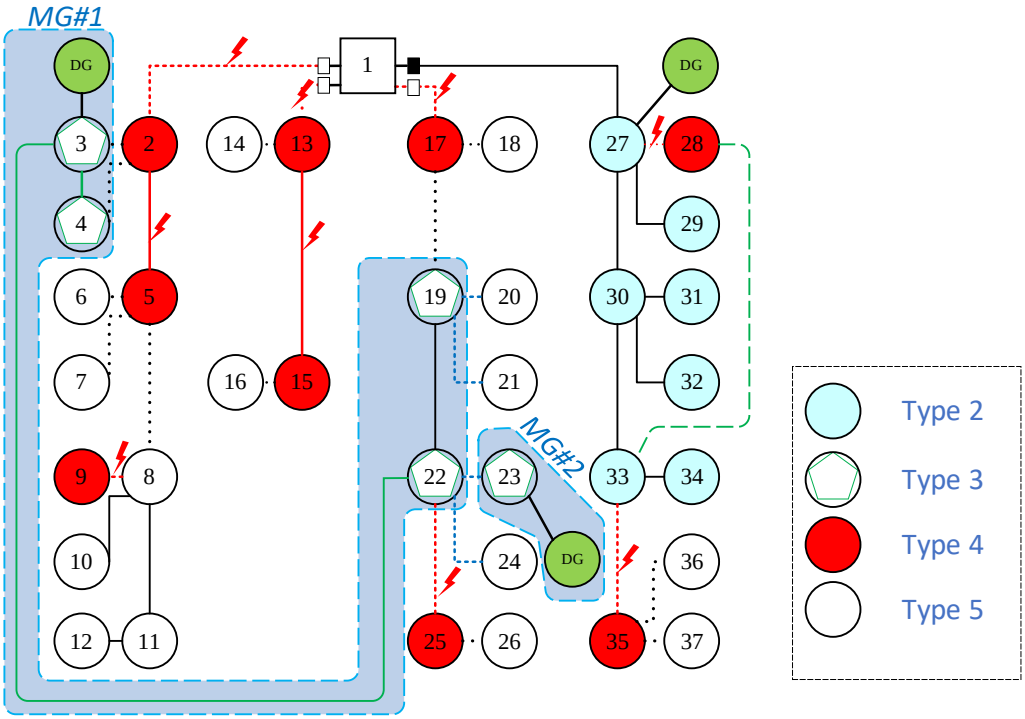


Figure 50. Interruptions identification for a sample damage scenario on 37-node test system

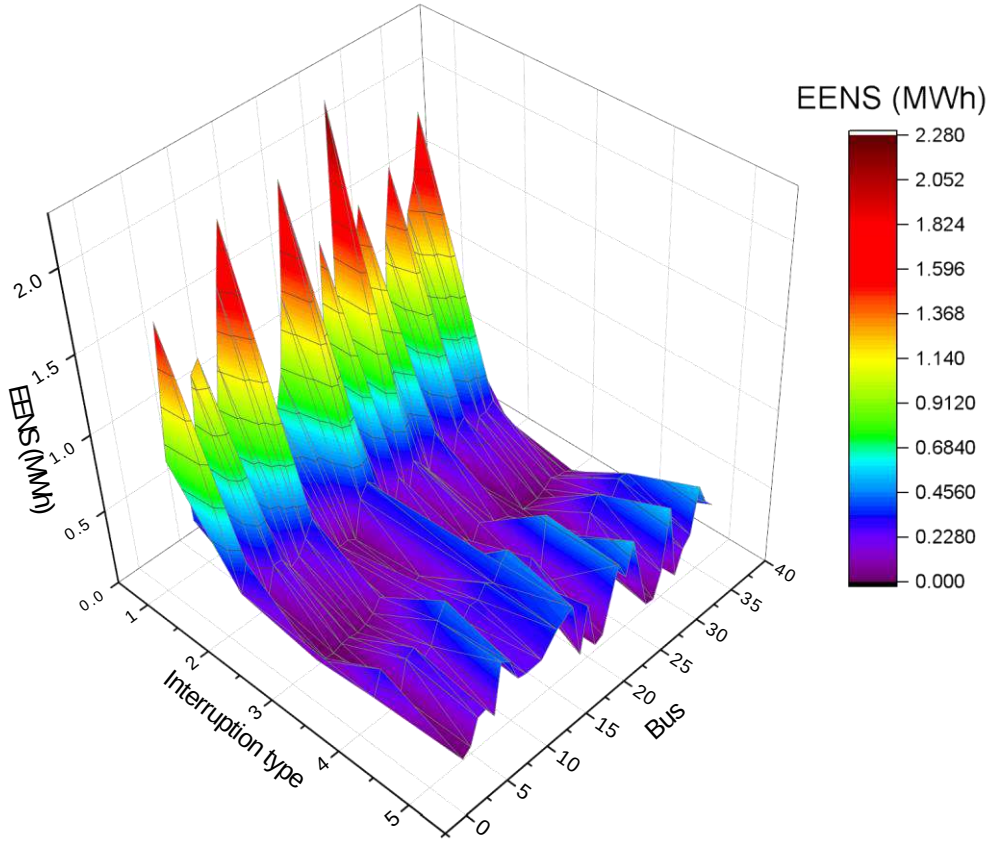
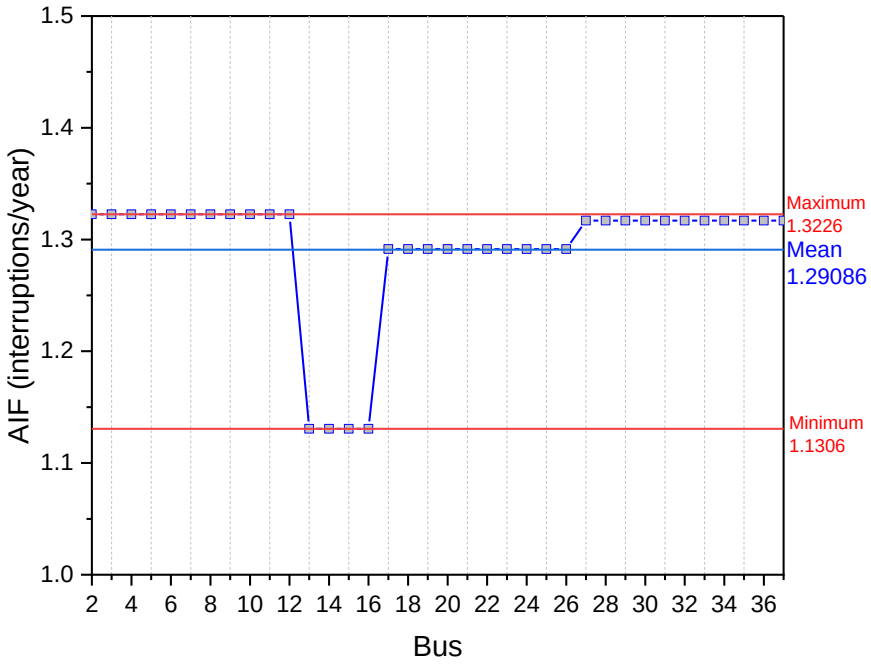
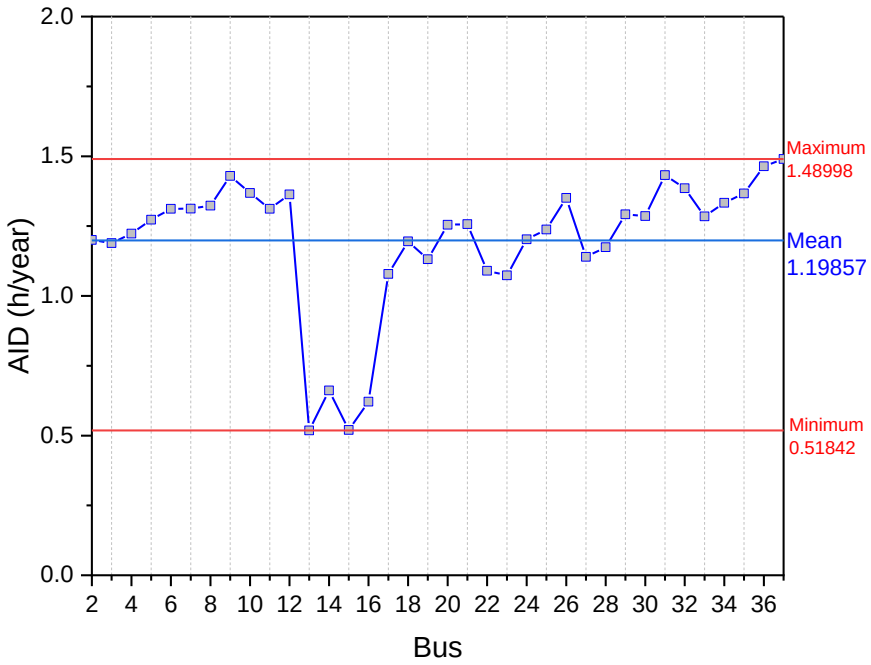


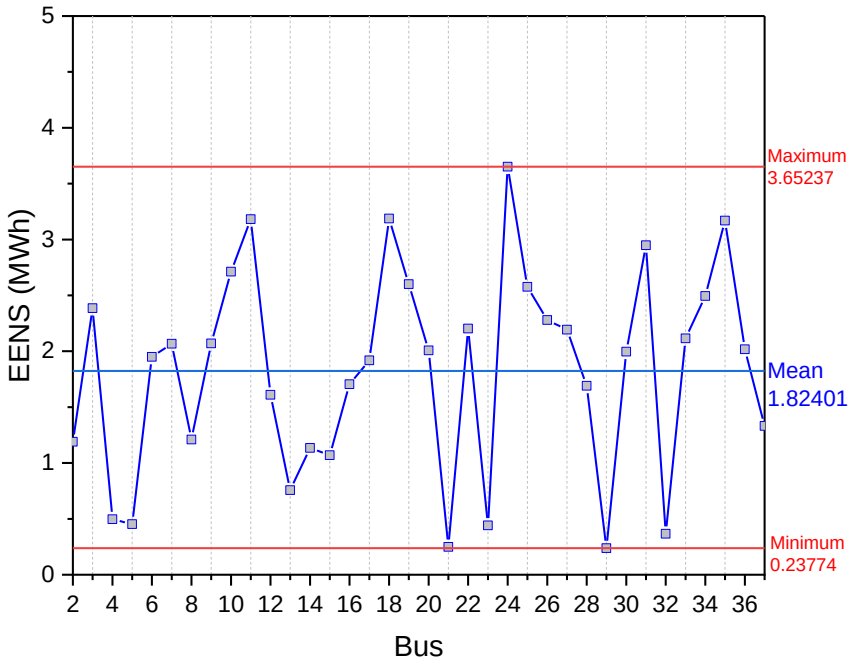
Figure 51. Nodal-oriented EENS for 37-node test system per interruption types


AIF (interruptions/year)
Bus
Maximum
1.3226
Mean
1.29086
Minimum
1.1306

(a)


AID (h/year)
Bus
Maximum
1.48998
Mean
1.19857
Minimum
0.51842

(b)



(c)

Figure 52. Nodal-oriented results of resiliency measures for the 37-node test system: (a) AIF, (b) AID, and (d) EENS

Moreover, the proposed evaluation model's effectiveness and efficiency can be seen in Table 8 when compared to the two models introduced in past studies. According to the proposed model, all interruptions of types 1 to 5 can be calculated in a shorter computing time than the models presented in [91] and [92]. A further benefit of our model is that it has no infeasible cases, which indicates that it is effective when used in resilience-driven studies. For instance, the proposed model took 0.41 seconds to calculate 5 types of interruptions. In contrast, the two references took 0.56 and 0.75 seconds, respectively to calculate just the interruption type 3. Additionally, our model provides more accurate results than the two references, considering the more realistic conditions after occurring an extreme event. This means that it can be applied to a wide range of resilience-driven applications, such as providing more reliable data for decision-making and helping to design more resilient systems.

Table 8. Number of infeasible cases and CPU time of different models (IEEE 37-node test system)

Model	Av. CPU time (sec)	Infeasible case/10000	Interruption type
Proposed model	0.41	0	1-5
[91]	0.56	212	3
[92]	0.75	272	3

4.4.6.2 Resilience-driven infrastructure planning-line hardening case

For the application, we entered the proposed metrics obtained from the evaluation model based on linear programming into the two-stage stochastic optimization problem of the planning. All lines are considered candidates for hardening, costing $5924/pole.

Load shedding has a base cost of $14/kWh multiplied by its importance factor. In addition, a base cost of $2000 per hour is assumed for line repairs. In this study, 50 damage line scenario samples with the same probability have been used. Table 9 presents the results of planning for different hardening budget constraints. This table includes resilience indicators, hardened lines, and average operating costs. A typhoon rate of two per year is assumed. The results for the base case, i.e., no hardening, are given in row one. Comparing the results of this mode with other modes shows how optimal hardening of the line can affect the network's performance function. Using a budget allocation of $500,000 for line hardening, the EENS shows a decrease of approximately 15.7%, and the average costs due to storms have decreased by up to 15.4%.

Table 9. Optimal results of line hardening plans in different budget limits for 37-node test system.

SAIFI (interruptions/year)	SAIDI (h/year)	EENS (MWh/year)	Line hardened	max budget ($)	expected cost ($/year)
1.307	2.212	118.425	-	0	1372235.105
1.255	1.894	99.789	3-4,17-18,27-29	500000	1160208.437
1.238	1.750	92.137	1-13,17-18,27-28,27-29	750000	1091774.152
1.225	1.601	83.524	17-18,22-25,27-28,27-29,33-35	1000000	1040158.259

4.4.7 User Interface

An overview of the proposed optimization model is outlined in Fig.53.

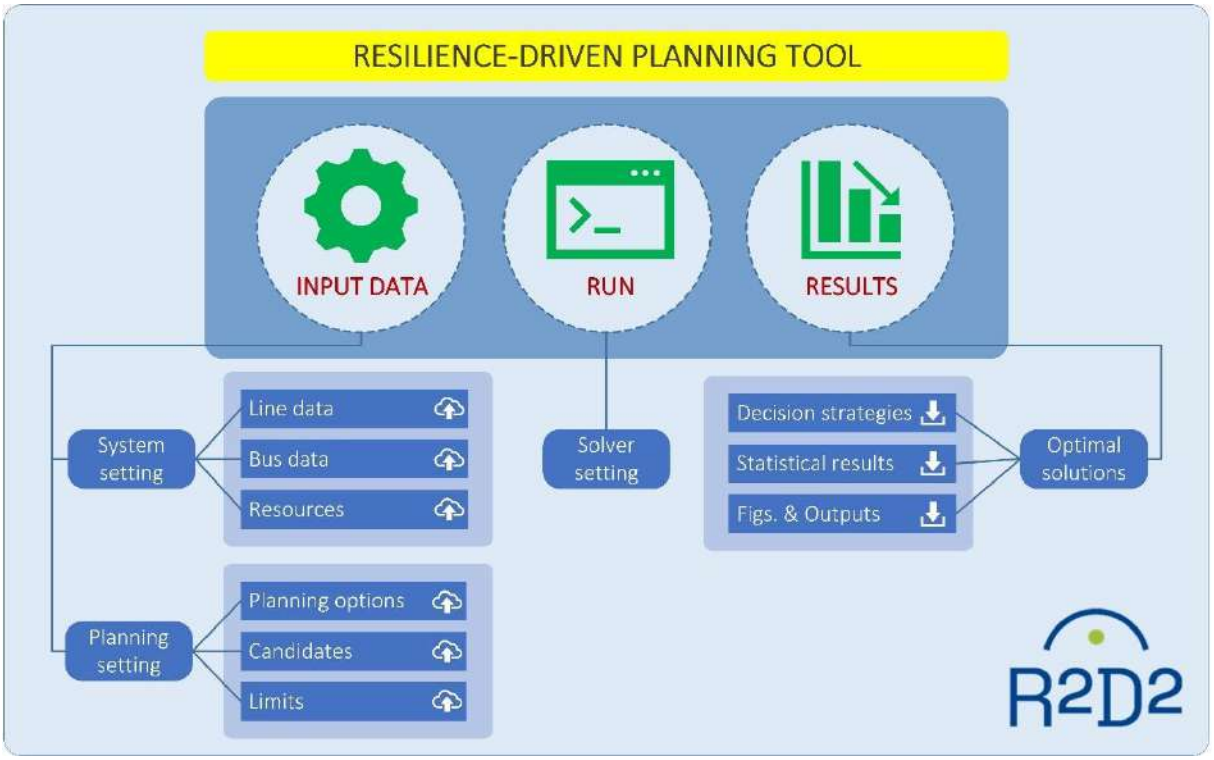


Figure 53. An overview of resilience-driven investment planning tool

4.4.8 Resources

Optimization problems have been simulated using CPLEX [93] and General Algebraic Modelling Language (GAMS) [94] on a mid-range laptop with an Intel Core i3-1115G4 processor at 3 GHz and 4 GB of RAM.

4.4.9 Post-disruption distribution system operation and restoration strategy based on flexible Microgrid formation and scheduling

4.4.9.1 Internal Architecture of the tool

To reduce service interruption costs and support fundamental facilities in a distribution system subject to catastrophic failures, a pragmatic and effective way is to separate the system into multiple microgrids to maintain the electrical connection between distributed generators and critical loads. Forming microgrids is a dynamic process requiring a set of sequential switch operations to develop and extend the faulted distribution system. Subsequently, the formed microgrids should be sustainably scheduled to energize as many loads as possible. In the microgrid scheduling scheme, a key task is to handle the stochastic power of intermittent generators and loads in a robust and non-conservative manner to achieve a reasonable trade-off between system security and outage cost reduction. While the microgrids are operating, a tailored restoration scheme should be implemented to clear the existing faults and restore the system back to the normal operating state. During the restoration process, the repair crews should be dispatched in coordination with load pick to reduce system interruption time and accelerate load energization.

Considering the potential strategies (microgrid formation, scheduling, and restoration) for distribution system resilience enhancement, this tool aims to provide an integrated operation and restoration solution for distribution systems subject to catastrophic events, including flexible microgrid formation, sustainable microgrid scheduling, and efficient restoration. By employing this tool in post-disruption distribution systems, end users can achieve:

1) Service interruption cost reduction by responsive microgrid formation that provides emergency support to critical loads using limited distributed energy sources;

2) Autonomous post-disruption system operation by sustainable microgrid scheduling considering source-load uncertainties;

3) Efficient system restoration by coordinated repair crew dispatch and frequency-constrained cold load pickup.

In order to achieve these goals, the following submodules have been developed:

1) Flexible microgrid formation submodule: This submodule provides the optimal and final microgrid topology to be formed as well as a set of sequential switch operations required to develop the faulted system to the desirable microgrids. After a catastrophic event that leads to multiple faults in the distribution system, the protection system is triggered to prevent the faults from spreading, resulting in only a small part of the system operating. To extend and interconnect the initial subsystems, the proposed flexible microgrid formation submodule is two-stage. The first stage determines the final and optimal microgrid topology to be formed, and the second stage searches for a set of sequential switch operations toward the desirable microgrids. In the first stage, available DGs are flexibly allocated into microgrids with the objective of maximizing energized loads, and each microgrid is required to be operated radially for protection coordination and short current reduction. The switch operations provided by the second stage are frequency-aware, indicating that the frequency dynamics are calculated and constrained in each switch operation.

2) Sustainable microgrid scheduling submodule: After the microgrids are formed, it is crucial to schedule the microgrid in a sustainable manner to reduce affected customers and avoid potential operational failures. With the increasing penetration of renewable energy sources into the distribution system, power generation manifests high stochasticity and intermittency. Besides, the load power demand is uncertain due to the intrinsic stochasticity of customers' behaviors. The source-load stochasticity requires a robust microgrid scheduling scheme to balance the state fluctuation in the distribution system. A robust microgrid scheduling scheme considering the source-load stochasticity is developed. The uncertain power of DGs and loads is formulated with the joint chance constraint to develop a non-conservative scheduling scheme that guarantees the overall violation of system states under a desirable probability. Furthermore, the proposed scheduling scheme is implemented with model predictive control to provide real-time dispatch values for DGs and loads in the distribution system.

3) Dynamic system restoration submodule: While the formed microgrids are sustainably operating, the existing faults should be cleared in order to restore the faulted distribution system back to normal operation. A dynamic distribution system restoration strategy considering the coordination between repair crew dispatch and cold load pickup is developed. The repair crew dispatch is formulated with chance constraints to incorporate the stochastic repair time, which is updated dynamically according to the fault knowledge acquisition. Then the repair crew dispatch is implemented with the model predictive control

to restore the faulted distribution system step by step. After a fault is cleared, some unrecoverable areas can be energized, indicating that load pickups can be conducted to reduce outage costs. However, the restoration process for catastrophic events normally lasts for a long period, e.g., hours or even days, so the cold load effect should be considered to provide a safe operation. By modelling the cold load pickup power, this submodule calculates the frequency dynamics subject to a load pickup, i.e., the rate of change of frequency, frequency nadir, and steady-state frequency. The load pickup decisions provided by this submodule are under safe frequency conditions, i.e., the rate of change of frequency, frequency nadir, and steady-state frequency are maintained under pre-defined limits.

The internal collaboration of the three developed submodules and their external requirements are depicted in Fig.54. As shown, the tool requires input data from the C3PO database for developing the mathematical model. These data include the distribution system's initial operating state after the occurrence of faults, historical load demands and generator outputs for modelling their stochasticity, repair resources (e.g., location and number of depots and crews), and frequency response parameters of generators for formulating the transient frequency variation. Additionally, the tool receives outage information (location of faults) from Use Case 36 when faults occur, triggering the execution of the flexible microgrid formation submodule. By employing this submodule, microgrids are formed by two stages, i.e., the first-stage topology determination provides the optimal and final topology of microgrids to be formed, and the second-stage switch operation provides the switching sequence to drive the faulted system to the desirable microgrids. After microgrids are successfully formed, their boundaries and the status of the electric components are used for making decisions for the subsequent microgrid scheduling and system restoration schemes. On this basis, the sustainable microgrid scheduling submodule provides a robust scheduling scheme against the stochastic and time-varying load demands and generator outputs. Mathematically, the stochasticity is described by joint chance constraints to reflect the overall violation of system states under a desirable probability. While the formed microgrids are sustainably functioning, the dynamic system restoration submodule is executed, based on the microgrid topology provided by the flexible microgrid formation submodule and the system operating state provided by the sustainable microgrid scheduling submodule. The dynamic system restoration submodule coordinates the repair crew dispatch and cold load pickup in the post-disruption distribution system. Specifically, repair crews are dispatched to the faults resulting in the maximum restored load capacity, and the removal of a fault enables to pick up cold loads separated by the fault. The repair crew dispatch and cold load pickup interact with each other by sending out a fault clearance signal and updating system states. The restoration results are fed back to the sustainable microgrid scheduling submodule to indicate the extended scale of microgrids, based on which the scheduling scheme is updated.

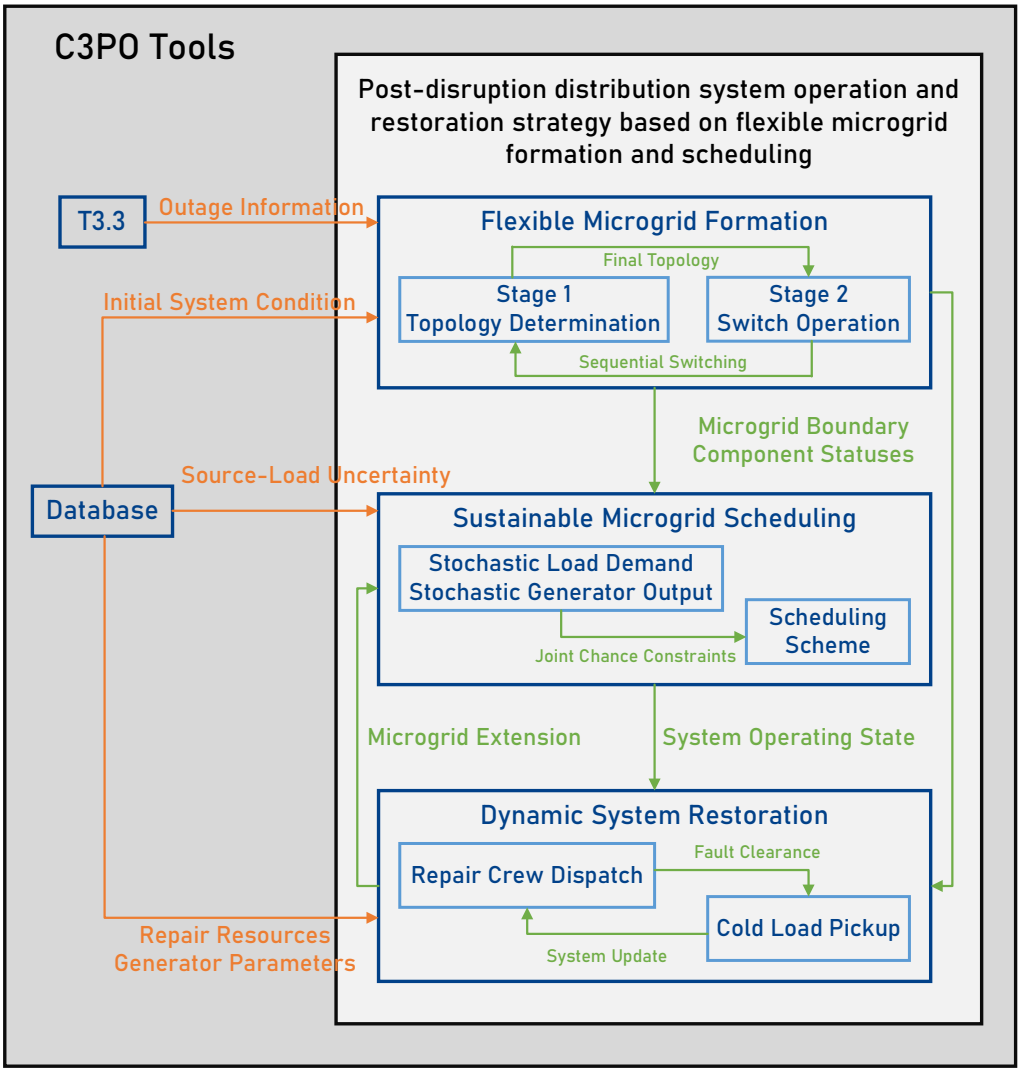


Figure 54. Architecture of the developed tool

This tool is developed as an off-line simulation measure that helps distribution system operators make decisions under catastrophic events, by providing an integrated distribution system resilience-enhancing solution that includes flexible microgrid formation, sustainable microgrid scheduling, and dynamic system restoration. As mentioned, this tool will receive outage information (location of extreme-weather-event-induced outages) as inputs from the advanced event simulator of T3.3.1, triggering the execution of the flexible microgrid formation submodule.

4.4.9.2 User Interface

This tool will deliver a relevant report to the distribution system operators, including simulation results of microgrid formation, microgrid scheduling, and system restoration in the Xanthi distribution system pilot cite to demonstrate the resilience-enhancing effect of the developed tool. As an early example of the final deliverable, the user interface of this tool will be illustrated based on a real-world 136-node test feeder.

The user interface initially shows the network topology of the target distribution system. For example, Fig.55 depicts the normal operation of the 136-node distribution system, where the substation is located at node 1, and CLs and DGs are marked as triangles and rectangles, respectively. The blue colour indicates the energization of electric components (nodes and branches).

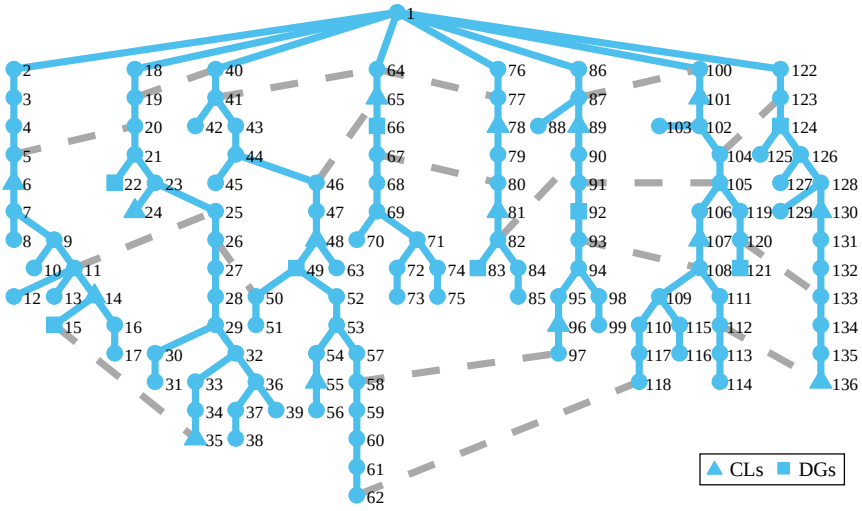


Figure 55. Normal operation of the 136-node distribution system

The initial fault condition is also given after a catastrophic event hits the system. Fig.56 depicts the operating parts (namely min-MGs) of the 136-node distribution system with the loss of substation and multiple internal faults.

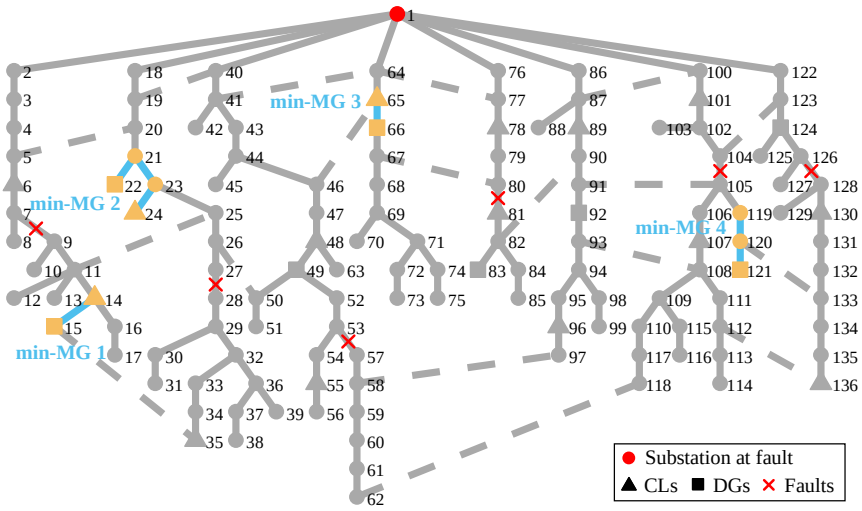


Figure 56. Initial fault condition of the 136-node distribution system

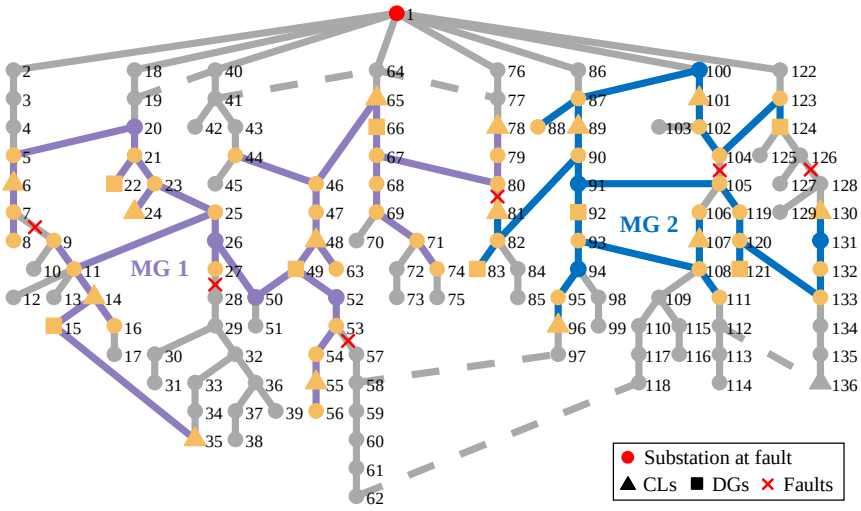


Figure 57. Final topology of microgrids

Then the flexible microgrid formation submodule is employed to provide the optimal microgrid topology and the switching operations required to form the desirable microgrids. The final topology of microgrids is shown in Fig.57, indicating that 2 microgrids are waiting to be formed, and their energized nodes and branches are indicated by purple and blue, respectively. The nodes with load pickup are marked as yellow. Microgrid 1 contains min-MGs 1, 2, and 3, and microgrid 2 contains min-MG 4 only, indicating that the interconnection of different min-MGs should be considered while forming microgrid 1. Fig.58 details the step-by-step switch operations to form microgrid and microgrid 2. Before each step, the already energized nodes and branches are depicted in blue, and the served loads are depicted in yellow. Every two steps are shown together in Fig. 59. The switch operations to form microgrid 1 are:

1) At the 1st step, extend min-MG 1 and pick up CL 35 and normal load 9; Extend min-MG 2 and pick up CLs 6 and 55 and normal loads 53 and 56; Extend min-MG 3 and pick up CL 78 and normal load 80. All the 3 min-MGs are energized separately.

2) At the 2nd step, interconnect min-MGs 1 and 2 on synchronization branch (11, 25) (it is assumed that the interconnection condition like human resources and equipment support is satisfied). Then extend the interconnected min-MG (1 and 2) and pick up CL 48 and normal loads 27 54. As for min-MG 3, nodes 68, 69, and 71 are energized, and normal loads 67, 69, and 71 are picked up.

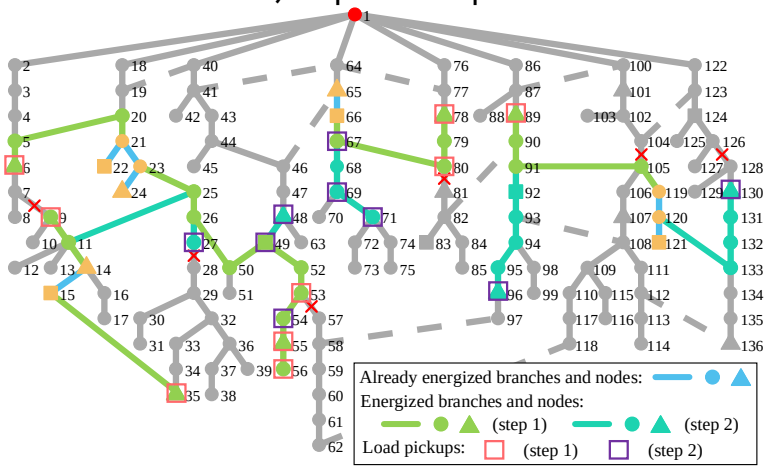
3) At the 3rd step, extend the interconnected min-MG (1 and 2) and pick up normal loads 5, 25, 44, 46, and 47, and extend min-MG 3 and pick up normal loads 68, 74, and 79.

4) At the 4th step, interconnect the preciously connected min-MG (1 and 2) and min-MG 3 on synchronization branch (46, 65). By now, all 3 initial min-MG have been interconnected. Then extend the interconnected min-MG (1, 2, and 3) and pick up normal loads 7, 8, 16, 63. The desirable topology of microgrid 1 has been reached, and the switch operations to form microgrid 1 have finished.

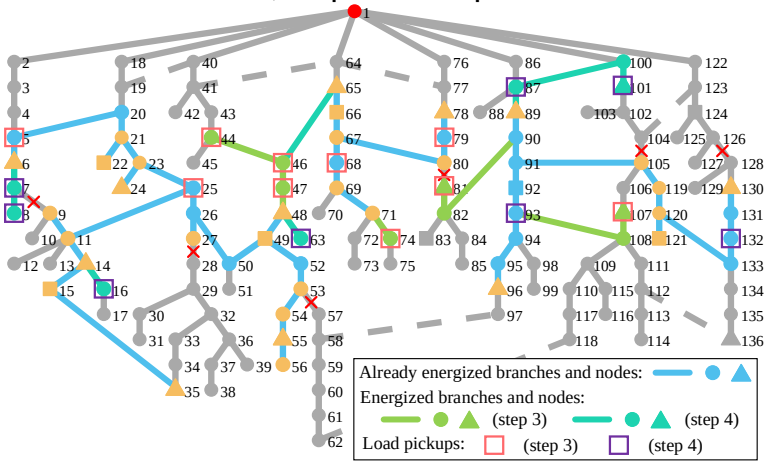
Compared to microgrid 1, the switch operations to form microgrid 2 are more straightforward, as it contains only one min-MG, and no interconnection operation is required. However, due to the low inertia, more switch operations are needed to form microgrid 2. Based on the employed control schemes of DGs, microgrid 2's inertia is provided by DG 121 only, which significantly limits the load pickup at each step by the fast-changing frequency

dynamics. The maximum load pickup power is 477.8 kW in microgrid 2, while it is 996.1 kW after min- microgrids 1 and 2 are interconnected in microgrid 1. The low inertia in microgrid 2 requires a prolonged witching scheme with a smaller amount of load pickup at each step. Since no interconnection is required while forming microgrid 2, its switch operations are straightforward and thus not listed in detail like that of microgrid 1.

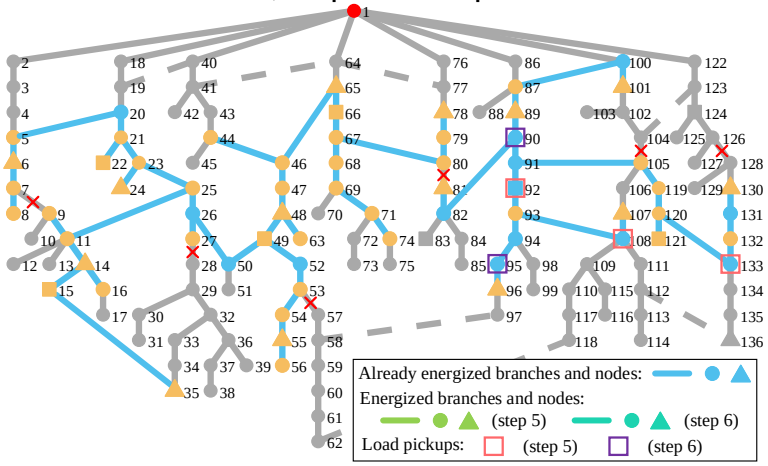
a) step 1 and step 2



b) step 3 and step 4



c) step 5 and step 6



d) step 7 and step 8

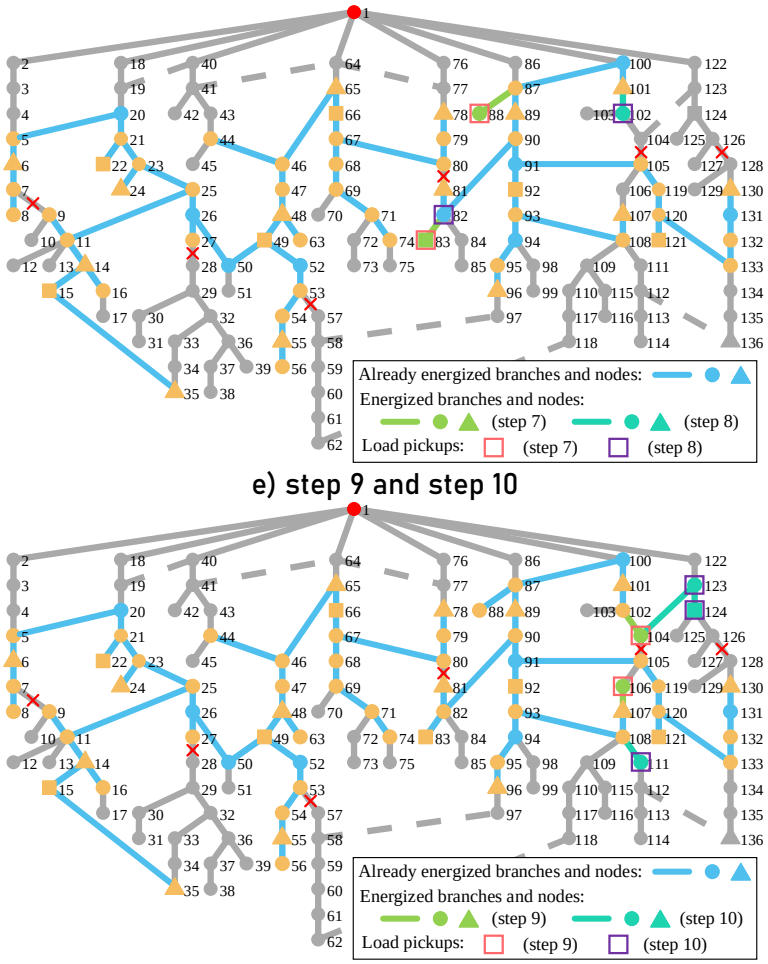


Figure 58. Sequential switch operations toward the determined 2 microgrids

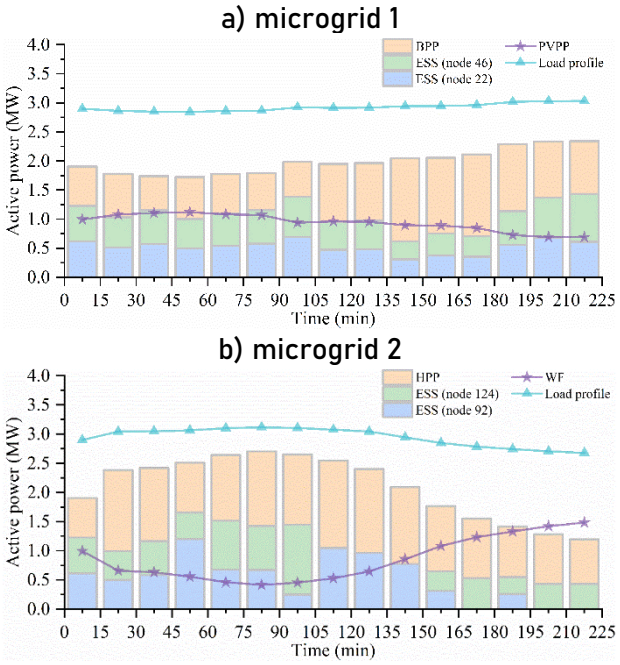


Figure 59. Active power scheduling scheme of microgrids 1 and 2

After microgrids 1 and 2 are successfully formed, the sustainable microgrid scheduling submodule is executed, and the scheduling scheme is shown in Fig. 60. The first 15-time steps (0-225 min) are depicted. As shown, the fluctuating power from renewable energy sources is well addressed by looking ahead a few time steps when making decisions for the current time step in the model predictive control implementation. The peak-valley differences of loads and DGs in microgrid 1 are respectively 0.19 MW and 0.43 MW. The respective differences for microgrid 2 are 0.45 MW and 1.1 MW. This indicates that only approximately 40% of the DG power fluctuation is conveyed to loads.

To demonstrate the effect of the dynamic system restoration submodule, a more severe fault condition is considered, as shown in Fig. 61. The loss of the substation and 13 permanent branch faults separate the system into 6 microgrids. There are 3 repair crews, and their dispatch scheme is detailed in Table 10. It is indicated to restore at priority the faulted branches adjacent to CLs, e.g., (87, 89), (5, 6), and (128, 130), while the faulted branches located near the end of the system, e.g., (11, 13), (34, 35), and (134, 135), should be restored at a later stage.

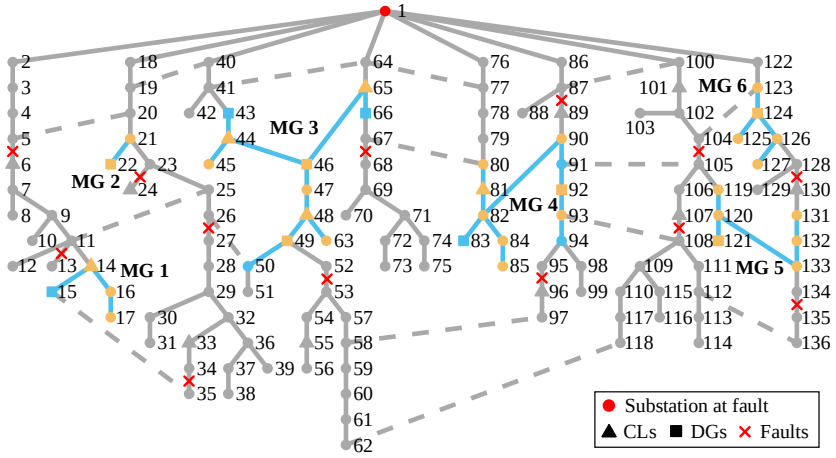


Figure 60. Active power scheduling scheme of microgrids 1 and 2

Table 10. Repair crew dispatch scheme for the faulted 136-node distribution system

Restoration time instant (min)	Faulted branches	Repair crew	Restoration time instant (min)	Faulted branches	Repair Crew
26	(87, 89)	2	38	(5, 6)	3
46	(128, 130)	1	54	(104, 105)	2
65	(23, 24)	3	78	(107, 108)	1
83	(52, 53)	2	98	(67, 68)	3
109	(26, 27)	2	117	(95, 96)	1
133	(11, 13)	3	149	(134, 135)	2
154	(34, 35)	1			

As an example, the cold load pickups during 26-86 min in microgrids 4, 5, and 6 are shown in Fig. 63. At the 26th min, branch (87, 89) is restored and energized, enabling the CLs at node 101 and normal loads at node 87 to be picked up. When the frequency is restored 10 mins later at the 36th min, the loads at node 102 are picked up. Although the loads at nodes 88 and 89 could be energized by microgrid 4, it is unsafe to restore them due to the low inertia of microgrid 4. So, no loads are restored in microgrid 4 at the 46th min. At the same time,

branch (128, 130) is restored. Then microgrid 5 and microgrid 6 are interconnected, and the loads at node 129 are picked up. Later at the 56th min after branch (104, 105) is fixed, microgrid 4 is connected to the interconnected microgrid 5 and microgrid 6 through the path 102-104-105-119. At this time, the CLs at node 89 are picked up in the interconnected system with inertia provision from DGs 83, 121, and 124. Subsequently, the CLs at node 130 are restored at the 66th min. The large loads at node 99 are still not allowed to be energized, so no loads are picked up at the 76th min. At the 83rd min when a new branch (107, 108) is in service, the loads at nodes 107 and 108 are picked up. The following load pickups are similar. The frequency dynamics of 3 cold load pickups at the 26th, 36th, and 56th min are depicted in Fig.62. It indicates that the primary factor limiting the amount of cold load pickup in microgrids is the RoCoF, which can easily violate the preset limit due to low inertia. This underlines that cold load pickup in low-inertia microgrids should be conducted carefully to avoid drastic frequency drops. In addition, it is safer to restore large loads after interconnecting more microgrids. For example, picking up 458.3 kW loads is allowed at the 56th min when microgrid 4, microgrid 5, and microgrid 6 are interconnected. In contrast, the allowable load pickup amount before the interconnection is only 141.2 kW.

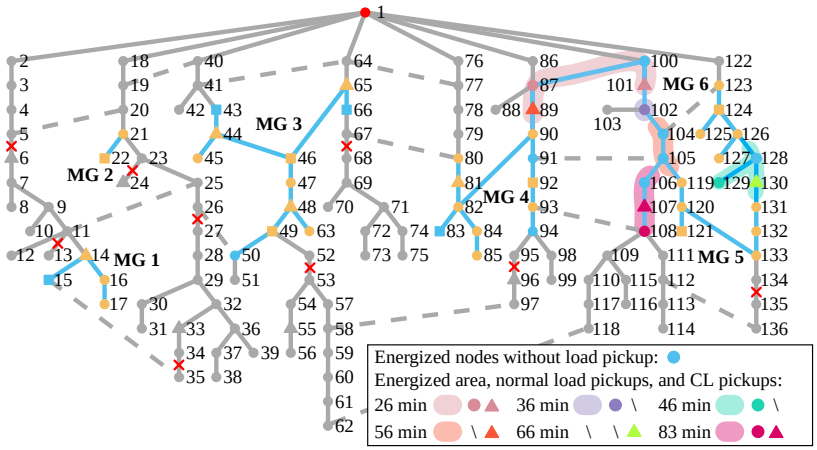


Figure 61. The cold load pickups related to microgrids 4, 5, and 6 (26-86 min)

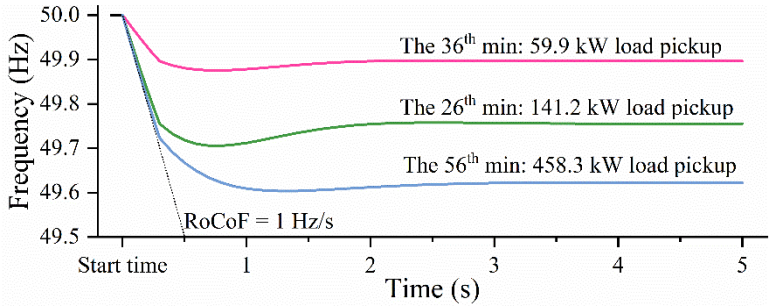


Figure 62. Frequency drops of 3 cold load pickups at the 26th, 36th, and 56th min

4.4.9.3 Resources

This tool is developed in the MATLAB environment with the SIMULINK toolbox installed, and the external toolboxes, including MATPOWER, YALMIP and GUROBI, are required.

4.5 OPERATION AND PLANNING OF ADVANCED MULTI-ENERGY MICROGRIDS FOR ENHANCEMENT OF RESILIENCE (TASK 3.5)

Extreme weather events, characterised by their HILF, can disrupt system components and cause severe damage. The increasing interdependencies between different energy sectors, e.g., power, gas, and heat, further exacerbate the consequences of HILF events [95]. To tackle these challenges, the concept of resilience has been adopted in the field of integrated energy systems [96]. Considering the potentially serious disruptions, the primary objective of a resilient energy system during extreme events is to maintain the uninterrupted supply of essential loads across different energy sectors, rendering a system-wise load restoration problem [97].

The energy industry is rapidly transforming due to decentralization, decarbonization, and digitization, which challenge the traditional top-down approach to energy systems. MGs [79], as localized small energy systems, are being integrated into energy systems to coordinate various small-sized energy sources effectively. MGs have advanced control capabilities that, through smart control of installed DERs and efficient energy exchanges, offer a promising solution to enhance resilience and facilitate the transition to a low-carbon energy system [80].

4.5.1 Internal Architecture of the tool

The aim of the tool is to develop an optimal planning and operation strategy of an advanced microgrid for load restorations, involving the pre-positioning as well as the routing and scheduling of MPSs in a coupled power-transport network. As a result, the objectives are reducing load shedding costs and enhancing the system overall resilience under the context of microgrids.

- Detailed architecture of the tool

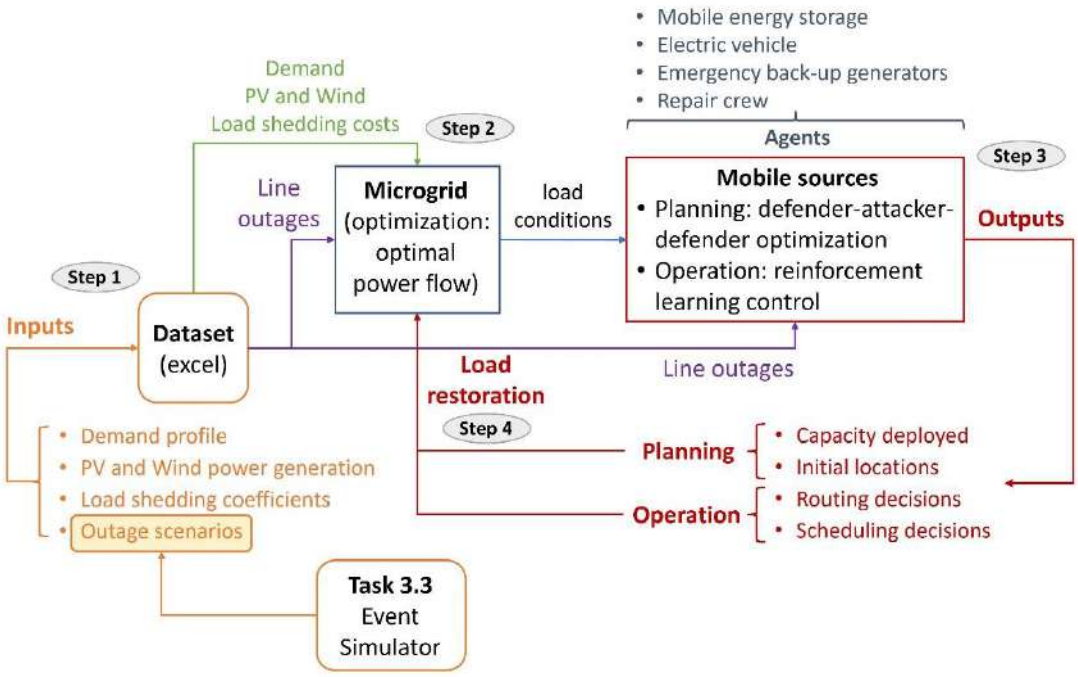


Figure 63. The architecture of the tool for Task 3.5. (outages from T3.3)

- Description of the components of the tool

The tool includes four steps, which can be described as below:

Step 1. Prepare dataset, including demand profiles, renewable power generation, load shedding cost coefficients to identify essential and non-essential loads, and potential outage scenarios within the microgrid.

Step 2. The microgrid central controller (MGCC) receives the datasets and optimizes the power dispatches, load shedding quantities, and optimal power flows within the microgrid.

Step 3. Plan and operate the candidate MPSs to enhance microgrid resilience after observing the load conditions and outage scenarios.

Step 4. The planned and operated outputs (i.e., planned capacity, initial locations, routing decisions, and scheduling decisions) will be sent back to the microgrid to evaluate the load restoration process and calculate the load shedding cost.

- The models to be used for the tool development

In this section, the model descriptions of microgrids and MPSs are provided.

1. Microgrid

This task focuses on a smart microgrid model, which is a localized, small-scale energy system that can generate, store, and distribute electricity to a specific area or community, typically consisting of multiple buildings or facilities [98]. Unlike traditional centralized power grids that rely on a single power source and large-scale distribution networks, microgrids operate on a smaller and more decentralized scale [99]. Here are the key characteristics and components of the considered microgrid in this task, of which its structure is illustrated in Fig.64.

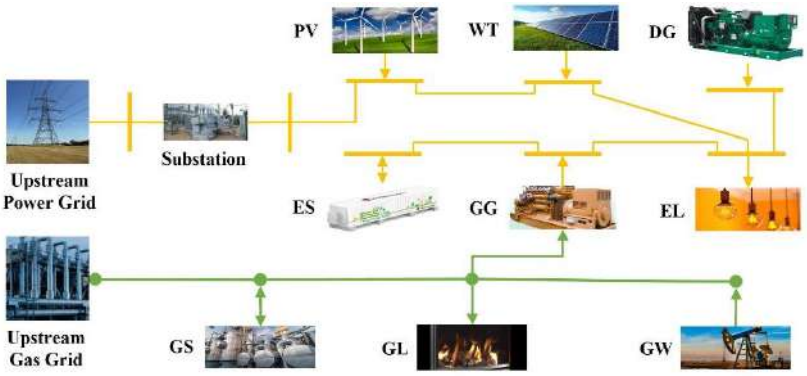


Figure 64. Structure of proposed smart microgrid

Local generation: Microgrids often include on-site power generation sources, such as solar panels, wind turbines, natural gas generators, or combined heat and power (CHP) systems. These local generators can produce electricity independently of the main grid.

Energy storage: Microgrids may incorporate energy storage systems, such as batteries, to store excess energy generated during periods of low demand and release it when demand is high or when the local generation sources are not producing power.

Demand side response: Microgrids can integrate a variety of demand-side management strategies, to optimize energy use while maintain the energy supplies of critical loads.

Control systems: Microgrids are equipped with advanced control systems (e.g., microgrid central controller - MGCC) that monitor and manage the flow of electricity within the network. These control systems can optimize energy use, balance supply and demand, and ensure grid stability.

Grid connectivity: While microgrids are designed to operate autonomously, they can also be connected to the main power grid. This connectivity allows microgrids to import or export electricity as needed. During emergencies or grid outages, microgrids can disconnect from the main grid and operate independently, providing a source of backup power.

Resilience and reliability: Microgrids are known for their resilience and reliability. They are capable of "islanding", which means they can continue to supply power to their local area even when the main grid experiences disruptions or failures.

2. Networked-Microgrids

We focus on the coordination problem of an NMG cluster involving multi-interconnected MGs towards overall resilience enhancement, as illustrated in Fig. 65. In general, these MGs can be connected with each other and regulate their own energy resources for power sharing to facilitate load restoration process after the major power outages in the distribution network.

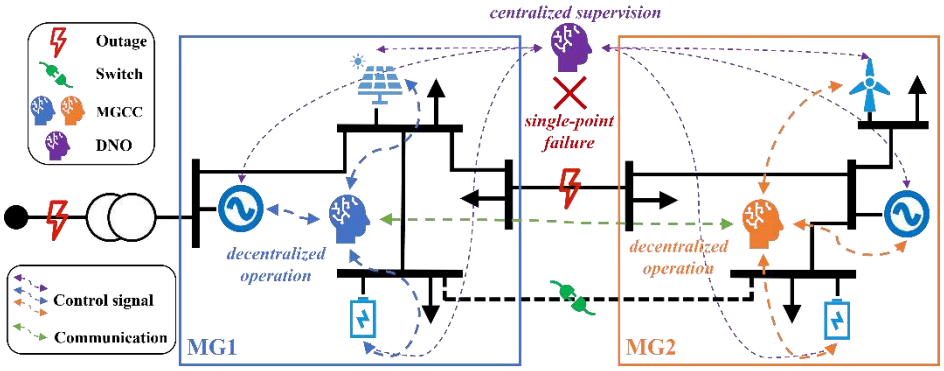


Figure 65. Scheme of NMGs towards resilience enhancement. It also illustrates the transition from centralized supervision (purple) via DNO to decentralized operation (blue and orange) via NMGs

NMGs can be implemented to enable additional flexibility for resilient operations by cooperatively sharing extra power resources [80]. Furthermore, each MG can have a heterogeneous topological and operational design that is more flexible to target local power supplies. More importantly, MGs operate in a decentralized manner that can prevent the system from a single-point failure. Finally, these MGs operate in parallel, which can expedite the restoration process. The proposed framework of NMGs for resilience enhancement is illustrated in Fig.65. After the power outages (e.g., main connection, distribution line) and also the single-point failure of centralized supervision, each MG is equipped with a MGCC that can regulate the power dispatches of controllable resources (e.g., PVs, WTs, DGs, and ESs) inside its own region, utilize tie-lines or smart switches, and then manage power exchanges with each other. In this context, these two MGs have their own controllability and can operate within a decentralized framework without central commands from DNO, enabling a fast response time. As such, the overall resilience performance can be improved significantly.

3. Mobile Power Sources and Repair Crews

Along with other resources within the microgrid, the massive number of mobile resources, such as MEGs, mobile energy systems (MESs), private electrical vehicles and public electric buses (EVs), and RCs, can be routed during extreme events to balance the critical load, due to their significant advantages related to mobility and flexibility compared to static resources.

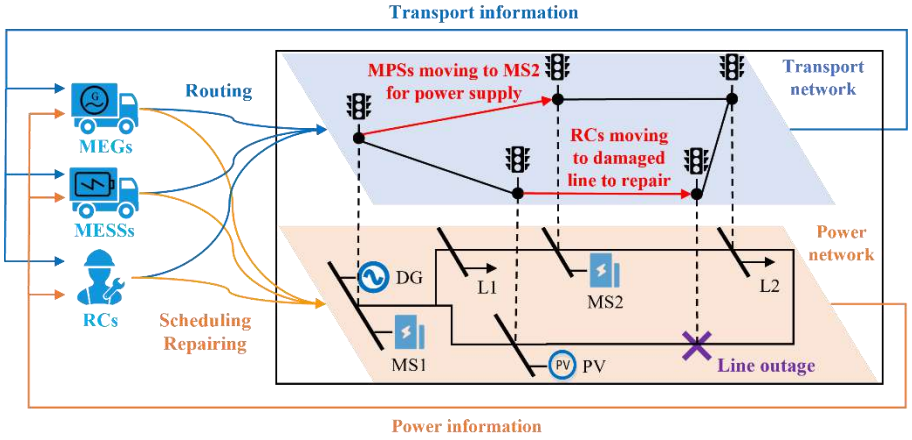


Figure 66. Routing and scheduling behaviours of mobile sources in a power-transport network for resilience enhancement

This task focuses on the resilience-driven coordinated dispatch problem of MPSs and RCs within a power-transport network including both routing and scheduling/repairing behaviours of these mobile sources, as illustrated in Fig.66. In general, electric components (e.g., buses and lines) in the power network are located on different transport nodes, while MPSs and RCs can move upon the transport network and choose to connect with their corresponding candidate nodes [100]. Specifically, we consider MEGs and MESSs as two types of MPSs that can choose to connect with the candidate nodes, e.g., MESS stations (MSs) [101]. Following [102], this task assumes that both MESSs and MEGs have black-start capability during the load restoration process. The role difference between MESSs and MEGs is that MESSs can charge power at one location with sufficient power supply and then discharge power at another location suffering load shedding, while MEGs can only provide power supply for the power network. In other words, MESSs play a role similar to demand-side response, whereas MEGs play a role similar to traditional generators but with mobility features. Regarding RCs, the candidate nodes are the initial depots and the locations of line outages. Inside the power network, static DERs, such as photovoltaics (PVs) and diesel generators (DGs), are installed suitably. In terms of the demand side, the power system captures both essential and non-essential loads to highlight the primary objective of load restoration [103].

- Algorithms to be used for the tool development

This task develops a multi-level strategic planning model and a series of model-free smart control algorithms to optimally design and operate the decentralized mobile sources under the multi-energy microgrid concept for enhancement of resilience. Specifically, there two models:

1. **Planning Model**

The first model focuses on developing resilience-driven planning for optimal design of microgrids, which includes the sizing and pre-positioning of MPSs. The objective is to develop a three-level DAD model for optimal sizing and pre-positioning of MPSs in a microgrid. The upper-level problem will aim to optimize the sizing results under normal operation, while the middle-level problem and lower-level problem will be merged as a subproblem to select the contingencies that can cause the most severe damage. The linearized AC power flow will be used to model microgrid operations and capture technical constraints related to voltage and power losses. Incorporation of uncertainties related to renewable energy sources and load profiles will be done using stochastic programming.

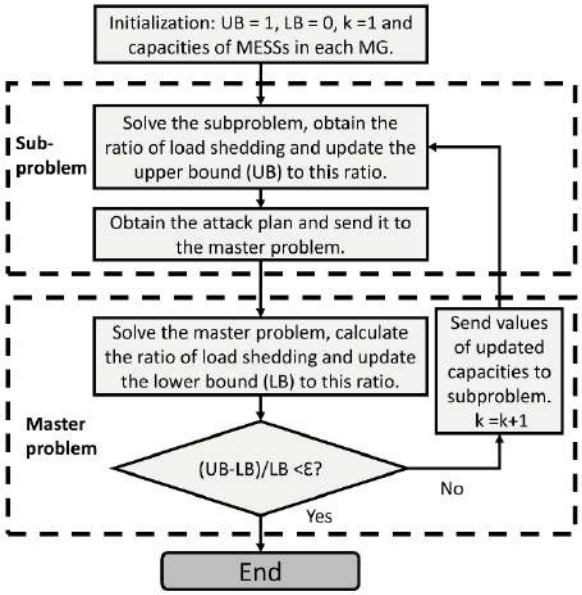


Figure 67. Resilience-driven planning strategies for the optimal sizing of MPSs in the context of microgrids

To consider the trade-off between total system cost and resilience (e.g., total load shedding), the objective function at the planning level should include MPS allocation cost and operational cost in the MG. To solve the suggested three-level optimization problem, the first step is to merge the middle-level problem and lower-level problem into a single-level formulation, which is realized as a max–min subproblem to identify the worst-case scenario (e.g. the attack action causing most load shedding), while the upper-level problem is designed as a master problem to make decisions on MPS sizing and pre-positioning. The flowchart of the proposed three-level DAD model can be found in Fig. 67. The subproblem and the master problem will be solved via a C&CG method iteratively until convergence [104]. Note that the C&CG algorithm has been widely used to efficiently solve various mathematical models featuring robust optimization.

Additionally, both internal uncertainties and external contingencies are incorporated in the planning model. Uncertainties with renewable energy sources and load profiles are captured via a scenario-based stochastic programming approach in MG operations, while the influence of contingencies including multiple line outages are considered via the suggested DAD model. Specifically, the subproblem can produce different attack actions relating to different line outages and select the attack action that can cause the largest load shedding cost. After obtaining the selected attack action, the master problem will update the current optimal sizing and pre-positioning results against this attack.

2. **Operation Model**

The second model focuses on the advanced control of mobile power sources (MPSs) in the concept of the microgrids with flexible DERs and mobile sources that can significantly improve the resilience of the microgrid during extreme events through islanding schemes. In addition, some internal lines could be damaged when an outage occurs. To address the core system uncertainties and dynamics while ensuring fast response of these decentralized DERs and mobile sources, a model-free and data-driven approach called reinforcement learning (RL) [105] will be applied to deliver optimal control decisions by utilizing experiences

acquired from repeated interactions with the resilience-driven microgrid operation environment. Additionally, digitalization of district microgrids will provide unique opportunities for effective management of the energy system during extreme events by turning off non-essential demand when the network is stressed while maintaining the supply of essential demand. Specifically, the model-free and data-driven MARL method proposed in this task to solve the operation problems for NMGs and mobile sources can be detailed by the following two practical implementations:

Markov Decision Process: Reformulating the optimisation problems of NMGs and mobile sources into a Markov Decision Process (MDP) [105], where:

Agents are the microgrid central controller (MGCC) or mobile sources themselves.

Environment is everything outside the agent, such as the operation models of MGs, energy network, and transport network.

The architecture of the MDP (i.e., the dynamic interactions between the agents and the environment) is illustrated in Fig.68. These agents can sense the status of the external environment (State) and the reward of feedback (Reward), as well as learn and make decisions (Action). The decision-making function of the agents refers to making different actions according to the state of the external environment, and the learning function refers to adjusting the strategy according to the state and reward observed from the external environment.

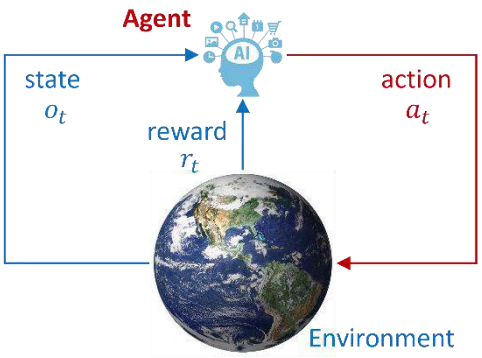


Figure 68. Markov Decision Process

In Fig.68, an agent acts within an environment by sequentially taking actions over a sequence of time steps, in order to maximize a cumulative reward. The components of a MDP can be defined as

- a state space: a collection of the environment state.
- an action space: a collection of the agent's actions.
- a control policy: a function of the agent to decide the next action according to the environmental state.
- a transition function: a dynamics distribution with conditional transition probability that satisfies the Markov property, i.e., representing the probability that the environment will change to a new state at the next time step after the agent makes an action according to the current state.
- a reward: after the agent makes an action according to the current state, the environment will give an immediate reward to the agent to represent the achievement

of the agent acquiring from the environment when making an action at the current state.

The agent's decision in terms of which action is chosen at a certain state is driven by the control policy. More specifically, the agent deploys its control policy to interact with the MDP and emits a trajectory of states, actions and rewards over the time steps. The agent starts from the perceived initial environment, then decides to take a corresponding action, the environment feeds back to the agent an instant reward and changes accordingly to the new state, and then the agent makes one action according to state, reward is obtained, and the environment is changed to the new state accordingly. This interaction can continue until the end of the episode.

Reinforcement Learning: To solve the above MDP, this task proposes a novel reinforcement learning (RL) method. In order to address the highly stochastic and dynamic energy-transportation network, RL method, as a model-free and data-driven approach, can be adopted to solve the 1) resilient energy management problems of NMGs; and 2) joint routing and scheduling problems of mobile sources, without relying on the system models. By learning the actions through extensive offline simulations with the environment, each MGCC or mobile resource agent can directly deploy the well-trained RL control policy to different state conditions in milliseconds without solving an optimization problem, which is very important to the resilient operation problem due to the demand of fast response time.

4.5.2 Data exchanges, communication with other tools

Since this tool focuses on the planning and operation of mobile sources (microgrid is only for operation), the outage scenarios after the extreme events are one of the critical inputs. In this context, this tool requires to link with **Task 3.3 "Spatial and Temporal Modelling and Quantification of Cascading Physical Events".**

Specifically, the event simulators developed in Task 3.3 will generate a series of outage scenarios, afterwards, this tool will take the outage scenarios as the inputs and make the optimal planning and operation strategies to enhance the resilience of energy supplies.

4.5.3 User Interface

The tool will be user friendly once all the software resources (next subsection) are installed. In general, the tool includes three modules:

Data inputs: all the input data can be organized into an excel file, the tool developer will provide the instructions and the examples of input data.

Optimizations: once the input data is feed into the tool, the planning and operation solutions will be obtained by the proposed algorithms.

Illustrations: all the planned and operated solutions as well as the microgrid and mobile source operations, including

1) Planning results: the planned locations and capacities of mobile sources; and
2) Operation results: the power dispatches of DERs, network power flows, routing and scheduling decisions of mobile sources, and the load restorations,

will be presented/plotted in a separated Python dashboard for analysis.

4.5.4 Resources

The tool will be implemented on the Python Programming Language. The solutions of planning model will be optimized via the **Gurobi Python Interface** [106]. The routing and scheduling behaviours of operation model will be trained using the deep neural networks via the TensorFlow Platform [107].

4.5.5 Case Studies

The case study applications are carried out in this section by analysing the operation strategies of NMGs and the dispatch behaviours of mobile sources in providing resilience enhancement under two experiment MG networks.

1. Resilience-driven Planning of Mobile Power Sources

Fig. 71 illustrates the network structure of an AC MG utilized in this paper. In the MG, conventional generators (i.e., diesel generators) are installed as conventional generation resources, while PV devices and MPSs units are deployed in the MG through power converters. Note that MESSs are connected with bus 3 as shown in Fig. 71, which is only for presentation, since the final location of each MPS will be decided via the DAD model. Additionally, MPSs employed in the model belong to utility-owned units as suggested in [108]. Data relating to load and PV profiles are extracted from [109], where load profiles in the MG are illustrated in Fig. 72. Uncertainties with load profiles and renewable energy sources are represented via 10 scenarios obtained from the stochastic programming approach.

Additionally, to capture the main focus of MGs during an extreme event (e.g., essential load restoration), the case studies presented hereafter consider the discrimination of essential and non-essential loads. As suggested in [110], around 30% of total loads in the MG is regarded as essential loads with large shedding cost, while other loads are assumed to be non-essential loads with relatively lower shedding cost. Specifically, buses 3 in the MG are assigned with essential loads (e.g., hospitals and data centres) covering 30% of the total load found in the MG, while other buses are equipped with non-essential loads (e.g., kitchen and toilet appliances) covering the rest 70% of the total load.

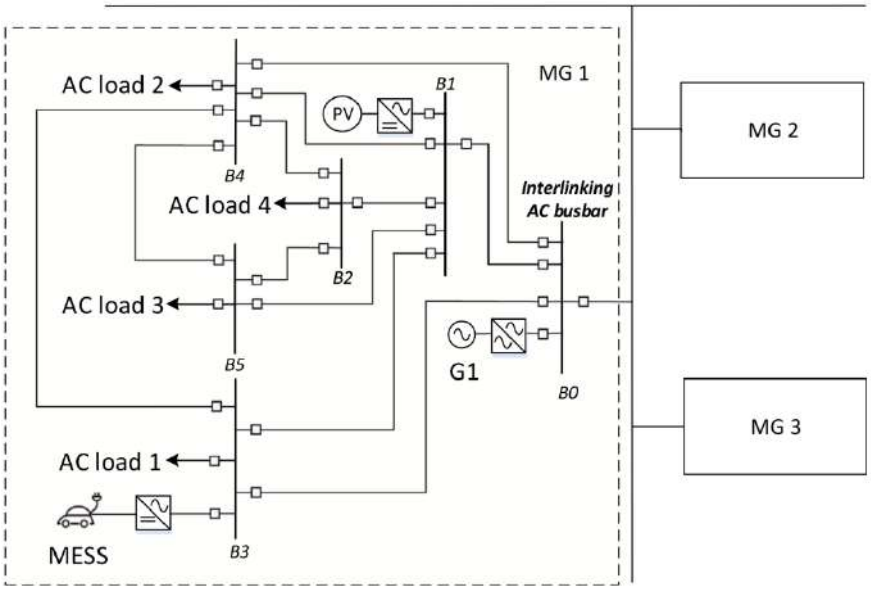


Figure 69. The MG system used in case studies

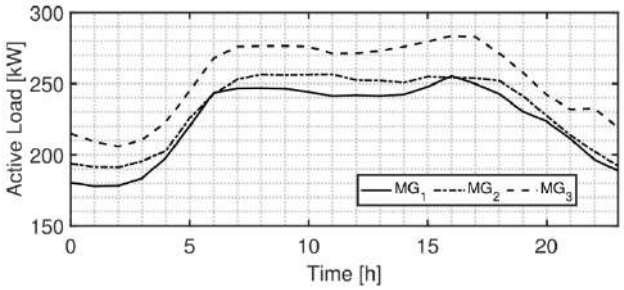


Figure 70. Data illustration of load profiles in these MGs

- **Optimal sizing and pre-positioning of MESSs**

Results on optimal sizing and pre-positioning of MESSs can be found in Table 11 under two sets of attack budgets, where AB = 6 and AB = 3 represent that the event can cause at most 6 and 3 line outages respectively. Regarding power capacities, the MESS in MG 2 obtains the largest capacity, while the MESS in MG 1 owns the smallest capacity. The reason is that the conventional generator in MG 2 has the largest rating, which requires much larger MESS capacity for more effective energy transmitting. Compared to MG 2, MG 1 has a generator with small rating and a relatively low load level, which both reduce the need for a large MESS capacity. Table 11 also shows that much larger MESS capacities are required with the increase of attack budgets from AB = 3 and AB = 6.

Regarding initial locations of MESSs, it seems that bus 3 and bus 0 in each MG are the most common chosen locations. The potential reason is that these buses are more important than other buses in each MG. For instance, bus 3 is connected with essential loads, while bus 0 is connected with the conventional generator in each MG.

Table 11. Optimal sizing and pre-positioning results of MESSs in each MG under different attack budgets

Attack budget	No. of MG	MESS capacity	Initial location
AB=6	MG1	118 kW	Bus 3
	MG2	212 kW	Bus 5
	MG3	197 kW	Bus 0
AB=3	MG1	97 kW	Bus 3
	MG2	115 kW	Bus 0
	MG3	108 kW	Bus 4

- **MESS routing and scheduling behaviours**

Behaviours of MESS routing in each MG against the worst contingency can be found in Table 12, where 'T' corresponds to transportation. It can be found that all MESSs move back and forth between bus 0 and other buses (e.g., bus 3 and bus 5) for charging and discharging. In other words, when the energy content of a MESS is low, it can move to bus 0 for charging and then travel to one bus that needs power supply. Additionally, it can be found that average traveling times of MESSs inside each MG are reduced with the increase of MESS capacities or attack budgets. In other words, MESSs with large capacities may require fewer traveling times due to the stronger ability of charging and discharging. When attack budgets are increased, the MG system tends to increase the capacity of MESSs against more severe contingency. Larger capacities allow much higher energy content and relatively longer discharging durations for load restoration, which leads to decrease of average traveling times (i.e., due to being connected to the grid).

Charging/discharging behaviours of MESSs in each MG under the worst contingency are illustrated in Fig. 73. It worth noting that the value of final energy content of each MESS equals to the initial value, which corresponds to the cycling constraint of battery units for realistic simulations. Except for the influence of severe contingencies, it can also be found that load and PV profiles have influence on charging/discharging patterns of MESSs, especially when the attack budget is low. For instance, Fig. 73(b) illustrates that all the storage devices charge during the hours of high sunshine (i.e., around 10–15 h). Additionally, MESSs charge when the load level is relatively low and discharge when the load level has significantly increased (e.g., during 5–10 h).

Table 12. MESS routing decisions inside MGs against the final worst contingency

Time (h)	AB=6			AB=3		
	MG 1	MG 2	MG 3	MG 1	MG 2	MG 3
0	3	5	0	3	0	4
1	3	T	0	3	0	T
2	T	0	0	T	0	0
3	0	0	T	0	0	0
4	0	0	5	0	T	0
5	0	0	5	0	5	0
6	T	T	5	T	5	T
7	3	4	5	5	5	3

8	3	4	T	5	5	3
9	3	4	0	5	5	3
10	3	4	0	5	T	3
11	3	4	0	T	0	3
12	3	T	0	0	0	T
13	T	0	T	0	0	0
14	0	0	4	0	0	0
15	0	0	4	0	T	0
16	0	0	4	T	5	0
17	0	T	4	3	5	T
18	T	5	T	3	5	5
19	3	5	0	T	5	5
20	3	5	0	5	T	5
21	3	5	T	5	0	5
22	3	5	2	5	T	T
23	3	5	2	T	5	0

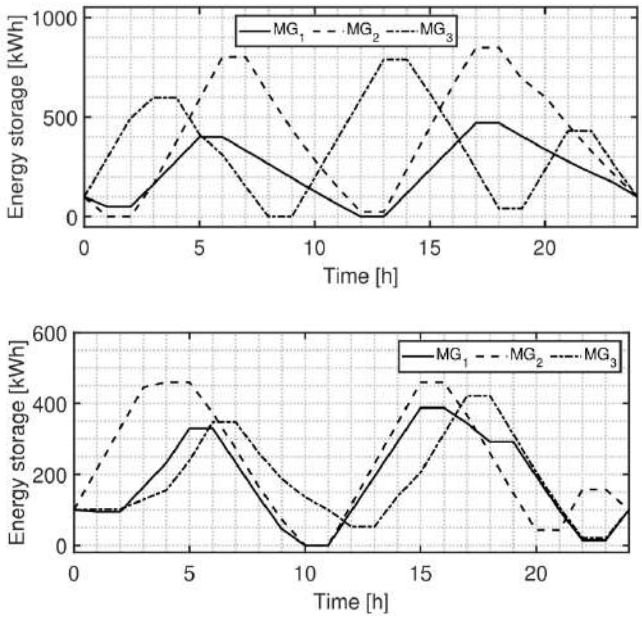


Figure 71. Charging/discharging patterns of MESSs in each MG: (a) AB = 6, (b) AB = 3

2. Resilience-Oriented Coordination of NMGs

To assess the coordination effect of NMGs towards resilience enhancement, a modified IEEE 15-bus distribution network containing 3 NMGs, 2 tie-lines, and 4 smart switches is utilized for the experiment, as shown in Fig. 74. It is noted that the NMGs in this experiment are used to support load restorations for line outages. To achieve this target, MGs can use both 1) generation resources (e.g., DGs, PVs, WTs, ESs) to directly support its own loads; and 2) network reconfigurations to allow power exchanges with their connected MGs. In this context, the modified IEEE 15-bus distribution network can be divided into three regions

(MGs), of which each MG owns 1 DG, 1 PV or WT, and 1 ES. To capture the impact of extreme events, multiple line outages can happen in distribution network, where the potential outage locations are depicted in Fig. 74.

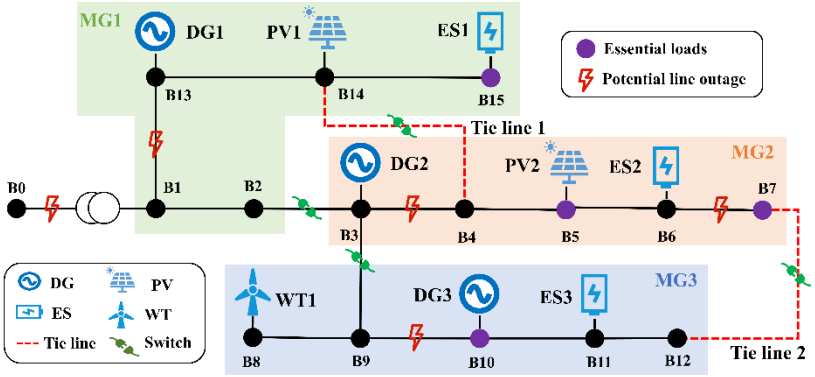


Figure 72. The modified IEEE 15-bus distribution network with 3 NMGs

For specific case studies, Fig. 75 shows the behaviours of smart switches and power exchanges. Fig. 76 and 77 show the DER dispatches and power suppliers of 3 NMGs, respectively.

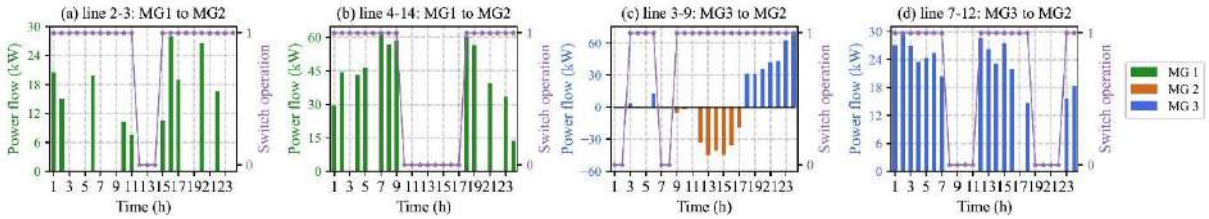


Figure 73. Switch operations and power exchanges among 3 NMGs via 4 connected lines (a)-(d)

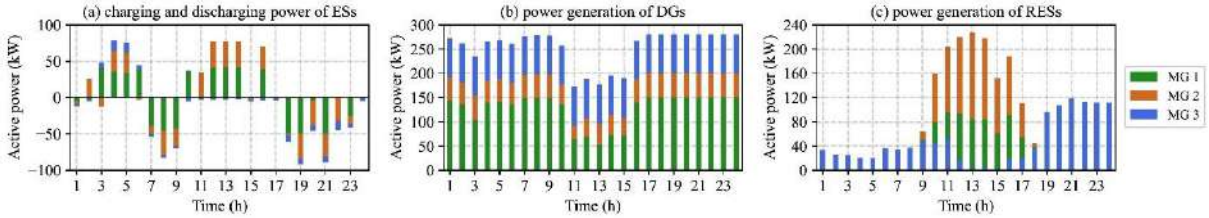


Figure 74. Power dispatches of (a) ESs, (b) DGs, and (c) RESs of 3 NMGs

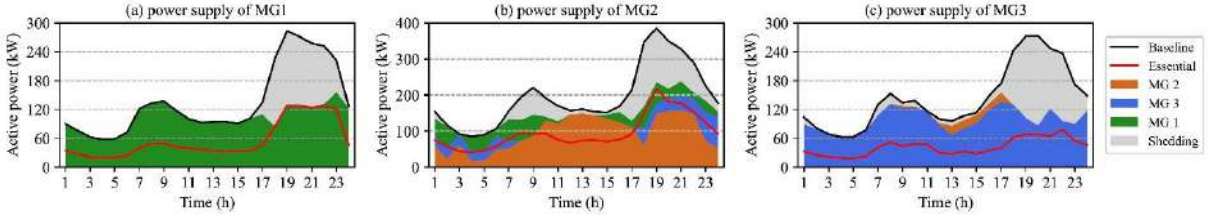


Figure 75. Load profiles, load shedding, and power supplies of 3 NMGs (a)-(c)

- **Power Exchanges among NMGs and Switch Operations**

It can be observed from Fig. 75 that both MG 1 (green) and MG 3 (blue) are learned to supply power to MG 2. This is mainly driven by the following three reasons. First, MG 1 and MG 3 are characterized by their abundant resources (e.g., large DG capacity), resulting in the energy surplus supplied to MG 2 with the energy deficit of relatively high demand levels. Second, the smart switch operations prompt the transmission channel to enhance the capability of power exchanges among the 3 NMGs. Third, the particular (middle) location of MG 2 allows it to connect with both MG 1 and MG 3, leading to more options for power supply.

In particular, the smart switch operations of lines 2-3 and 4-14 are close in the morning and evening, as depicted in Fig. 75(a)-(b). This allows MG 1 to be capable of supplying power to MG 2 (green) through these two lines. The reason why MG 1 does not supply power to MG 2 at midday is that MG 2 is characterized by abundant PV resources (Fig. 76(c)), which is enough to supply its midday demand. Similarly, as shown in Fig. 75 (c)-(d), MG 3 (blue) is operated to supply MG 2 via lines 3-9 and 7-12 with the close switch operations. However, MG 2 (orange) is operated to supply MG 3 through line 3-9 at midday because of its excessive PV resources.

- **Dispatches of DERs**

It can be observed from Fig. 76(a) that the flexibility of ESs in both MG 1 and MG 2 is fully explored via the significant charging and discharging power magnitudes, while ES in MG 3 behaves inactively over the day. Specifically, the first charging behaviours of ESs in MG 1 and MG 2 occur at the beginning of the day (hours 1-6) for the purpose of discharging to supply the secondary demand peaks in the early morning (hours 7-9). Meanwhile, the second charging and discharging cycle occurs at midday (hours 10-16) and at night (hours 17-24), respectively. This is because ESs in MG 1 and MG 2 are learned to shift PV generation from midday to supply the primary demand peaks at night. The reason why ES in MG 3 behaves inactively is that the MG 3's two demand peaks can be mostly met by its installed DG and WT, with no need for ES.

In terms of the dispatches of DGs and RESs in Fig. 76(b)-(c), their aggregated power generation exhibits a complementary effect, which can effectively supply the overall demand requirements of 3 NMGs.

- **Power Supply and Load Restoration**

It can be found that MG 1 in Fig. 77(a) solely uses its own resources (green) to supply itself; while MG 2 in Fig. 77(b), apart from itself (orange), also receives a significant amount of power supply from both MG 1 (green) and MG 3 (blue) in the morning and at night; and lastly, MG 3 in Fig. 77(c) mainly relies on its own resources (blue) but also receives a certain level of power supply from MG 2 (orange) in the midday. Those power exchanges among 3 NMGs are caused by i) the abundant resources in MG 1 and MG 3; ii) the high demand requirements in MG 2; iii) the severe power outages occurring in MG 2; and iv) the smart switch operations making the power transmission available. More importantly, all the essential loads (red lines) in 3 NMGs are fully supplied, while the load shedding (grey area) belonging to non-essential loads happens during the two peak demand periods.

Table 13. Load shedding quantity of 3 NMGs in the modified IEEE 15-bus network

MG	MG1	MG2	MG3	Total
Essential load (kW)	0	0	0	0
Non-essential load (kW)	786	1,111	988	2,885

As shown in Table 13, the resilience enhancement for essential loads outperforms that for non-essential loads, respectively resulting in completely zero and 2,885 kWh of total load shedding quantity, yielding a 75% resilience index of the entire network.

3. Towards Microgrid Resilience Enhancement Via Mobile Power Sources and Repair Crews

To assess the effectiveness of the proposed RL method in capturing realistic MPS and RC dispatch behaviours, a modified IEEE 33-bus power network is shown in Fig. 78(a). The power network has 8 essential loads, 15 non-essential loads, 6 PVs, 3 DGs, and 5 MSs. Mobile resources deployed for load restoration include 1 MEG, 1 MESS and 1 RC. In the transport network, we assume that these resources can move to any candidate node through their routing characteristics, where detailed transport network structures between these candidate nodes (i.e., MSs for MPSs and damaged components for RCs) can be found Fig. 78 (b) and (c).

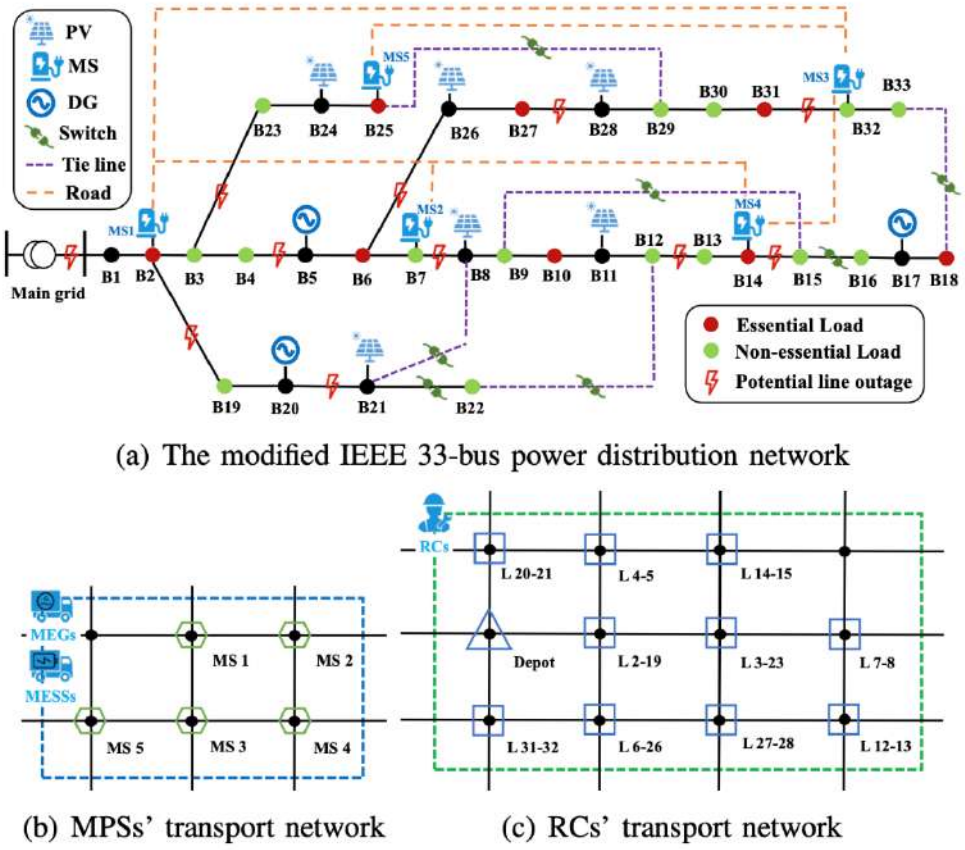


Figure 76. The coupled power-transport network utilized for case studies: (a) the modified 33-bus power distribution network, (b) the transport network with MSs for MPSs, (c) the transport network with damaged components for RCs

To capture the impact of extreme events, we assume that multiple line outages can happen in the power network, as depicted in Fig. 78(a). Specifically, the Monte Carlo sampling technique can be used to generate a manageable number of scenarios based on the fragility curve suggested in [100]. For each episode, a random outage scenario will be sampled from the fragility curve to represent the damaged conditions. Within the distribution network as

shown in Fig. 78(a), the potential lines with higher damaged probabilities are easier to be selected into the outage scenario.

- **Analysis of Dispatch Behaviours and Switch Operations**

This section aims at validating the control policy for dispatch behaviours of three resources, while the MG switch operations and load conditions are also involved. A scenario with 6 line outages (lines 4–5, 14–15, 2–19, 3–23, 6–26 and 31–32) is selected here. Additionally, serious traffic congestion mainly happens in the afternoon during the rush hours.

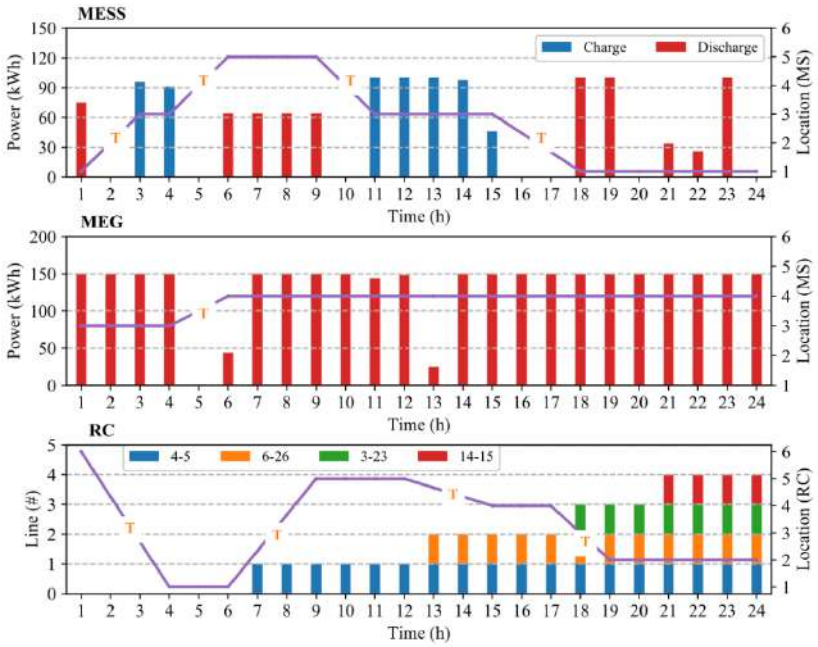


Figure 77. Dispatch behaviours of MESS, MEG and RC

We first examine the dispatch behaviours of three MESS, MEG and RC agents, as depicted in Fig. 79. As for MESS in Fig. 79 (the top subfigure), its routing behaviours are between MSs 1, 3 and 5. Specifically, the MESS chooses to discharge power at MSs 1 and 5 for demand supply, since both MS1 at bus 2 and MS 5 at bus 25 connect with essential loads. Additionally, the discharging behaviours of MESS mainly occur at the periods of morning and night, when demand is relatively high. Now, let us look at the charging behaviours of MESS when it runs out of energy. The first charge occurs in the evening at MS 3 where MEG chooses to connect for power supply during the first few hours, as shown in Fig. 79 (the middle subfigure). Such phenomena also exhibit the coordination effect of MESS and MEG in both mobility and flexibility. The second charge occurs in the mid-day when free PV resources are abundant.

Furthermore, the interesting results can be found that it takes MESS 2 hours (15:01-17:00) to travel from MS 3 to MS 1 in the afternoon while taking only 1 hour (1:01- 2:00) from MS 1 to MS 3 in the morning. This is because the serious road congestion happening in the afternoon leads to another hour traveling time. On the other hand, MEG chooses to connect with MS3 at bus 32 and MS 4 at bus 14 for power supply, since MS 4 is connected with essential load and one serious damage happens around bus 14. As for RC in Fig. 79 (the bottom subfigure), it chooses to repair the damaged lines 4–5, 6–26, 3–23, and 14–15

sequentially. After these four lines are all repaired, RC has run out of its resources and is incapable of repairing more. It is also mentioned here the reason why RC firstly repairs line 4–5 is that repairing this line can restore the associated power flow, in which bus 2 is connected with essential load. In this case, there is no need for MEG to connect with MS 1 at bus 2 towards resilience enhancement.

Finally, load conditions for both essential and non-essential types are compared in Fig. 80. Overall, the resilience enhancement for essential loads exhibits better performance than that for non-essential loads, respectively causing 291 kWh and 4,217 kWh total load shedding quantity. Thus, the system needs to pay serious cost for non- essential loads (6,326 £) compared to the essential loads (728 £).

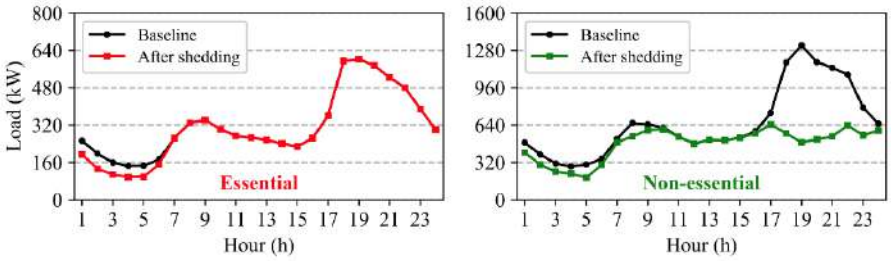


Figure 78. Aggregated baseline and load after shedding in 33-bus system

4.6 KNOWLEDGE SHARING – CYBER THREAT INTELLIGENCE AND CASCADING EVENTS (TASK 3.6)

This tool will have two main parts.

- The first part (**Cyber Threat Intelligence**) will provide cyber threat intelligence capabilities utilizing information from internal and external (online) sources through Big Data analytical methods.
- The second part (**Cascading events initiated by natural and climatic disturbances**) will focus on cascading events initiated by natural and climatic disturbances and their quantifiable impacts on the resilience of the physical electricity infrastructure.

4.6.1 Cyber Threat Intelligence

4.6.1.1 Internal Architecture of the tool

4.6.1.1.1 Aim of the tool

Cyber Threat Intelligence (CTI) is a vital component in contemporary cybersecurity applications. It serves several key roles, including threat detection and prevention, by collecting and analysing data from various sources to identify emerging threats and IoCs. The R²D² Cyber Threat Intelligence tool provides situational awareness by offering real-time and historical information about the threat landscape, including threat actors, tactics, and

targeted environments. It also aids in vulnerability management by correlating threat intelligence with identified vulnerabilities, helping prioritize patching and remediation efforts. During security incidents, the CTI tool assists in incident response and investigation by providing contextual information and relevant threat intelligence. It enables proactive threat hunting activities and facilitates collaboration and information sharing within trusted communities. Ultimately, the CTI tool enhances the R^2D^2 cybersecurity tools' capabilities by delivering actionable intelligence to make informed decisions, defend against threats, and respond effectively to security incidents.

In this context, the adoption and implementation of MISP (Malware Information Sharing Platform & Threat Sharing) is highly recommended. – an open-source threat intelligence platform designed to facilitate the secure exchange of structured threat data among organisations, security researchers, and analysts. MISP offers a comprehensive suite of capabilities, features, and modules, along with a powerful API interoperability, making it an ideal choice for enhancing our cybersecurity posture and enabling seamless integration with existing systems.

MISP offers various features and modules to enhance its functionality and adaptability. Data import/export capabilities allow seamless integration with external sources, enriching the threat intelligence pool. Real-time notifications are facilitated through webhooks, supporting automated data exchange with external systems and custom integrations.

The platform's flexibility is evident in its customization options, allowing organisations to tailor user roles, event attributes, and taxonomies to specific needs. Furthermore, MISP provides STIX2 export support, adhering to the standardised Structured Threat Information eXpression (STIX) format for compatibility with other security tools. Sharing groups enable secure collaboration with trusted partners, promoting effective threat intelligence sharing.

4.6.1.1.2 Detailed Architecture

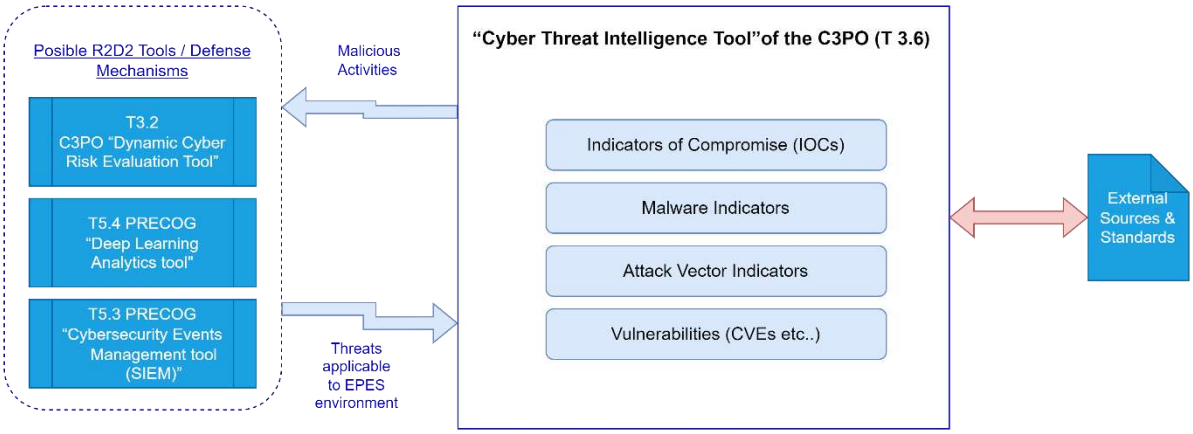


Figure 79. R^2D^2 Cyber Threat intelligence Tool Architecture

4.6.1.1.3 Description of Components

The tool comprises a single primary component which is the platform that manages CTI. MISP offers a range of capabilities to streamline the threat intelligence sharing process. Users can create and manage cybersecurity events containing critical information about

threats and associated IOCs. Granular attribute management allows for detailed threat descriptions, covering IP addresses, domains, file hashes, and more.

MISP also embeds expandable taxonomies that facilitate classifying and correlating threat data, making it easier to identify interconnected patterns and analyse trends. Users can report sightings of specific attributes, bolstering the validation and credibility of shared threat data.

Additionally, MISP supports the use of custom object templates, empowering organisations to create specialised data objects to describe unique threat information or incident types. The platform's delegation features ensure controlled sharing of information, providing the right access controls for different collaborating entities. Integration with various taxonomies, including popular ones like MITRE ATT&CK, enables harmonisation and standardised data categorization.

The CTI Tool is designed to facilitate the collection, sharing, storing, and collaboration of cybersecurity-related information among organizations and communities. It provides among others the following functionality:

- CTI management:
    - Data Collection: it allows users to collect and aggregate various types of threat intelligence data, including indicators, attributes, events, and reports. This data can be sourced from internal observations, external feeds, and threat intelligence providers.
    - Storage and Organization: it provides a structured repository for storing and managing threat intelligence data. It uses a hierarchical structure where information is organized into events, attributes, and objects, enabling users to efficiently categorize, search, and retrieve relevant data.
    - Sharing and Collaboration: it enables the sharing of threat intelligence data among trusted communities and organizations. Users can define sharing groups, establish data sharing agreements, and control the dissemination of information based on predefined access levels. This fosters collaboration and helps in the collective defense against cyber threats.
    - Integration and Interoperability: it offers extensive integration capabilities, allowing users to connect and exchange data with other security tools, platforms, and services. It supports standard formats like STIX (Structured Threat Information Expression) and supports various data exchange protocols, enabling seamless interoperability with different systems.
    - Analysis and Correlation: it provides features to analyze and correlate threat intelligence data. It includes built-in functionalities for data enrichment, attribute normalization, and correlation to identify relationships between indicators and events. These capabilities enhance the understanding of threats and aid in proactive defense measures.
    - Customization and Extension: it allows users to customize and extend the platform to meet specific requirements. It provides the flexibility to

define custom data models, create new object templates, and extend existing functionalities through plugins and APIs.

- Automation and Integration with Security Operations: it supports automation through APIs and integrates with security operations tools like SIEMs (Security Information and Event Management), IDS/IPS (Intrusion Detection/Prevention Systems), and threat intelligence platforms. This enables the automated ingestion, analysis, and response to threat intelligence data within an organization's security infrastructure.

- Vulnerabilities management: Vulnerability feeds like the National Vulnerability Database (NVD) and MITRE Common Vulnerabilities and Exposures (CVEs) provide essential information about known vulnerabilities in software and systems. Here's a brief description of each:

  - National Vulnerability Database (NVD): The National Vulnerability Database (NVD) is a comprehensive vulnerability database maintained by the National Institute of Standards and Technology (NIST) in the United States. It serves as a central repository for information about vulnerabilities in various software products and systems. NVD collects vulnerability information from multiple sources, including vendors, security researchers, and other vulnerability databases.

    NVD provides standardized vulnerability descriptions, severity ratings, impact metrics, affected product versions, and other relevant details. It assigns CVSS scores to assess the severity of vulnerabilities. NVD also includes references to related advisories, patches, and mitigations.

    The NVD vulnerability feed is widely used by organizations, security teams, vulnerability scanners, and security information and event management (SIEM) systems to stay informed about known vulnerabilities and prioritize their remediation efforts.

  - MITRE Common Vulnerabilities and Exposures (CVEs): The MITRE CVE (Common Vulnerabilities and Exposures) system is a community-driven effort to provide a standardized naming scheme for vulnerabilities. CVEs are unique identifiers assigned to specific vulnerabilities in software, hardware, or systems. Each CVE identifier consists of the prefix "CVE-" followed by a year and a unique number (e.g., CVE-2021-12345).

    MITRE maintains the CVE List, which includes entries for known vulnerabilities along with relevant details such as vulnerability descriptions, affected software versions, references to advisories and patches, and other related information. CVEs aim to provide a common language and reference point for discussing and sharing vulnerability information across different organizations, tools, and platforms.

    The MITRE CVEs are widely adopted and used as a reference in vulnerability management processes, penetration testing, security assessments, and security research. They help security teams identify and track vulnerabilities, prioritize remediation efforts, and communicate about specific security issues consistently.

4.6.1.1.4 Techniques & Algorithms

Regarding the techniques, algorithms, and mathematical models used for interconnecting MISP with other entities, it is essential to clarify that MISP is an existing open-source threat intelligence platform with a well-established architecture, design and programmable interfaces. As such, the core functionalities and features of MISP have already been developed and implemented, and the platform is actively maintained by the community.

For the proposed interconnection with other systems, the development approach will be progressive and iterative as deemed necessary during the implementation. As technical interfaces and requirements for integration with specific systems become known in detail, the necessary code for seamless interconnection will be developed accordingly. This incremental development process ensures that the integration is tailored to meet the specific needs and configurations of the external systems, thereby optimising the effectiveness and efficiency of data exchange and processing.

The development team will adopt best practices and industry standards for secure data sharing and API interoperability to ensure the integrity and confidentiality of the exchanged threat intelligence. Additionally, the team will follow established coding standards and practices, such as version control and documentation, to maintain a high level of software quality and ease of collaboration with the broader community.

By adopting this progressive development approach, we can maximise the potential of MISP as a powerful tool for threat intelligence sharing inside the project, while ensuring seamless integration with all the required interdependent systems.

4.6.1.1.5 Data Exchanges & Interfaces

MISP's API offers a robust and powerful mechanism for seamless integration with external systems. Users can programmatically create, update, and delete events, providing automation for threat intelligence workflows. Attribute handling through the API allows adding, modifying, and retrieving attribute data, streamlining data management processes.

The API also supports complex searches and queries, enabling organisations to extract specific threat intelligence data efficiently. Interacting with galaxies and taxonomies through the API allows for dynamic classification and correlation of threat data. Overall, MISP's API interoperability empowers organisations to automate and integrate their threat intelligence processes effectively.

The CTI Tool will exchange information with both internal and external components. More specifically, it will consume information from external sources to feed internal R^2D^2 tools, like the R^2D^2 T3.2 Dynamic Risk Evaluation Tool and the R^2D^2 T5.3 PRECOG SIEM, but will also share malicious activities identified by the R^2D^2 Tools, with the community, thus contributing to the protection of the energy community against cyber actors.

The CTI Tool will utilize at least the following feeds for consuming CTI: The feeds of the deployed version of MISP will include the following sources:

- abuse.ch SSL IPBL - abuse.ch - feed format: csv
- alienvault reputation generic - .alienvault.com - feed format: csv
- All current domains belonging to known malicious DGAs - osint.bambenekconsulting.com - feed format: csv
- blocklist.de/lists/all.txt - blocklist.de - feed format: freetext

- blocklist.greensnow.co - greensnow.co - feed format: csv
- blockrules_of_rules.emergingthreats.net - rules.emergingthreats.net - feed format: csv
- ci-badguys.txt - cinsscore.com - feed format: freetext
- CIRCL OSINT Feed - CIRCL - feed format: misp
- cybercrime-tracker.net - all - cybercrime-tracker.net - feed format: freetext
- CyberCure - Blocked URL Feed - www.cybercure.ai - feed format: csv
- CyberCure - Hash Feed - www.cybercure.ai - feed format: csv
- CyberCure - IP Feed - www.cybercure.ai - feed format: csv
- diamondfox_panels - pan-unit42 - feed format: freetext
- DigitalSide Threat-Intel OSINT Feed - osint.digitalside.it - feed format: misp
- DNS CH TXT version.bind - dataplane.org - feed format: csv
- DNS recursion desired IN ANY - dataplane.org - feed format: csv
- DNS recursion desired - dataplane.org - feed format: csv
- Domains from High-Confidence DGA-based C&C Domains Actively Resolving - osint.bambenekconsulting.com - feed format: csv
- Feodo IP Blocklist - abuse.ch - feed format: csv
- firehol_level1 - iplists.firehol.org - feed format: freetext
- http://cybercrime-tracker.net gatelist - http://cybercrime-tracker.net gatelist - feed format: freetext
- http://cybercrime-tracker.net hashlist - http://cybercrime-tracker.net hashlist - feed format: freetext
- IP protocol 41 - dataplane.org - feed format: csv
- ip-block-list - snort.org - https://snort.org - feed format: freetext
- IPs from High-Confidence DGA-Based C&Cs Actively Resolving - requires a valid license - osint.bambenekconsulting.com - feed format: csv
- ipspamlist - ipspamlist - feed format: csv
- IPsum (aggregation of all feeds) - level 1 - lot of false positives - IPsum - feed format: freetext
- IPsum (aggregation of all feeds) - level 2 - medium false positives - IPsum - feed format: freetext
- IPsum (aggregation of all feeds) - level 3 - low false positives - IPsum - feed format: freetext
- IPsum (aggregation of all feeds) - level 4 - very low false positives - IPsum - feed format: freetext
- IPsum (aggregation of all feeds) - level 5 - ultra false positives - IPsum - feed format: freetext
- IPsum (aggregation of all feeds) - level 6 - no false positives - IPsum - feed format: freetext
- IPsum (aggregation of all feeds) - level 7 - no false positives - IPsum - feed format: freetext
- IPsum (aggregation of all feeds) - level 8 - no false positives - IPsum - feed format: freetext
- malshare.com - current all - malshare.com - feed format: freetext
- malsilo.domain - MalSilo - feed format: csv
- malsilo.ipv4 - MalSilo - feed format: csv
- malsilo.url - MalSilo - feed format: csv
- Malware Bazaar - abuse.ch - feed format: csv
- MalwareBazaar - abuse.ch - feed format: misp

- Metasploit exploits with CVE assigned - eCrimeLabs - feed format: csv
- mirai.security.gives - security.gives - feed format: freetext
- OpenPhish url list - openphish.com - feed format: freetext
- Panels Tracker - Benkow.cc - feed format: csv
- PhishScore - PhishStats - feed format: csv
- Phishtank online valid phishing - Phishtank - feed format: csv
- pop3gropers - home.nuug.no - feed format: csv
- sipinvitation - dataplane.org - feed format: csv
- sipquery - dataplane.org - feed format: csv
- sipregistration - dataplane.org - feed format: csv
- SMTP data - dataplane.org - feed format: csv
- SMTP greet - dataplane.org - feed format: csv
- SSH Bruteforce IPs - APNIC Community Honeynet Project - feed format: csv
- sshpwauth.txt - dataplane.org - feed format: csv
- Telnet Bruteforce IPs - APNIC Community Honeynet Project - feed format: csv
- TELNET login - dataplane.org - feed format: csv
- The Botvrij.eu Data - Botvrij.eu - feed format: misp
- This list contains all browser mining domains - A list to prevent browser mining only - ZeroDot1 - CoinBlockerLists - feed format: freetext
- This list contains all domains - A list for administrators to prevent mining in networks - ZeroDot1 - CoinBlockerLists - feed format: freetext
- This list contains all optional domains - An additional list for administrators - ZeroDot1 - CoinBlockerLists - feed format: freetext
- threatfox indicators of compromise - abuse.ch - feed format: csv
- Threatfox - abuse.ch - feed format: misp
- Tor ALL nodes - TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor exit nodes" feed. - feed format: csv
- Tor exit nodes - TOR Node List from dan.me.uk - careful, this feed applies a lock-out after each pull. This is shared with the "Tor ALL nodes" feed. - feed format: csv
- URL Seen in honeypots - APNIC Community Honeynet Project - feed format: freetext
- URLHaus Malware URLs - abuse.ch - feed format: csv
- URLhaus - abuse.ch - feed format: misp
- VNC RFB - dataplane.org - feed format: csv
- VXvault - URL List - VXvault - feed format: freetext

Other sources of information that will be considered for the needs of the R^2D^2 CTI Tool include CERTs, CSIRTs, and the EE-ISAC.

The CTI Tool will support the exchange of data using at least the following data formats:

- MISP: The MISP data format is based on the JSON (JavaScript Object Notation) standard, which is a lightweight and human-readable data interchange format. It follows a hierarchical structure and uses key-value pairs to represent different attributes of an event or indicator.

  At its core, MISP focuses on the concept of events, which represent specific incidents or observations. Each event consists of various attributes, which provide details about the observed data. These attributes can include

information such as IP addresses, domain names, email addresses, file hashes, and more.

In addition to attributes, MISP also supports objects, which are reusable templates that provide a structured way to describe complex data. Objects allow users to define custom data models and create instances of those models within events.

The MISP data format also incorporates various metadata fields to provide additional contextual information. This includes timestamps, the source of the data, the distribution level (e.g., private, community, or sharing group), and other administrative details.

STIX 1.x: STIX 1.x is an XML-based data format designed to enable the exchange of structured threat intelligence information. It provides a standardized framework for representing various aspects of cyber threat data, including indicators, observables, threat actors, campaigns, and more.

The main components of STIX 1.x are:

- Indicators: These represent specific patterns or characteristics of malicious activity, such as IP addresses, domain names, file hashes, or behavioral patterns. Indicators can be used to detect and identify potential threats.
- Observables: These are specific instances or occurrences of indicators within a particular context. Observables provide additional details about the observed data, such as the time of detection, location, or associated entities.
- TTPs: TTPs (Tactics, Techniques, and Procedures) describe the methods and approaches used by threat actors to carry out attacks. They provide insights into the behavior, tools, and procedures employed by adversaries.
- Threat Actors: These entities represent individuals, groups, or organizations responsible for carrying out cyber threats. Threat actors can be classified based on their motivations, capabilities, or affiliations.
- Exploits: Exploits describe vulnerabilities in software, systems, or networks that can be leveraged by threat actors to gain unauthorized access or carry out attacks.

STIX 1.x also incorporates various other elements, such as relationships between entities, time-based properties, handling markings for data sharing, and related metadata.

- STIX 2.x: STIX 2.x is an updated version of the STIX specification, which builds upon the foundation of STIX 1.x and introduces several improvements. STIX 2.x is a JSON-based data format designed for representing, sharing, and exchanging structured cybersecurity threat intelligence. It provides a standardized framework for expressing various elements of threat information in a more flexible and extensible manner. Key features of STIX 2.x include:
  - Objects: STIX 2.x defines a set of core objects, such as indicators, observables, threat actors, campaigns, and more. These objects are

represented as JSON structures and provide a structured way to describe different aspects of threat intelligence. Objects can be composed and nested to represent complex relationships and scenarios.

- Relationships: STIX 2.x allows the establishment of relationships between objects, enabling the representation of connections and associations within threat intelligence. For example, a threat actor object can be linked to a campaign object to indicate their affiliation.
- Cyber Observables: STIX 2.x introduces the concept of Cyber Observables, which represent specific data elements associated with threat intelligence, such as IP addresses, domain names, file hashes, email addresses, and more. Cyber Observables provide a standardized way to capture and share granular details about observed data.
- Markings: STIX 2.x incorporates a flexible marking system that enables the classification and handling of sensitive information. Markings can be applied to objects and indicate their distribution limitations, handling restrictions, or privacy requirements.
- Extensions: STIX 2.x supports the use of extensions to accommodate domain-specific or organization-specific requirements. Extensions allow for the inclusion of additional properties or objects that are not part of the core specification, enhancing the expressiveness and customization of STIX data.

4.6.1.2 User Interface

Description of the user interface to be developed, including preliminary mock up, dashboards, charts, etc.

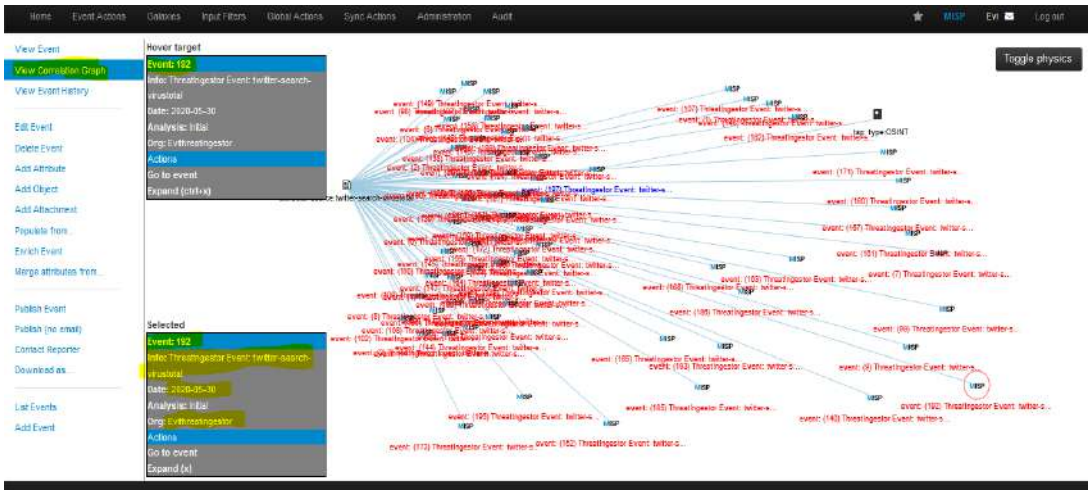


Figure 80. Reported threats correlation graph in MISP

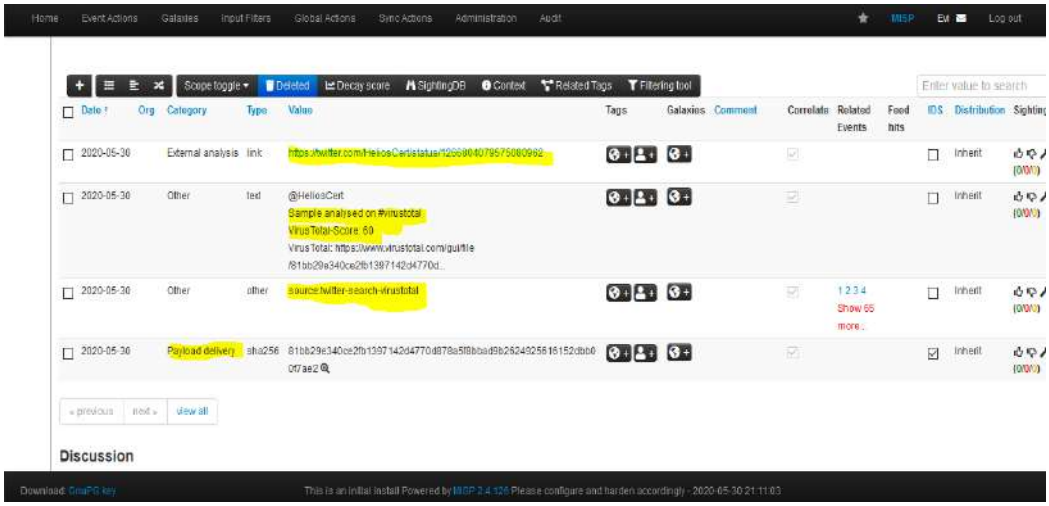


Figure 81. Reported events in MISP

4.6.2 Cascading events initiated by natural and climatic disturbances

4.6.2.1 Aim Internal Architecture of the tool

Aim of the tool

The objective of this tool is to serve as a comprehensive repository for storing data and knowledge pertaining to events that influence the resilience of the power system. It will encompass two types of extreme events, windstorms and wildfires. The related information will be provided from the modular extreme event simulators of T3.3. The tool will feature a dedicated section providing general information for each event, along with a file repository where users can archive reports and assessments. Users will have seamless access to this knowledge sharing platform through a user-friendly web interface, offering convenient and efficient navigation.

Type of information in the knowledge sharing platform

The tool will include the following types of information:

- Report Purpose and Context: It will provide a clear understanding of the report's objective, which is to evaluate the spatial and temporal impact of HILF events on the distribution system under examination.

- Analysis Methodology: Information about the analytical approach used, such as the utilization of C3PO modular event simulators, will be included to describe how the assessments were conducted.

- Network Details: The report will specify the location within the network being analyzed, for example, mentioning the specific feeder (e.g., feeder 33) and the broader network (e.g., Xanthi network).

- Extreme Event Details: Details about the specific event being analyzed, including its type (e.g., windstorm or wildfire), the exact time of its occurrence and its duration.
- Weather-related Characteristics: Information regarding the weather's conditions, such as the average wind speed during the event ([e.g., 30, 32, 35] m/sec), which have influenced the power system's resilience.
- Impact on Distribution Lines: Specific powerlines affected by the event, indicating which lines were damaged and went offline, resulting in outages that caused load shedding.
- Loads Affected: Identification of the loads impacted by these outages during the specified duration, giving insight into which parts of the distribution system were affected.
- Controllable Units: Information on the controllable units dispatch throughout the event, including the aggregated active power generation.
- Load Shedding Assessment: Information on load curtailments in the course of the examined HILF event and total energy not supplied.
- Operational Cost Evaluation: An approximation of the total operational cost incurred during the examined time horizon, providing insight into the financial implications of the event's impact.

Collectively, this information will allow users to gain a comprehensive understanding of the event's effects on the power system's resilience in terms of its technical aspects, within the defined geographical context.

4.6.2.2 Detailed Architecture of the tool

To ensure efficiency, scalability, and seamless user access, our tool will employ a standard web-service architecture composed of three fundamental components: a robust database server, a responsive back-end infrastructure, and a front-end environment. This triumvirate of components forms the backbone of our web application and will be subject to in-depth analysis in the sections that follow.

Central to this architecture is our database server, engineered to store and manage the wealth of information surrounding the cascading events impacting power system resilience. This repository will contain data using widely recognized and user-friendly formats such as. json or .xml.

Beyond mere data storage, the database management system will be thoughtfully designed to ensure streamlined access for our users. Information about these cascading events will be readily available via secure HTTPS requests, safeguarded to be accessible

exclusively to authorized users. These users will be authenticated through well-established and trusted authentication methodologies, ensuring the integrity and security of the knowledge-sharing platform.

In the subsequent sections, we delve into the intricate workings of the key components that constitute our software application. Together, they form a robust, user-friendly, and secure platform that empowers users to explore and comprehend the multifaceted impacts of events on power system resilience, fostering informed decision-making and enhancing the overall resilience of the electricity network.

- Database Server: this system will store the information that is necessary for the description of the cascading events. The format of the stored information will be one of the widely used and convenient ones, such as .json or .xml. The database management system that will be developed will assist the ease of access for the involved services and optimize the internal procedures of the database operations.
- Back-end Framework: this software service is the intermediate point between the stored information within the database server and the front-end framework which demonstrates the results. It executes the required operations to retrieve the data from the database and process them according to the specifications of the designed products. For its implementation, one of the well-known frameworks will be used, such as MS SQL Server, MySQL, etc.
- Front-end Framework: this service will use the functionalities of the back-end framework in order to demonstrate the necessary modules that will depict the results of the cascading incidents. The particular software environment presents the outcomes of the processed information through a variety of illustrative components, such as figures, tables, flowcharts, etc. For its deployment, there is a wide variety of broadly used software environments, such as AngularJS, React, etc., where the most suitable one will be selected.

4.6.2.3 User Interface

The UI of this tool will be designed to offer users a comprehensive and visually compelling perspective on cascading events impacting EPES infrastructures, particularly those arising from natural and climatic disturbances. To enhance user-friendliness and streamline access to desired information, the platform will feature a user-friendly search engine. This tool allows users to effortlessly navigate the repository of data, making it easier than ever to find and extract meaningful insights, thereby empowering users to make informed decisions in the realm of power system resilience.

4.6.2.4 Resources & Technologies

The creation of this knowledge-sharing tool will leverage a sophisticated stack of technologies to ensure efficiency, reliability, and user-friendliness. For the backend infrastructure, we will carefully select from a range of suitable database servers, including

MS SQL Server, MySQL, and MongoDB. These database servers will provide a secure and organized repository for storing critical event data and knowledge. The backend development will be powered by well-established frameworks such as Django, Ruby on Rails, or Node.js, enabling seamless data processing, retrieval, and analysis. On the front-end, cutting-edge technologies like JavaScript, Angular JS, or React will be employed, to craft an intuitive and visually engaging user interface. These front-end frameworks will not only enhance the user experience but also enable us to efficiently present complex data through interactive graphs, tables, figures, and user-friendly drop-down menus. The thoughtful integration of these technologies will contribute to the creation of a dynamic and effective knowledge-sharing platform for assessing power system resilience in the face of diverse events.

4.7 IMPLEMENTATION AND DEPLOYMENT PLAN

Gantt of the development of the product - year 2

Activity 1: Basic development

Activity 2: User Interface development

Activity 3: KPIs at component level

Activity 4: Unit test

Activity 5: early SW delivery

Activity 6: SW documentation & deliverable preparation

Activity 7: Final SW delivery

Months	M13 - Oct.23				M14 - Nov.23					M15 - Dec.23				M16 - Jan.24				M17 - Feb.24					M18 - Mar.24				M19 - Apr.24				M20 - May24					M21 - Jun.24				M22 - Jul.24				M23 - Aug.24					M24 - Sep.24			
Weeks	40	41	42	43	44	45	46	47	48	49	50	51	52	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
Activity 1																																																					
Activity 2																																																				
Activity 3																																																				
Activity 4																																																				
Activity 5																																																				
Activity 6																																																				
Activity 7																																																				

5. Conclusions and next steps

This document has provided an in-depth presentation and analysis of the functionalities, special features, and innovations of the C3PO product, which will be developed within the activities of WP3 in the framework of the R^2D^2 project. The analysis encompasses a rich literature review of the investigated research area that the R^2D^2 project handles, identifying open problems of the field, the challenges that are typically faced and the limitations of the current solutions that have been proposed to tackle the current problems. Furthermore, a deep inspection of the several submodules that will be implemented under the C3PO framework is extensively presented and analysed in order to highlight the innovations and the contributions of the deployed toolkit, aligned with the use cases that each module employs, the development workflow of the product, the involved actors and the pilot sites.

A brief summary of the submodules that will be developed within the WP3 activities of the R^2D^2 project is included in what follows:

- T3.1: the Cyber Risk Assessment Tool employs static risk management practices to provide more insights to the EPES about its cyber vulnerabilities, taking into consideration its assets, its controls and their criticality.
- T3.2: the component of Dynamic Cyber-Risk Status Evaluation will be used to identify and mitigate the cyber threats that emerge during the operation of the EPES through asset tracking, cyber threat likelihood and vulnerability criticality evaluation for critical assets.
- T3.3: the component of Spatial and Temporal Modelling and Quantification of Cascading Physical Events employs spatiotemporal algorithms crafted for modelling windstorms and wildfires and assessing their impact on the network.
- T3.4: The objective of this tool is to offer a resilience-driven investment and operational planning framework to mitigate or prevent cascading effects, along with a holistic operational and recovery solution for distribution systems during catastrophic events, including adaptable microgrids.
- T3.5: an efficient planning and operational approach for load restoration is designed in this application within an advanced multi-energy microgrid, through strategically positioning, routing, and scheduling mobile power resources.
- T3.6: in this submodule, cyber threat intelligence capabilities are offered through Big Data analytical methods, along with a repository that will provide assessment reports about cascading events.

In the upcoming working months that are allocated by the R^2D^2 project, the next steps will be done in order to initiate the second stage of this task:

- T3.1: Start creating the deployment model and the infrastructure of the tool (database, web server, visualization, etc.).
- T3.2: Initiate the necessary processes for deploying the model and the infrastructure of the tool (database, web server, visualization, etc.).

- T3.3: Build the Python code for the advanced event simulators and the MATLAB code for the AC-CFM model.
- T3.4: Deploy and test the performance of the resilient planning tool within the Simulink framework.
- T3.5: Develop the Python code that will be used for the optimization of the planning model and the routing and scheduling behaviors of the operational model.
- T3.6: Begin working on the generation of the Big Data analytical methods for the cyber threat intelligence and the repository for the assessment reports on the tracked cascading events.

6. References

6.1 REFERENCES

[1] Smart Grid Task Force - Expert Group 2 - Cybersecurity, "Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management.," 2019.

[2] ISO/IEC 27005:2022 -Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[3] ANSI/ISA-62443-3-2-2020, Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design

[4] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, A. Hahn, Guide to Industrial Control Systems (ICS) Security, Tech. Rep. NIST SP 800-82r2, National Institute of Standards and Technology (Jun. 2015).880. doi:10.6028/NIST.SP.800-82r2.

[5] AMERICA'S CYBER DEFENSE AGENCY - CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. online at :https://www.cisa.gov/downloading-and-installing-cset

[6] R. W. Y. Habash, V. Groza, D. Krewski and G. Paoli, "A risk assessment framework for the smart grid," 2013 IEEE Electrical Power & Energy Conference, Halifax, NS, Canada, 2013, pp. 1-6, doi: 10.1109/EPEC.2013.6802930.

[7] M. D. Smith and M. E. Paté-Cornell, "Cyber Risk Analysis for a Smart Grid: How Smart is Smart Enough? A Multiarmed Bandit Approach to Cyber Security Investment," in IEEE Transactions on Engineering Management, vol. 65, no. 3, pp. 434-447, Aug. 2018, doi: 10.1109/TEM.2018.2798408.

[8] Hewett, Rattikorn, Sudeeptha Rudrapattana, and Phongphun Kijsanayothin. "Cyber-security analysis of smart grid SCADA systems with game models." In Proceedings of the 9th annual cyber and information security research conference, pp. 109-112. 2014.

[9] Maziku, H., Shetty, S. and Nicol, D.M., 2019. Security risk assessment for SDN-enabled smart grids. Computer Communications, 133, pp.1-11.

[10] Syrmakesis, A.D., Alcaraz, C. & Hatziargyriou, N.D. Classifying resilience approaches for protecting smart grids against cyber threats. Int. J. Inf. Secur. 21, 1189–1210 (2022). https://doi.org/10.1007/s10207-022-00594-7

[11] M. Panteli and P. Mancarella, "Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events," IEEE Syst. J., vol. 11, no. 3, pp. 1733–1742, Sep. 2017.

[12] Y. Lin, Z. Bie, and A. Qiu, "A review of key strategies in realizing power system resilience,"Global Energy Interconnection, vol. 1, no. 1, pp. 70–78, 2018.

[13] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, "Critical points and transitions in an electric power transmission model for cascading failure blackouts," Chaos, vol. 12, no. 4, pp. 985–994, 2002.

[14] M. Vaiman et al., "Risk assessment of cascading outages: Methodologies and challenges," IEEE Trans. Power Syst., vol. 27, no. 2, pp. 631–641, May 2012.

[15] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, "Boosting the power grid resilience to extreme weather events using defensive islanding," IEEE Trans. Smart Grid, vol. 7, no. 6, pp. 2913–2922, Nov. 2016.

[16] Y. P. Fang, N. Pedroni, and E. Zio, "Comparing network-centric and power flow models for the optimal allocation of link capacities in a cascade-resilient power transmission network," IEEE Syst. J., vol. 11, no. 3, pp. 1632–1643, Sep. 2017.

[17] M. Noebels and M. Panteli, "Assessing the Effect of Preventive Islanding on Power Grid Resilience," in Proc. IEEE Milan PowerTech., 2019, pp. 1–6.

[18] H. Guo, C. Zheng, H. H. C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system," Renew. Sustain. Energy Rev., vol. 80, pp. 9–22, 2017.

[19] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," Phys. Rev. E - Statist. Phys., Plasmas, Fluids, Related Interdisciplinary Topics, vol. 69, no. 4, pp. 1–4, 2004.

[20] P. Hines, E. Cotilla-Sanchez and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?," Chaos, vol. 20, no. 3, pp. 033122, Sept. 2010.

[21] P. D. H. Hines, I. Dobson, E. Cotilla-Sanchez and M. Eppstein, ""Dual Graph" and "Random Chemistry" Methods for Cascading Failure Analysis," 2013 46th Hawaii International Conference on System Sciences, Wailea, HI, USA, 2013, pp. 2141-2150, doi: 10.1109/HICSS.2013.1.

[22] X. Zhang, C. Zhan, and C. K. Tse, "Modeling the dynamics of cascading failures in power systems," IEEE J. Emerg. Sel. Topics Circuits Syst., vol. 7, no. 2, pp. 192–204, Jun. 2017.

[23] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," Probab. Eng. Informational Sci., vol. 19, no. 1, pp. 15–32, 2005.

[24] I. Dobson, "Estimating the propagation and extent of cascading line outages from utility data with a branching process," IEEE Trans. Power Syst., vol. 27, no. 4, pp. 2146–2155, Nov. 2012.

[25] J. Kim, K. R. Wierzbicki, I. Dobson, and R. C. Hardiman, "Estimating propagation and distribution of load shed in simulations of cascading blackouts," IEEE Syst. J., vol. 6, no. 3, pp. 548–557, Sep. 2012.

[26] M. A. Rios, D. S. Kirschen, D. Jayaweera, D. P. Nedic, and R. N. Allan, "Value of security: Modeling time-dependent phenomena and weather conditions," IEEE Trans. Power Syst., vol. 17, no. 3, pp. 543–548, Aug. 2002.

[27] K. Zhou, I. Dobson, and Z. Wang, "The Most Frequent N-K Line Outages Occur in Motifs That Can Improve Contingency Selection," in IEEE Transactions on Power Systems, doi: 10.1109/TPWRS.2023.3249825

[28] B. A. Carreras, D. E. Newman, and I. Dobson, "North American Blackout Time Series Statistics and Implications for Blackout Risk," in IEEE Transactions on Power Systems, vol. 31, no. 6, pp. 4406-4414, Nov. 2016, doi: 10.1109/TPWRS.2015.2510627.

[29] J. Xie, I. Alvarez-Fernandez and W. Sun, "A review of machine learning applications in power system resilience," in IEEE Power and Energy Society General Meeting, 2020-August, 2020, https://doi.org/10.1109/PESGM41954.2020.9282137

[30] Arteaga, J. M. H., Hancharou, F., Thams, F., & Chatzivasileiadis, S. (2019, June 1). Deep learning for power system security assessment. 2019 IEEE Milan PowerTech, PowerTech 2019. https://doi.org/10.1109/PTC.2019.8810906

[31] Y. Wang, M. Liu, and Z. Bao, "Deep learning neural network for power system fault diagnosis," in Chinese Control Conference, CCC, 2016-August, pp. 6678–6683, 2016, https://doi.org/10.1109/ChiCC.2016.7554408

[32] T. Ahmad, Y. Zhu, and P. Papadopoulos, "Predicting cascading failures in power systems using graph convolutional networks," presented at NeurIPS 2021 Workshop on Tackling Climate Change with Machine Learning, 2021

[33] R. Pi, Y. Cai, Y. Li, and Y. Cao, "Machine Learning Based on Bayes Networks to Predict the Cascading Failure Propagation," in IEEE Access, vol. 6, pp. 44815-44823, 2018, doi: 10.1109/ACCESS.2018.2858838.

[34] M. J. Eppstein and P. D. Hines, "A "random chemistry" algorithm for identifying collections of multiple contingencies that initiate cascading failure," IEEE Trans. Power Syst., vol. 27, no. 3, pp. 1698–1705, Aug. 2012.

[35] H. Sabouhi, A. Doroudi, M. Fotuhi-Firuzabad, and M. Bashiri, "Electrical power system resilience assessment: A comprehensive approach," IEEE Syst. J., vol. 14, no. 2, pp. 2643–2652, Jun. 2020.

[36] S. Yang, W. Chen, X. Zhang, C. Liang, H. Wang, and W. Cui, "A graph based model for transmission network vulnerability analysis," IEEE Syst. J., vol. 14, no. 1, pp. 1447–1456, Mar. 2020.

[37] A. Muir and J. Lopatto, "Final report on the August 14, 2003 blackout in the United States and Canada: Causes and recommendations," U.S.-Canada Power System Outage Task Force, Rep. AR-1165, 2004.

[38] J. M. Ordacgi Filho, "Brazilian blackout 2009: Blackout watch," in Proc. PAC World Mag., Mar. 2010, pp. 36–37.

[39] H. Cetinay, S. Soltan, F. A. Kuipers, G. Zussman, and P. Van Mieghem, "Analyzing cascading failures in power grids under the AC and DC power flow models," Perform. Eval. Rev., vol. 45, no. 3, pp. 198–203, 2018.

[40] P. D. Hines and P. Rezaei, "Cascading failures in power systems," in Smart Grid Handbook, vol. 1, Hoboken, NJ: Wiley, 2016.

[41] W. Yuan, J. Wang, F. Qiu, C. Chen, C. Kang and B. Zeng, "Robust Optimization-Based Resilient Distribution Network Planning Against Natural Disasters," in IEEE Trans. on Smart Grid, vol. 7, no. 6, pp. 2817-2826, Nov. 2016.

[42] S. Ma; B. Chen; Z. Wang, "Resilience Enhancement Strategy for Distribution Systems under Extreme Weather Events," in IEEE Trans. on Smart Grid, vol.PP, no.99, pp.1-1.

[43] M. Panteli, D. N. Trakas, P. Mancarella and N. D. Hatziargyriou, "Boosting the Power Grid Resilience to Extreme Weather Events Using Defensive Islanding," IEEE Trans. on Smart Grid, vol. 7, no. 6, pp. 2913-2922, Nov. 2016.

[44] M. Panteli; P. Mancarella, "Modeling and Evaluating the Resilience of Critical Electrical Power Infrastructure to Extreme Weather Events," IEEE Systems Journal, vol.PP, no.99, pp.1-10.

[45] C. Wang; Y. Hou; F. Qiu; S. Lei; K. Liu, "Resilience Enhancement with Sequentially Proactive Operation Strategies", IEEE Transactions on Power Systems, vol.PP, no.99, pp.1-1.

[46] M. Panteli; P. Mancarella; D. Trakas; E. Kyriakides; N. Hatziargyriou, "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems," in IEEE Trans on PWRS , vol.PP, no.99, pp.1-1

[47] A. Bagchi, A. Sprintson and C. Singh, "Modeling the impact of fire spread on the electrical distribution network of a virtual city," 41st North American Power Symp., Starkville, MS, USA, 2009, pp. 1-6.

[48] M. Choobineh, B. Ansari, and S. Mohagheghi, "Vulnerability assessment of the power grid against progressing wildfires," Fire Safety Journal, vol. 73, pp. 20–28, 2015.

[49] S. Mohagheghi, and S. Rebennack, "Optimal resilient power grid operation during the course of a progressing wildfire," International Journal of Electrical Power & Energy Systems, vol. 73, pp. 843-852, 2015.

[50] B. Ansari, and S. Mohagheghi, "Optimal energy dispatch of the power distribution network during the course of a progressing wildfire," Int. Trans. Electr. Energ. Syst., vol. 25, pp. 3422-3438, 2015.

[51] IEEE Standard for Calculating the Current-Temperature Relationship of Bare Overhead Conductors," IEEE Std 738-2012 (Revision of IEEE Std 738-2006 - Incorporates IEEE Std 738-2012 Cor 1-2013), vol., no., pp.1-72, Dec. 23 2013.

[52] M. Nazemi and P. Dehghanian, "Powering Through Wildfires: An Integrated Solution for Enhanced Safety and Resilience in Power Grids," in IEEE Transactions on Industry Applications, vol. 58, no. 3, pp. 4192-4202, May-June 2022, doi: 10.1109/TIA.2022.3160421.

[53] R. Serrano, M. Panteli and A. Parisio, "Risk Assessment of Power Systems Against Wildfires," 2023 IEEE Belgrade PowerTech, Belgrade, Serbia, 2023, pp. 01-06, doi: 10.1109/PowerTech55446.2023.10202967.

[54] S. Talebi, M. Vakilian, M. Bahrami and M. Lehtonen, "Equipment Hardening Strategies to Improve Distribution System Resilience against Wildfire," 2022 International Conference on Smart Energy Systems and Technologies (SEST), Eindhoven, Netherlands, 2022, pp. 1-6, doi: 10.1109/SEST53650.2022.9898416.

[55] M. Abdelmalak and M. Benidris, "Enhancing Power System Operational Resilience Against Wildfires," in IEEE Transactions on Industry Applications, vol. 58, no. 2, pp. 1611-1621, March-April 2022, doi: 10.1109/TIA.2022.3145765.

[56] H. Gao, Y. Chen, S. Mei, S. Huang, and Y. Xu, “Resilience-oriented pre-hurricane resource allocation in distribution systems considering electric buses,” Proc. IEEE, vol. 105, no. 7, pp. 1214–1233, 2017.

[57] M. Esfahani, N. Amjady, B. Bagheri, and N. D. Hatziargyriou, "Robust resiliency-oriented operation of active distribution networks considering windstorms," IEEE Trans. Power Syst., vol. 35, no. 5, pp. 3481–3493, 2020.

[58] H. T. Nguyen, J. Muhs, and M. Parvania, "Preparatory operation of automated distribution systems for resilience enhancement of critical loads," IEEE Trans. Power Deliv., vol. 36, no. 4, pp. 2354–2362, 2020.

[59] Q. Zhang, Z. Wang, S. Ma, and A. Arif, "Stochastic pre-event preparation for enhancing resilience of distribution systems," Renew. Sustain. Energy Rev., vol. 152, p. 111636, 2021.

[60] Z. Wang and J. Wang, "Self-healing resilient distribution systems based on sectionalization into microgrids," IEEE Trans. Power Syst., vol. 30, no. 6, pp. 3139–3149, 2015.

[61] C. Chen, J. Wang, F. Qiu, and D. Zhao, "Resilient distribution system by microgrids formation after natural disasters," IEEE Trans. Smart Grid, vol. 7, no. 2, pp. 958–966, 2015.

[62] T. Ding, Y. Lin, Z. Bie, and C. Chen, "A resilient microgrid formation strategy for load restoration considering master-slave distributed generators and topology reconfiguration," Appl. Energy, vol. 199, pp. 205–216, 2017.

[63] Y. Wang et al., "Coordinating multiple sources for service restoration to enhance resilience of distribution systems," IEEE Trans. Smart Grid, vol. 10, no. 5, pp. 5781–5793, 2019.

[64] Q. Shi et al., "Network reconfiguration and distributed energy resource scheduling for improved distribution system resilience," Int. J. Electr. Power Energy Syst., vol. 124, p. 106355, 2021.

[65] Q. Shi et al., "Post-extreme-event restoration using linear topological constraints and DER scheduling to enhance distribution system resilience," Int. J. Electr. Power Energy Syst., vol. 131, p. 107029, 2021.

[66] A. Arif, S. Ma, Z. Wang, J. Wang, S. M. Ryan, and C. Chen, "Optimizing service restoration in distribution systems with uncertain repair time and demand," IEEE Trans. Power Syst., vol. 33, no. 6, pp. 6828–6838, 2018.

[67] A. Arif, Z. Wang, C. Chen, and J. Wang, "Repair and resource scheduling in unbalanced distribution systems using neighborhood search," IEEE Trans. Smart Grid, vol. 11, no. 1, pp. 673–685, 2019.

[68] S. Yao, P. Wang, and T. Zhao, "Transportable energy storage for more resilient distribution systems with multiple microgrids," IEEE Trans. Smart Grid, vol. 10, no. 3, pp. 3331–3341, 2018.

[69] W. Yuan, J. Wang, F. Qiu, C. Chen, C. Kang, and B. Zeng, "Robust optimization-based resilient distribution network planning against natural disasters," IEEE Trans. Smart Grid, vol. 7, no. 6, pp. 2817–2826, 2016.

[70] X. Wang, M. Shahidehpour, C. Jiang, and Z. Li, "Resilience enhancement strategies for power distribution network coupled with urban transportation system," IEEE Trans. Smart Grid, vol. 10, no. 4, pp. 4068–4079, 2018.

[71] S. Ma, S. Li, Z. Wang, and F. Qiu, "Resilience-oriented design of distribution systems," IEEE Trans. Power Syst., vol. 34, no. 4, pp. 2880–2891, 2019.

[72] Q. Shi et al., "Resilience-oriented DG siting and sizing considering stochastic scenario reduction," IEEE Trans. Power Syst., vol. 36, no. 4, pp. 3715–3727, 2020.

[73] IEEE standard for the specification of microgrid controllers, IEEE 2030.7-2017, 2017.

[74] C. Chen, J. Wang, F. Qiu and D. Zhao, "Resilient distribution system by microgrids formation after natural disasters," IEEE Trans. Smart Grid, vol. 7, no. 2, pp. 958-966, March 2016.

[75] M. N. Ambia, K. Meng, W. Xiao and Z. Y. Dong, "Nested formation approach for networked microgrid self-healing in islanded mode," IEEE Trans. Power Delivery, vol. 36, no. 1, pp. 452-464, Feb. 2021.

[76] K. S. A. Sedzro, X. Shi, A. J. Lamadrid and L. F. Zuluaga, "A heuristic approach to the post-disturbance and stochastic pre-disturbance microgrid formation problem," IEEE Trans. Smart Grid, vol. 10, no. 5, pp. 5574-5586, Sept. 2019.

[77] F. H. Aghdam, N. T. Kalantari, B. Mohammadi-Ivatloo, "A stochastic optimal scheduling of multi-microgrid systems considering emissions: A chance constrained model," J. Cleaner Prod., vol. 275, pp. 122965, Dec. 2020.

[78] S. Lei, C. Chen, Y. Li and Y. Hou, "Resilient disaster recovery logistics of distribution systems: co-optimize service restoration with repair crew and mobile power source dispatch," IEEE Trans. Smart Grid, vol. 10, no. 6, pp. 6187-6202, Nov. 2019.
[79] G. Strbac, N. Hatziargyriou, J. P. Lopes, C. Moreira, A. Dimeas, and D. Papadaskalopoulos, "Microgrids: Enhancing the resilience of the european megagrid," IEEE Power Energy Mag., vol. 13, no. 3, pp. 35– 43, May-Jun. 2015.

[80] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al-Turki, "Networked microgrids for enhancing the power system resilience," Proc. IEEE, vol. 105, no. 7, pp. 1289–1310, Jul. 2017.

[81] Y. Wang, A. O. Rousis, and G. Strbac,"Resilience-driven optimal sizing and pre-positioning of mobile energy storage systems in decentralized networked microgrids," Appl. Energy, vol. 305, p. 117921, 2022.

[82] D. Qiu, Y. Wang, W. Hua, and G. Strbac, "Reinforcement learning for electric vehicle applications in power systems: A critical review." Renewable and Sustainable Energy Reviews, vol. 173, p. 113052, Mar. 2023.

[83] A. Zakaria, F. B. Ismail, M. S. H. Lipu and M. A. Hannan, "Uncertainty models for stochastic optimization in renewable energy applications," Renew. Energy, vol. 145, pp. 1543-1571, Jan. 2020.

[84] M. Choobineh, B. Ansari, and S. Mohagheghi, "Vulnerability assessment of the power grid against progressing wildfires," Fire Safety Journal, vol. 73, pp. 20–28, 2015.

[85] R. Billinton and W. Li, Reliability Assessment of Electric Power Systems Using Monte Carlo Methods. Boston, MA: Springer US, 1994. doi: 10.1007/978-1-4899-1346-3.

[86] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and Quantification of Operational and Infrastructure Resilience in Power Systems," IEEE Transactions on Power Systems, vol. 32, no. 6, pp. 4732–4742, 2017, doi: 10.1109/TPWRS.2017.2664141.

[87] "Resilient Electricity Networks for Great Britain (RESNET)." Accessed: Feb. 07, 2022. [Online]. Available: https://gtr.ukri.org/projects?ref=EP%2FI035757%2F1#/tabOverview

[88] Noebels, M., Preece, R., Panteli, M. "AC Cascading Failure Model for Resilience Analysis in Power Networks." IEEE Systems Journal (2020).

[89] M. F. Uddin, "Addressing Accuracy Paradox Using Enhanched Weighted Performance Metric in Machine Learning," 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 2019, pp. 319-324, doi: 10.1109/ITT48889.2019.9075071.

[90] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '16), New York, NY, USA: Association for Computing Machinery, 2016, pp. 785-794. [Online]. Available: https://doi.org/10.1145/2939672.2939785.

[91] C. Chen, J. Wang, F. Qiu, and D. Zhao, "Resilient distribution system by microgrids formation after natural disasters," IEEE Trans. Smart Grid, vol. 7, no. 2, pp. 958–966, Mar. 2016.

[92] T. Ding, Y. Lin, G. Li, and Z. Bie, "A new model for resilient distribution systems by microgrids formation," IEEE Trans. Power Syst., vol. 32, no. 5, pp. 4145–4147, Sep. 2017.

[93] IBM ILOG CPLEX, 2019. [Online]. Available: https://www.ibm.com/analytics/cplex-optimizer

[94] GAMS Development Corporation, 2019. [Online]. Available: http://www.gams.com

[95] A. Poudyal, S. Poudel, and A. Dubey, "Risk-based active distribution system planning for resilience against extreme weather events," IEEE Trans. Sustain. Energy, Nov. 2022.

[96] IEEE PES Task Force, "Methods for analysis and quantification of power system resilience," IEEE Trans. Power Syst., 2022.

[97] Y. Wang, A. O. Rousis, and G. Strbac, "On microgrids and resilience: A comprehensive review on modeling and operational strategies," Renew. Sust. Energ. Rev., vol. 134, p. 110313, Dec. 2020.

[98] N. Hatziargyriou, H. Asano, R. Iravani and C. Marnay, "Microgrids", IEEE Power Energy Mag., vol. 5, no. 4, pp. 78-94, Jul./Aug. 2007.

[99] D. E. Olivares et al., "Trends in microgrid control", IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1905-1919, Jul. 2014.

[100] S. Lei, J. Wang, C. Chen, and Y. Hou, "Mobile emergency generator pre-positioning and real-time allocation for resilient response to natural disasters," IEEE Trans. Smart Grid, vol. 9, no. 3, pp. 2030–2041, May 2018.

[101] S. Lei, C. Chen, H. Zhou, and Y. Hou, "Routing and scheduling of mobile power sources for distribution system resilience enhancement," IEEE Trans. Smart Grid, vol. 10, no. 5, pp. 5650–5662, Sept. 2019.

[102] Q. Zhang, Z. Wang, S. Ma, and A. Arif, "Stochastic pre-event preparation for enhancing resilience of distribution systems," Renew. Sust. Energ. Rev., vol. 152, p. 111636, Dec. 2021.

[103] Y. Wang, A. O. Rousis, and G. Strbac, "A three-level planning model for optimal sizing of networked microgrids considering a trade-off between resilience and cost," IEEE Trans. Power Syst., vol. 36, no. 6, pp. 5657– 5669, Apr. 2021.

[104] S. Lei, C. Chen, Y. Li, and Y. Hou, "Resilient disaster recovery logistics of distribution systems: Co-optimize service restoration with repair crew and mobile power source dispatch," IEEE Trans. Smart Grid, vol. 10, no. 6, pp. 6187–6202, Nov. 2019.

[105] R. S. Sutton and A. G. Barto, Reinforcement learning: An introduction. MIT press, 2018.

[106] Gurobi Optimization, LLC, "Gurobi Optimizer Reference Manual," 2023. [Online]. Available: https://www.gurobi.com

[107] Martín Abadi, et. al., TensorFlow: Large-scale machine learning on heterogeneous systems, 2015. Software available from tensorflow.org.

[108] Wu X, Conejo AJ. "An efficient tri-level optimization model for electric grid defense planning," IEEE Trans Power Syst, vol. 32, no. 4, pp. 2984-94, Jul. 2017.

[109] Lin Y, Bie Z. "Tri-level optimal hardening plan for a resilient distribution system considering reconfiguration and DG islanding," Appl. Energy, vol. pp. 1266–1279, Jan. 2018.

[110] Zeng B, Zhao L. "Solving two-stage robust optimization problems using a column-and-constraint generation method," Oper. Res. Lett., vol. 41, no. 5, pp. 457–61, Sept. 2013.

[111] E. L. Ratnam, S. R. Weller, C. M. Kellett, and A. T. Murray, "Residential load and rooftop P generation: an Australian distribution network dataset," Int. J. Sustain. Energy, vol. 36, no. 8, pp. 787–806, Oct. 2017.

6.2 ACRONYMS

Table 14. Acronyms

Acronym	Meaning
WP3	Work Package 3
M24	Month 24 of the R2D2 project
EPES	Electrical Power Energy Systems
OT	Operational technology
IT	Information Technology
DS	Distribution System
AMI	Advanced metering infrastructure
BC	Business Case
CTI	Cyber Treat Intelligence
DER	Distributed energy resources
DMS	Distribution Management System

DSO	Distribution System Operator
EU	European Union
HV	High Voltage
IoT	Internet of Things
MPS	Mobile Power Source
MESS	Mobile Energy Storage System
LFSM-O	Limited Frequency Sensitive Mode – Over-frequency
LV	Low Voltage
MV	Medium Voltage
PMU	Phasor Measurement Unit
RES	Renewable Energy Sources
RCC or RSC	Regional Coordination Centre / Regional Security Coordinator
RTU	Remote Terminal Unit
SCADA	System Control and Data Acquisition
TSO	Transmission System Operator
UC	Use Case
MEG	Mobile Energy Generator
MG	Microgrid
NMG	Networked Microgrid
RC	Repair Crews
RA	Risk Assessment
CSET	Cyber Security Evaluation Tool
CISA	Cybersecurity and Infrastructure Security Agency
SG	Security Guidance
MAB	Multi-armed Bandits
SDN	Software-Defined Networking
IED	Intelligent Electronic Device
DoS	Denial of Service
APT	Advanced Persistent Threat
HILF	High-Impact Low-Frequency
PH	Progressive Hedging
BCD	Block Coordinate Descent
CCG	Column-and-Constraint Generation
DG	Distributed Generator
DLR	Dynamic Line Rating
CL	Critical Loads
DAD	Defender-Attacker-Defender
RTP	Risk Treatment Plan
UI	User Interface
VM	Virtual Machine
PLC	Programmable Logic Controllers
DB	Database
VA	Vulnerability Assessment
CPE	Common Platform Enumeration
IoC	Indicator of Compromise
ML	Machine learning
CTC	Cyber Terrain Characterization
CVSS	Common Vulnerability Scoring System
NLP	Natural Language Processing
Tfidf	Term frequency – inverse document frequency
FCM	Fuzzy Cognitive Map
AC-CFM	AC Cascading Failure Model
XGBoost	eXtreme Gradient Boosting
SMOTE	Synthetic Minority Over-sampling Technique
RTS	Reliability Test System
ESS	Energy Storage System
RAMLP	Resiliency Assessment Metrics by Linear Programming Model
LF	Load Flow

EENS	Expected Energy Not Supplied
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
GAMS	General Algebraic Modelling Language
RoCoF	Rate of Change of Frequency
MGCC	Microgrid Central Controller
WT	Wind Turbine
MES	Mobile Energy System
MESS	Mobile Energy System Station
EV	Electric Vehicle
PV	Photovoltaic
MPS	Mobile Power Source
RL	Reinforcement Learning
MDP	Markov Decision Process
MARL	Multi-agent Reinforcement Learning
MISP	Malware Information Sharing Platform & Threat Sharing
API	Application Programming interface
STIX	Structured Threat Information eXpression
IDS/IPS	Intrusion Detection/Prevention System
CVE	Common Vulnerabilities and Exposure
NVD	National Vulnerability Database
NIST	National Institute of Standards and technology
HTTPS	Hypertext Transfer Protocol Secure

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.