



# From conceptual use cases to real demonstration – Digital Twin for cyber-physical grid resilience

Deliverable No: D5.1  
Work package: WP5

Official delivery date: 30.09.2026  
Actual delivery date: 01.10.2026

Dissemination level: Public



Project: 101136119 | HORIZON-CL5-2023-D3-01 | [www.twineu.net](http://www.twineu.net)

© Copyright 2024-2027 by the TwinEU Consortium. All Rights Reserved.

### Disclaimer

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.

| Document Authors         |                            |
|--------------------------|----------------------------|
| May Myat Thwe (TUD)      | Geethu Joseph (CRESYM)     |
| Shafiulla Syed (TUD)     | Lenos Hadjidemetriou (UCY) |
| Abhishek Saini (TUD)     | Olivier Bretteville (RTE)  |
| Simona Renzaglia (TUD)   | Thibaut Vermeulen (RTE)    |
| Alexandru Stefanov (TUD) | David Herve (RTE)          |
| Bahman Ahmadi (TUD)      | Markos Asprou (UCY)        |
| Peter Palensky (TUD)     | Lucas Saludjian (RTE)      |

| Version | Date       | Authors                                                                                                     | Notes                 |
|---------|------------|-------------------------------------------------------------------------------------------------------------|-----------------------|
| 0.1     | 26.11.2024 | May Myat Thwe, Shafiulla Syed, Alexandru Stefanov                                                           | 1 <sup>st</sup> draft |
| 0.2     | 28.05.2025 | May Myat Thwe, Shafiulla Syed, Alexandru Stefanov, Geethu Joseph, Lenos Hadjidemetriou, Olivier Bretteville | 2 <sup>nd</sup> draft |
| 0.3     | 15.05.2026 | All authors                                                                                                 | 3 <sup>rd</sup> draft |
| 0.4     | 17.07.2026 | May Myat Thwe, Shafiulla Syed, Abhishek Saini, Alexandru Stefanov, Simona Renzaglia                         | 4 <sup>th</sup> draft |
| 0.5     | 15.09.2026 | All authors                                                                                                 | 5 <sup>th</sup> draft |
| 0.6     | 23.09.2026 | May Myat Thwe, Shafiulla Syed, Abhishek Saini, Bahman Ahmadi, Peter Palensky                                | 6 <sup>th</sup> draft |
| 1       | 24.09.2026 | Alexandru Stefanov                                                                                          | Final draft           |

|                                     |                                           |
|-------------------------------------|-------------------------------------------|
| Responsible Partner                 | TUD (Delft University of Technology)      |
| Checked by WP leader                | Alexandru Stefanov (TUD), 28.09.2026      |
| Verified by the Appointed Reviewers | Vokony István (BME), 09.09.2026           |
| Approved by Project Coordinator     | Padraic McKeever (Fraunhofer), 01.10.2026 |

## Table of Contents

|                                                                                                |    |
|------------------------------------------------------------------------------------------------|----|
| Executive Summary .....                                                                        | 11 |
| 1 Introduction .....                                                                           | 12 |
| 1.1 Background on Digital Twins and Their Significance in Cyber-Physical Grid Resilience ..... | 12 |
| 1.2 Key Challenges in Power Systems Cyber-Physical Grid Resiliency .....                       | 15 |
| 1.3 Objectives of the Work Reported in this Deliverable .....                                  | 16 |
| 1.4 Outline of the Deliverable .....                                                           | 17 |
| 2 Cyber Security Threats in Power Systems .....                                                | 18 |
| 2.1 Man-in-the-Middle Attacks .....                                                            | 18 |
| 2.1.1 Eavesdropping .....                                                                      | 18 |
| 2.1.2 Spoofing .....                                                                           | 19 |
| 2.1.3 False Data Injection .....                                                               | 20 |
| 2.2 Network-based Attacks .....                                                                | 20 |
| 2.2.1 Network Reconnaissance .....                                                             | 20 |
| 2.2.2 Lateral Movement .....                                                                   | 21 |
| 2.3 Phishing .....                                                                             | 21 |
| 2.4 Denial-of-Service Attacks .....                                                            | 22 |
| 3 T5.2 Overview .....                                                                          | 23 |
| 3.1 Challenges Addressed by the Task .....                                                     | 23 |
| 3.2 Architecture of Digital Twin and Description .....                                         | 23 |
| 3.3 Development Roadmap .....                                                                  | 24 |
| 3.3.1 Implemented Functions .....                                                              | 24 |
| 3.3.2 Software Platforms and Datasets Used for DT Development .....                            | 24 |
| 3.3.3 Timeline and Milestones .....                                                            | 25 |
| 3.3.4 Demonstration Plan .....                                                                 | 25 |
| 3.4 Developed Framework and Results Demonstration .....                                        | 26 |
| 3.4.1 Development of Integrated Digital Twin .....                                             | 26 |
| 3.4.2 Executed Cyber Attack Scenarios within DT Testbed .....                                  | 30 |
| 3.4.3 Anomaly Detection Using Federated Learning .....                                         | 31 |
| 3.4.4 Impact and Cascading Failure Analysis on the Operation of Interconnected Power Grids     | 33 |
| 3.5 Alignment with Digital Twin Concepts .....                                                 | 59 |
| 4 T5.3 Overview .....                                                                          | 60 |
| 4.1 Challenges Addressed by the Task .....                                                     | 60 |
| 4.2 Architecture of Digital Twin and Description .....                                         | 61 |
| 4.3 Development Roadmap .....                                                                  | 62 |
| 4.3.1 Implemented Functions .....                                                              | 62 |
| 4.3.2 Software Platforms and Datasets Used for DT Development .....                            | 63 |
| 4.3.3 Timeline and Milestones .....                                                            | 64 |

|       |                                                                                        |     |
|-------|----------------------------------------------------------------------------------------|-----|
| 4.3.4 | Demonstration Plan .....                                                               | 64  |
| 4.4   | Developed Framework and Results Demonstration .....                                    | 64  |
| 4.4.1 | Phase 1-Setup the Digital Twin .....                                                   | 64  |
| 4.4.2 | Phase 2-Development and Integration of Controllers and Coordination of Flexibility...  | 66  |
| 4.4.3 | Phase 3-Development of the Communication Layer .....                                   | 68  |
| 4.4.4 | Phase 4-Digital Twin Validation.....                                                   | 70  |
| 4.5   | Alignment with Digital Twin Concepts .....                                             | 73  |
| 5     | T5.4 Overview on Abnormal Market Participation Detection and Protocol Activation ..... | 75  |
| 5.1   | Challenges Addressed by the Task .....                                                 | 75  |
| 5.2   | Architecture of Digital Twins and Description.....                                     | 75  |
| 5.2.1 | ANELL's Distribution Grid DT and OMIE's LFM DT (Implementation of BUC Ib04).....       | 75  |
| 5.2.2 | REN's Transmission Grid DT and Portuguese Distribution Grid DT model (UC Ib12) .....   | 79  |
| 5.3   | Development Roadmap.....                                                               | 81  |
| 5.3.1 | ANELL's Distribution Grid DT and OMIE's LFM DT (Implementation of UC Ib04).....        | 81  |
| 5.3.2 | REN's Transmission Grid DT and Portuguese Distribution Grid DT model (UC Ib12) .....   | 81  |
| 5.4   | Developed Framework and Results Demonstration Results .....                            | 82  |
| 5.4.1 | ANELL's Distribution Grid DT and OMIE's LFM DT (Implementation of UC Ib04).....        | 82  |
| 5.4.2 | REN's Transmission Grid DT and Portuguese Distribution Grid DT model (UC Ib12) .....   | 84  |
| 5.5   | Alignment with Digital Twin Concepts .....                                             | 84  |
| 6     | T5.5 Overview .....                                                                    | 86  |
| 6.1   | Challenges Addressed by the Task .....                                                 | 86  |
| 6.2   | Architecture of Digital Twin and Description .....                                     | 87  |
| 6.3   | Development Roadmap.....                                                               | 89  |
| 6.3.1 | Implemented Functions .....                                                            | 89  |
| 6.3.2 | Software Platforms and Datasets Used for DT Development.....                           | 90  |
| 6.3.3 | Timeline and Milestones .....                                                          | 90  |
| 6.3.4 | Demonstration Plan .....                                                               | 90  |
| 6.4   | Developed Framework and Results Demonstration .....                                    | 94  |
| 6.4.1 | Cyber Physical DT Architecture .....                                                   | 94  |
| 6.4.2 | Event-Driven Orchestration Framework .....                                             | 94  |
| 6.4.3 | Real-Time Digital Representation of the Physical Grid .....                            | 94  |
| 6.4.4 | Information Flow Model .....                                                           | 94  |
| 6.4.5 | Implementation of Trainer and Trainee SCADA Interfaces.....                            | 95  |
| 6.4.6 | Scenario Generation and Game Master Control.....                                       | 97  |
| 6.4.7 | Operator Training Scenarios .....                                                      | 97  |
| 6.4.8 | Logging and replay basis .....                                                         | 98  |
| 6.5   | Alignment with Digital Twin Concepts .....                                             | 98  |
| 7     | Conclusion .....                                                                       | 99  |
|       | References .....                                                                       | 100 |

## List of Figures

|                                                                                              |    |
|----------------------------------------------------------------------------------------------|----|
| Figure 1-1: Digital twin [4].                                                                | 12 |
| Figure 1-2: Digital twin component.                                                          | 13 |
| Figure 1-3: The cyber physical system framework.                                             | 15 |
| Figure 2-1: Examples of cyber attacks in power systems.                                      | 18 |
| Figure 3-1: Overall architecture of DT for cyber security assessment.                        | 23 |
| Figure 3-2: Timeline for the DT development for cyber security assessment.                   | 25 |
| Figure 3-3: SLD of 380kV Dutch transmission network.                                         | 27 |
| Figure 3-4: Geography of synthetic Dutch transmission and distribution network.              | 27 |
| Figure 3-5: Integration of Dutch transmission and distribution network.                      | 28 |
| Figure 3-6: SLD of Dutch distribution network.                                               | 28 |
| Figure 3-7: Digital twin module for attack detection using federated deep packet inspection. | 31 |
| Figure 3-8: Performance of federated DPI under IID and non-IID setting.                      | 33 |
| Figure 3-9: Cascading failure caused by the initial cyber attack events.                     | 35 |
| Figure 3-10: Bus voltages and frequency.                                                     | 35 |
| Figure 3-11: Bus voltage angles and total load.                                              | 36 |
| Figure 3-12: Impact of a cyber attack on Dutch transmission network.                         | 37 |
| Figure 3-13: UFLS of loads and line over load tripping.                                      | 37 |
| Figure 3-14: Bus voltage angles and total active load.                                       | 37 |
| Figure 3-15: Bus voltages and bus frequencies.                                               | 38 |
| Figure 3-16: Generator GNA380 tripping.                                                      | 39 |
| Figure 3-17: Generator EEM15_3 tripping.                                                     | 40 |
| Figure 3-18: Generator DKG_15 tripping.                                                      | 40 |
| Figure 3-19: HVDC interconnector tripping.                                                   | 41 |
| Figure 3-20: Line tripping by out of zone distance protection.                               | 41 |
| Figure 3-21: Bus voltages and frequency dynamics.                                            | 42 |
| Figure 3-22: Bus voltage angles and total load.                                              | 42 |
| Figure 3-23: Cyber attack impact assessment caused by element switching attack.              | 43 |
| Figure 3-24: Cyber attack impact assessment caused by substation switching attack.           | 43 |
| Figure 3-25: Cyber attack impact assessment caused by substation spoofing attack.            | 44 |
| Figure 3-26: Flow chart of PNR quantification method.                                        | 46 |
| Figure 3-27: Bus voltages dynamics and PNR caused by switching cyber attack scenario.        | 50 |
| Figure 3-28: Weighted correlation matrix before reaching the PNR.                            | 50 |
| Figure 3-29: Weighted correlation matrix during the PNR.                                     | 51 |
| Figure 3-30: Elements disconnected caused by switching cyber attack scenario.                | 52 |

|                                                                                                                                                                                                 |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Figure 3-31: The SLD of the synthetic digital model of the Dutch power system (a) without and (b) with the mitigation strategy. Different colours indicate the voltage levels and loading. .... | 54 |
| Figure 3-32: Bus voltages (a) before and (b) after applying the mitigation strategy. ....                                                                                                       | 55 |
| Figure 3-33: Bus voltage angles (a) before and (b) after applying the mitigation strategy. ....                                                                                                 | 55 |
| Figure 3-34: Bus frequency (a) before and (b) after applying the mitigation strategy. ....                                                                                                      | 56 |
| Figure 3-35: Total load (a) before and (b) after applying the mitigation strategy. ....                                                                                                         | 56 |
| Figure 3-36: The SLD of the synthetic digital model of the Dutch power system (a) without and (b) with the mitigation strategy. Different colours indicate the voltage levels and loading. .... | 57 |
| Figure 3-37: Bus voltages (a) before and (b) after applying the mitigation strategy. ....                                                                                                       | 58 |
| Figure 3-38: Bus voltage angles (a) before and (b) after applying the mitigation strategy. ....                                                                                                 | 58 |
| Figure 3-39: Bus frequency (a) before and (b) after applying the mitigation strategy. ....                                                                                                      | 58 |
| Figure 3-40: Total load (a) before and (b) after applying the mitigation strategy. ....                                                                                                         | 59 |
| Figure 4-1: High level architecture of the Cypriot digital twin. ....                                                                                                                           | 62 |
| Figure 4-2: Timeline for implementation of congestion management use case. ....                                                                                                                 | 64 |
| Figure 4-3: A feeder developed in Simulink for the Cypriot distribution grid digital twin. ....                                                                                                 | 66 |
| Figure 4-4: High level controller integration architecture. ....                                                                                                                                | 67 |
| Figure 4-5: ThinkSpeak interface. ....                                                                                                                                                          | 69 |
| Figure 4-6: Grafana interface for monitoring and visualization. ....                                                                                                                            | 70 |
| Figure 4-7: Validation results under normal operating conditions. ....                                                                                                                          | 71 |
| Figure 4-8: Cyber attack impact on the distribution grid operation. ....                                                                                                                        | 72 |
| Figure 5-1: ÉTER architecture. ....                                                                                                                                                             | 76 |
| Figure 5-2: OMIE's market operator information system (SIOM) architecture. ....                                                                                                                 | 77 |
| Figure 5-3: SGAM component layer. ....                                                                                                                                                          | 77 |
| Figure 5-4: SGAM Communication layer. ....                                                                                                                                                      | 78 |
| Figure 5-5: SGAM information layer. ....                                                                                                                                                        | 78 |
| Figure 5-6: UC Ib12 component layer. ....                                                                                                                                                       | 80 |
| Figure 5-7: UC Ib12 communication layer. ....                                                                                                                                                   | 80 |
| Figure 5-8: UC Ib12 information layer. ....                                                                                                                                                     | 80 |
| Figure 5-9: BUC implementation - development plan (Gantt chart). ....                                                                                                                           | 81 |
| Figure 5-10: UC Ib12 - development plan (Gantt chart). ....                                                                                                                                     | 81 |
| Figure 6-1: French digital twin architecture. ....                                                                                                                                              | 88 |
| Figure 6-2: Timeline for task 5.5 development. ....                                                                                                                                             | 90 |
| Figure 6-3: MQIS Substation ....                                                                                                                                                                | 90 |
| Figure 6-4: Base case situation ....                                                                                                                                                            | 92 |
| Figure 6-5: Ramp-up in wind power unit ....                                                                                                                                                     | 92 |
| Figure 6-6: Congestion on the grid ....                                                                                                                                                         | 93 |

|                                                                 |    |
|-----------------------------------------------------------------|----|
| Figure 6-7: Wind Curtailment.....                               | 93 |
| Figure 6-8: Training Session Lobby .....                        | 95 |
| Figure 6-9: Session Creation Interface .....                    | 96 |
| Figure 6-10: Game Master Interface for trainer supervision..... | 96 |
| Figure 6-11: Trainee SCADA visualization .....                  | 97 |

## List of Tables

|                                                                                                                                               |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------|----|
| Table 1: Overview of the dynamic model and coordinated protection schemes for the integrated Dutch transmission and distribution network..... | 27 |
| Table 2: Cascading events caused by switching cyber attack.....                                                                               | 34 |
| Table 3: Cascading events caused by cyber attack load event. ....                                                                             | 38 |
| Table 4: Cascading events caused by spoofing cyber attack event. ....                                                                         | 39 |

## List of Abbreviations and Acronyms

| Acronym | Meaning                                  |
|---------|------------------------------------------|
| ADMS    | Advanced Distribution Management System  |
| AI      | Artificial Intelligence                  |
| AMI     | Advanced Metering Infrastructure         |
| APT     | Advanced Persistent Threat               |
| AVR     | Automatic Voltage Regulator              |
| BESS    | Battery Energy Storage System            |
| BFS     | Breadth-First Search                     |
| CPPS    | Cyber Physical Power Systems             |
| CPS     | Cyber Physical System                    |
| CRoF    | Control Room of the Future               |
| DDoS    | Distributed Denial of Service            |
| DER     | Distributed Energy Resources             |
| DNP3    | Distributed Network Protocol             |
| DoS     | Denial of Service                        |
| DSO     | Distribution System Operator             |
| DT      | Digital Twin                             |
| EAC     | Electricity Authority of Cyprus          |
| EWT     | Empirical Wavelet Transform              |
| FDI     | False Data Injection                     |
| FL      | Federated Learning                       |
| FSP     | Flexibility Service Provider             |
| GIS     | Geographic Information System            |
| GOOSE   | Generic Object-Oriented Substation Event |

|        |                                                  |
|--------|--------------------------------------------------|
| GOV    | Governor                                         |
| GPS    | Global Positioning System                        |
| GRU    | Gated Recurrent Unit                             |
| GUI    | Graphical User Interface                         |
| HIL    | Hardware-in-the-Loop                             |
| HMAC   | Hash based Message Authentication Codes          |
| HAS    | Hilbert Spectral Analysis                        |
| HT     | Hilbert Transform                                |
| IA     | Instantaneous Amplitude                          |
| ICMP   | Internet Control Message Protocol                |
| ID     | Instantaneous Damping                            |
| IDPS   | Intrusion Detection and Prevention Systems       |
| IED    | Intelligent Electronics Devices                  |
| IF     | Instantaneous Frequency                          |
| IIDM   | iTelsa Internal Data Model                       |
| IMF    | Intrinsic Mode Function                          |
| KPI    | Key Performance Indicator                        |
| LFMO   | Local Flexibility Market Operator                |
| MILP   | Mixed-Integer Linear Programming                 |
| MiTM   | Man in the Middle                                |
| ML     | Machine Learning                                 |
| MO     | Market Operator                                  |
| MV     | Medium Voltage                                   |
| OPC UA | Open Platform Communication Unified Architecture |
| OT     | Operational Technology                           |
| PMU    | Phasor Measurement Unit                          |

|       |                                          |
|-------|------------------------------------------|
| PNR   | Point of No Return                       |
| PSVM  | Positive-Sequence Voltage Magnitude      |
| PV    | Photovoltaic                             |
| RES   | Renewable Energy Sources                 |
| RMS   | Root Mean Square                         |
| ROCOF | Rate of Change of Frequency              |
| RSA   | Rivest Shamir Adleman                    |
| RTDS  | Real-Time Digital Simulator              |
| RTS   | Real-Time Simulator                      |
| RTU   | Remote Terminal Unit                     |
| SCADA | Supervisory Control and Data Acquisition |
| SE    | State Estimation                         |
| SGAM  | Smart Grid Architecture Model            |
| SMTP  | Simple Mail Transfer Protocol            |
| SO    | System Operator                          |
| SV    | Sampled Values                           |
| TCP   | Transmission Control Protocol            |
| TSO   | Transmission System Operator             |
| UFLS  | Under Frequency Load Shedding            |
| URL   | Uniform Resource Locator                 |
| UVLS  | Under Voltage Load Shedding              |
| WP    | Work Package                             |

## Executive Summary

The D5.1 deliverable presents the progress and results of Work Package 5 (WP5) of the TwinEU project, as carried out by the WP5 partners. The primary goal of this work package is to develop and demonstrate a Digital Twin (DT) framework tailored to specific use cases, aiming to identify and address various cyber security, market participation, and operational challenges in Cyber-Physical Power Systems (CPPS).

A key aspect of the assessment is the analysis of cyber security vulnerabilities and potential impact of cyber attacks on power systems with high penetration of Renewable Energy Sources (RES). Major cyber security threats identified include man-in-the-middle attacks, network-based intrusions, and Denial-of-Service (DoS) attacks targeting the CPPS.

This report addresses the various challenges faced by each partner in the work package to deliver digital twins for cyber-physical grid resilience from conceptual use cases to real demonstration. Task 5.2 focuses on the development of a digital twin of the power system and demonstrates cyber security applications. It detected the early-stage cyber attacks in Operational Technology (OT) communication networks, analysed the dynamics of power system cascading failures, and quantified the Point of No Return (PNR). Task 5.3 investigates the use of what-if scenarios within digital twin environments to assess the resilience of the power grid under various conditions. Task 5.4 deals with the detection of abnormal market behaviour and a range of potential threats to the power system. Task 5.5 is dedicated to the development of a digital twin-based demonstrator aimed at supporting power system operator training, leveraging existing tools and frameworks.

Each pilot has reported their specific use cases, addressed the challenges in their task, and provided a detailed description of their DT architecture and demonstration, along with the development roadmap. The demonstrations provide evidence of the T5.1 requirements within their respective pilot environments and tested scenarios. Where applicable, they also interact with interfaces and information exchanges developed in WP3 and WP4, contributing to the broader TwinEU federation framework. Federated learning across substations, as demonstrated in Task 5.2, is distinguished from federation and interoperability between digital twins.

Overall, D5.1 demonstrates the feasibility of the developed DT capabilities for the targeted WP5 use cases and documents their demonstrated maturity while the detailed implementation results and final validation outcomes are reported in Deliverable D5.2. Validation beyond the reported scenarios and pilot configurations, as well as broader deployment and operational-scale assessment, falls outside the scope of the work reported in this deliverable.



Unlike traditional simulation techniques, which provide only basic insights into system behaviour based on assumptions of possible events, a DT enables real-time scenario analysis of what is happening in the system. This allows for immediate and informed decision-making. Additionally, it helps predict future events and supports proactive control strategies by running simulations on the virtual model, continuously updated with real-time data from the physical system.

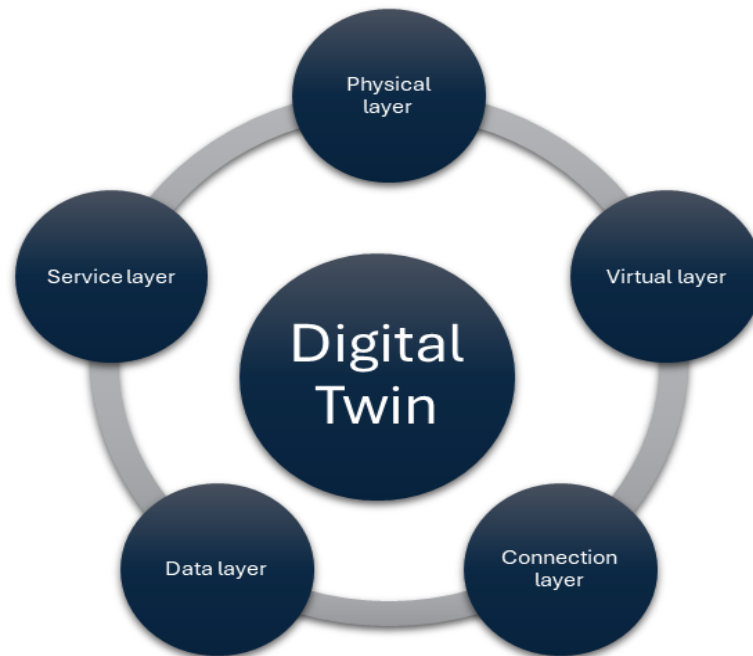


*Figure 1-2: Digital twin component.*

In its early stages, a DT was defined by three main components, such as a.) physical system, b.) virtual system, and c.) connection. The modern interpretation expands this into a five-dimensional model [3] as shown in Figure 1-2.

1. **Physical Layer:** Actual power grid elements like transformers, transmission lines, loads, generators, and substations. This layer reflects real-world infrastructure that must be monitored and controlled for reliable operation.
2. **Virtual Layer:** A high-fidelity digital replica or simulation model of the physical system. Accurate modelling, which incorporates system nonlinearities and physical state variables using tools like DIgSILENT PowerFactory, Real-Time Digital Simulator (RTDS), and PSCAD, is crucial for avoiding misinterpretation and ensuring effective control.
3. **Connection Layer:** The secure communication infrastructure that links the physical and virtual systems, enabling bidirectional data exchange (e.g., measurements, breaker statuses, control signals). This layer uses communication protocols such as IEC 61850, Distributed Network Protocol (DNP3) and Open Platform Communications Unified Architecture (OPC UA) to support real-time operations, including alarms and controls.
4. **Data Layer:** Responsible for data management tasks such as storage, filtering, interpretation, normalization, and time synchronization. It plays a key role in applying Machine Learning (ML) techniques for anomaly detection, state estimation, and fault prediction, ensuring accurate and timely data delivery while supporting integrity and historical analytics.

5. **Service Layer:** A functional module that extracts value from the DT by providing decision support, fault detection, and control recommendations. This layer enhances predictive maintenance, system optimization, and operator interfaces.

This evolution enables broader functionalities such as real-time forecasting, fault detection, decision support, and system optimization. As a result of this advancement, many processes that were traditionally part of offline power system operations, such as system stability analysis, planning, model validation, and disturbance analysis, can now be integrated into the online operation of the grid. Moreover, conventional control rooms that relied on low-dimensional models for situational awareness are being replaced by more complex and responsive frameworks enabled by DTs.

Digital twin frameworks proposed in recent literature can be categorized based on their approach: model-based, data-driven, or a hybrid of both. Each approach offers unique benefits and levels of fidelity, supporting different aspects of real-time power system monitoring, analysis, and control. The cyber-physical power grid integrates the electrical infrastructure (physical layer), digital communication systems (cyber layer), and intelligent control mechanisms (decision layer). This digital framework plays a crucial role in enhancing grid reliability, security, and performance. Key capabilities include:

- 1. Real-Time Monitoring and Visualization:** The DT continuously receives real-time measurements and state updates from the physical grid, which allows operators to monitor the system dynamically and respond to events with improved accuracy. It supports condition-based maintenance and enhances situational awareness. If the DT provides outputs through computations within a guaranteed time equal to or less than the operational time step, it is considered to operate in real time.
- 2. Predictive Maintenance:** With continuous real-time data, high-fidelity simulations enable deeper insights into system behaviour under various conditions. This improves control strategies and helps detect potential failures early. ML algorithms utilize this data to forecast equipment degradation and optimize component efficiency.
- 3. Event-Based Simulations:** In the event of a disturbance, such as a fault, load change, generation fluctuation, or Rate of Change of Frequency (ROCOF) event, the current system state is transferred to the virtual environment. DT runs simulations there to evaluate corrective actions before applying them to the actual grid. If the simulation output is substantially faster than the system's operational time step, it allows the DT to predict outcomes early enough to support control or scheduling decisions proactively.
- 4. Optimization and Planning:** When computations exceed the acceptable real-time operation window, the DT becomes valuable for planning and design. It enables optimal power flow analysis, load forecasting, and grid expansion planning through detailed "what-if" simulations without impacting the actual grid. Moreover, DT offers a safe virtual environment to test protection relay settings, automation systems, and control strategies using real-time data, allowing for more practical and realistic testing before physical implementation.
- 5. Resilience Against Cyber Attacks:** Digital twins enhance grid security by supporting the development of Artificial Intelligence (AI) and ML-based intrusion detection and prevention systems. They help recognize abnormal behaviour caused by cyber attacks and recommend defence strategies, such as anomaly detection, intrusion detection, and intrusion prevention. This helps create a robust cyber security framework capable of responding to both known and emerging threats.

## 1.2 Key Challenges in Power Systems Cyber-Physical Grid Resiliency

The Cyber-Physical Power System (CPPS) is an integration of the physical power network with a cyber network. The physical network comprises traditional power system components such as generators, transmission lines, and loads, while the cyber layer includes the communication infrastructure, advanced information systems, and decision-making algorithms. The overall workflow of a CPPS can be broadly categorized into three major sections : Elements, Interconnections, and Functions, as shown in Figure 1-3.

- The elements section includes components from both the physical and cyber domains, such as power plants, substations, optical cables, sensors, and controllers.
- The interconnections represent the interaction between the physical and cyber domains, facilitated by the bidirectional flow of energy and information.
- At the core lies the function component, the brain of the system, which is responsible for perceiving system states, making control decisions, and ensuring stable and reliable operation of all interconnected components.

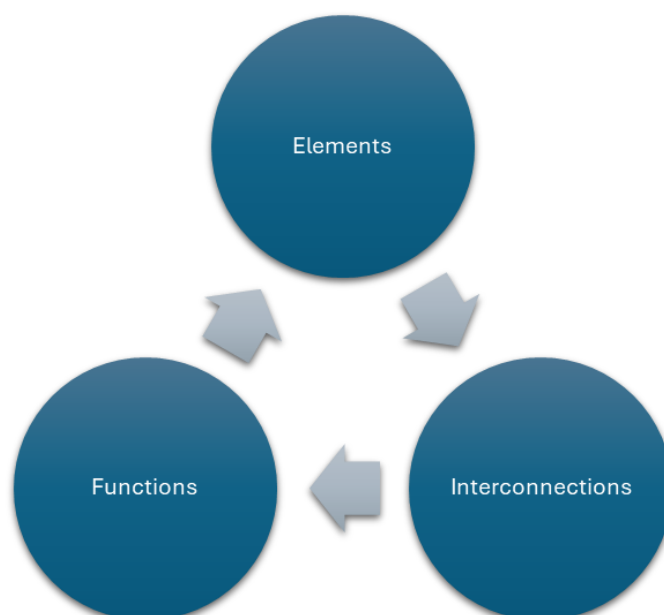


*Figure 1-3: The cyber physical system framework.*

The interconnection and interdependency between the cyber and physical components of a system significantly enhance system monitoring and enable more effective tracking of real-time system states, thereby contributing to high power system reliability and operational efficiency. However, while this CPS architecture offers substantial benefits, it also introduces several critical challenges. These include concerns related to cyber security, communication interdependencies, data and system privacy, and the need for secure control and protection operations within the power system network.

- **Cyber Security Threats** [8]: The major pillars of cyber security in CPS are Confidentiality, Integrity, and Availability, referred to as the CIA triad:
  - Confidentiality refers to the ability to prevent unauthorized access to sensitive information. It is essential for maintaining user privacy and protecting critical data from being disclosed to unauthorized individuals or systems.
  - Integrity ensures that data or resources cannot be altered or deleted without proper authorization. Cyber threats such as data tampering, false data injection, or

unauthorized deletion fall under integrity violations. Maintaining data accuracy and trustworthiness is vital for secure operation.

- o Availability ensures that data and services are accessible whenever required. In the context of CPS, this means that the system must remain functional and responsive, even during hardware failures or software upgrades. High availability is key to preventing disruptions in computing and control processes.

In recent years, cyber attacks targeting CPS have increased in both frequency and sophistication, involving diverse attack vectors and strategies. These evolving threats highlight the urgent need for robust cyber security frameworks to safeguard critical infrastructure.

- **Cyber and Physical Layer Interdependency** [9]: The interconnection between the cyber layer (communication and control) and the physical layer (smart grid infrastructure) creates a tightly coupled system where failures in one layer can affect the other, increasing complexity in system behaviour and resilience. Simply put, the overall performance of a CPS results from the interaction of multiple subsystems. Even minor deviations in the performance of any single subsystem, whether cyber or physical, can lead to operational instability and disrupt the functioning of the entire CPS. This interdependency makes it more challenging to meet the performance requirements of each individual subsystem within the CPS infrastructure.
- **Two-Way Communication** [10]: The CPS within a DT framework involves continuous bidirectional communication exchanging real-time system states and control commands between the physical and virtual networks. This ongoing interaction creates challenges in establishing a secure interface between the two layers. If these communication links are not adequately secured, they may become vulnerable entry points for potential cyber attacks.
- **Resilient Control and Protection** [11]: The integration of distributed energy resources has introduced uncertainty into the power grid, highlighting the need for highly coordinated control strategies to maintain system stability. Additionally, the complex interactions between cyber and physical components have made many conventional protection mechanisms incompatible with modern grid requirements. Therefore, it is essential to develop advanced protection mechanisms that can respond effectively to dynamic and evolving threats in real-time. Otherwise, attackers can reject or change this information and prevent the utility from taking necessary control actions. Compromised DER commands can cause power outages.
- **Trust and Privacy Concerns**: The creation of virtual or mirror models of the physical network often involves third-party consultants responsible for securing sensitive information and performing necessary analyses or modelling tasks. However, ensuring complete trust in these third parties can be challenging, especially regarding their ability to protect critical data. Therefore, implementing strong data encryption and security measures is essential to address privacy concerns and safeguard the integrity of the system.

### 1.3 Objectives of the Work Reported in this Deliverable

This deliverable aims at reporting demonstrations of digital twinning approaches aimed at assessing and enhancing the cyber-physical resilience of the power system. It presents the progress and results made within Work Package (WP) 5 as part of the digital twin development. The document outlines the challenges solved by each task in WP5, planning and development roadmap, system architecture, the timeline, key milestones, and the overall demonstration plan. Detailed implementation progress and results will be presented in a subsequent deliverable.

## **1.4 Outline of the Deliverable**

Chapter 2 discusses the vulnerabilities of the cyber-physical system to various types of cyber attacks, both at the system and cyber network levels. Chapters 3 through 6 outline the specific challenges encountered in each task and detail the development and architecture of the digital twin frameworks designed by the individual partners included in work package 5.

## 2 Cyber Security Threats in Power Systems

Along with the increased digitalization in the energy sector, the ways the cyber-physical power systems operate have also transformed. Digitalization of CPPS, which are part of critical infrastructures, enhances monitoring and control operations, intelligence, and advanced analytics. While implementing ICT in power grid operations offers efficiency, it introduces new vulnerabilities and cyber threats. While a cyber attack on typical ICT systems mainly only affects digital information, an attack on the ICT, OT, Supervisory Control, and Data Acquisition (SCADA) systems of a CPPS can potentially affect the real physical world and deliver more devastating damage. For example, cyber attacks on the power grid potentially deliver power outages and physical damages, loss of load, and power system instability. Moreover, sophisticated cyber attacks may cause system-wide cascading failures, leading to a blackout. Cyber security incidents related to power grids have been reported worldwide, as highlighted in Figure 2-1. For example, a BlackEnergy malware-based cyber attack on the power grid in Ukraine in 2015 resulted in power outages, affecting more than 30 substations and 225,000 customers [5]. Other cyber incidents associated with industrial CPPS are Stuxnet at the Iran nuclear power plant and VPNFilter on SCADA protocols. Similarly, in 2016, cyber attacks employed complex Advanced Persistent Threat (APT) strategies that took several months to reach their objectives and caused power outages. While these systems are vital infrastructures for modern society, this interconnectedness also makes CPS susceptible to cyber attacks, which can lead to severe consequences, including power system blackouts. Therefore, understanding and analysing cyber attack vectors on CPS is crucial, with the ultimate goal of devising and implementing effective defence strategies.

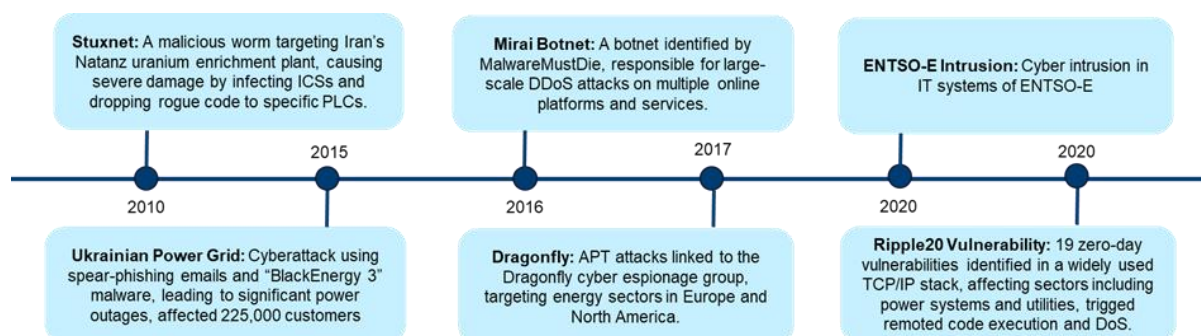


*Figure 2-1: Examples of cyber attacks in power systems.*

Many cyber attack techniques can potentially be applied to target power grids. This chapter identifies such attacks into different categories: man-in-the-middle attacks, network-based attacks, phishing, and denial of service.

### 2.1 Man-in-the-Middle Attacks

Man-in-the-Middle (MiTM) attacks, cyber attacks in which adversaries position themselves between two or more hosts to observe and maliciously interfere with communication traffic, pose a significant risk to power grids. These attacks, which can be eavesdropping, spoofing, and False Data Injection (FDI), can disrupt the regular operation of power grids.

#### 2.1.1 Eavesdropping

Eavesdropping, or sniffing, is an attack where adversaries intercept information transmitted over the network. The goal of eavesdropping is to intercept and gather information about the contents of

the transmitted data. Unlike other attacks, adversaries seek to observe and not change legitimate communication. Encrypted protocols can be used to mitigate the threat of eavesdropping. Due to encryption, adversaries or third parties cannot easily decipher the contents of the transmitted data. However, in a real SCADA system, most dataflows are unencrypted. Moreover, SCADA end devices such as station control systems, RTUs, protection relays, and merging units mainly rely on a broadcast communication mechanism, for instance, the Distributed Network Protocol (DNP3), in SCADA communications [6]. Such broadcast mechanisms are susceptible to eavesdropping and sniffing attacks. Adversaries can easily intercept communications by gaining unauthorized access to the OT system and exploiting the vulnerabilities of the broadcast communication mechanism.

Therefore, eavesdropping, a key component of advanced persistent threats, plays a crucial role, especially during the reconnaissance stage. It serves as a stealthy mechanism for adversaries to gather network intelligence passively, highlighting the need for proactive measures to counter this threat. The eavesdropping is mainly focused on the Advanced Metering Infrastructure (AMI). AMI establishes communications through wireless channels between a smart grid operator and smart metering devices. Adversaries may exploit the vulnerabilities present in wireless networks to intercept communications and capture transmitted data. Research also shows that eavesdropping can lead to privacy concerns for smart grid users, as seen in [14] and [15].

### 2.1.2 Spoofing

Spoofing is an attack where adversaries act as legitimate entities and disrupt normal communications. Such attacks can be performed through many forms of spoofing, such as emails, website URLs, text messages, Global Positioning System (GPS), and IP addresses. One of the spoofing attack types on power systems is IEC 61850 spoofing. The IEC 61850 standard is a modern power system communications standard used for automation and protection in digital substations. It enables information exchange through different communication protocols. The Generic Object-Oriented Substation Event (GOOSE) and Sampled Values (SV) protocols are employed to communicate critical substation events and measurements within a substation. However, it as it does not implement encryption, which makes it particularly vulnerable to packet sniffing and spoofing attacks [7].

By monitoring IEC 61850 traffic via the process and station buses, the attackers can create spoofed GOOSE packets that can maliciously open circuit breakers. When these packets are transmitted to a target relay, it is tricked into opening the circuit breaker, as the packet appears to originate from the station or a bay controller within the same substation. It is also possible to interfere protection functionality of relays due to spoofing of SV measurement data, causing protection equipment to not operate during critical fault conditions [18]. Such types of spoofing attacks can have disastrous consequences for power system operation and stability. A well-targeted spoofing attack can not only compromise but also disable equipment and components within a digital substation. Subsequently, this can instigate major system instabilities and may even induce cascading failures due to the sudden loss of multiple components. The potential for a system-wide collapse presents the need for comprehensive security measures. IEC 62351-6 is a standard that specifically addresses the cyber security of IEC 61850. It recommends an additional field to the GOOSE and SV data payloads for security-related information. This field contains a Rivest-Shamir-Adleman (RSA)-based digital signature to ensure payload integrity. Through this mechanism, sending and receiving Intelligent Electronic Devices (IEDs) are clearly identified, and it becomes impossible to manipulate the payload. Similarly, the standard also recommends usage of hash-based message authentication codes (HMACs) using cryptographic algorithms such as SHA-256 to ensure data integrity of GOOSE and SV frames. Such techniques can prevent spoofing and sniffing attacks. However, the suggested use of digital

signatures and security based on RSA and HMAC algorithms comes with associated costs as they are computationally demanding [8], [9].

### **2.1.3 False Data Injection**

The dominant research focus regarding cyber attacks on power systems is FDI attacks. These attacks can be performed by accessing station control systems and Remote Terminal Units (RTUs) located in substations and the SCADA master at the control centre. As a result, these attackers can inject fabricated SCADA measurements, thereby maliciously introducing correlated and consistent power flow data into the State Estimation (SE) processes to mislead system operators. A specific category of FDI attacks capable of altering estimated states while evading detection by the protective mechanisms inherent in the SE framework was demonstrated in [10]. An intriguing aspect of this type of attack is the assumption that the adversary has comprehensive knowledge of the targeted power system, which includes understanding the power network's topology and parameters. This knowledge enables the attacker to generate multiple FDIs on power flow measurements systematically. It has been shown that such FDI attacks could lead to significant economic repercussions by manipulating nodal prices in market operations or even result in physical consequences like line overloads. Beyond FDI attacks focused on state estimation, contemporary research has expanded to investigate scenarios targeting other critical applications, such as automatic generation control. Studies on the vulnerability of power systems have been conducted to analyse how FDI attacks can achieve their objectives with limited system knowledge or minimal attack resources, employing both static and dynamic (time-variant) FDI strategies. The field of detection and mitigation approaches is constantly evolving, with new strategies being proposed at the physical layer of power systems, leveraging model-based and data-driven detection techniques from control theory and ML perspectives [11], [12].

## **2.2 Network-based Attacks**

The communication network is the foundation for data transfer among connected devices in IT-OT systems. Consequently, a successful cyber attack may aim at various facets of the communication network, such as physical connections, device details, and the protocols being utilized. The two primary network-based attacks are network reconnaissance and lateral movement.

### **2.2.1 Network Reconnaissance**

Network reconnaissance involves gathering vital information about a computer network, including connected devices, network structure, protocols, applications, and services in an IT-OT environment. This process is instrumental in identifying vulnerabilities. Attackers often exploit the Internet Control Message Protocol (ICMP) to pinpoint active hosts on a network. An attacker can execute a ping ICMP scan using tools like tcpdump or Nmap, estimating the range of active IP addresses. This scan produces a list of IP addresses for hosts that respond to the ping request. Network administrators play a crucial role in defending against such attacks, for instance, by filtering and discarding ICMP packets. Another technique attackers use is a Transmission Control Protocol (TCP) scan, sending TCP SYN packets to various IP addresses. Active hosts respond with acknowledgment packets. However, this method requires considering the active ports, making it more time-consuming and resource-demanding, leading to a generally more complex process.

Through network reconnaissance, attackers can compile a list of active devices on the network. They can gain further insight into the active services from this list by scanning the open ports. For example, if port 80 is open, it suggests that a web server or HTTP service is operating on that host. An

open port 25 typically indicates the presence of a Simple Mail Transfer Protocol (SMTP) mail server. Additionally, attackers may employ host fingerprinting to determine the specific versions of applications running and identify possible vulnerabilities. In the context of cyber attacks targeting power grids, network reconnaissance is essential for locating target hosts and protocols within IT-OT systems. A notable example can be found in Ukraine in 2015, where attackers successfully identified vulnerabilities in the Microsoft Active Directory server, allowing them to gain unauthorized access to the Operational Technology (OT) systems in the control centre using stolen credentials. Similarly, during a cyber incident in Ukraine in 2016, attackers detected active protocols such as IEC 101, IEC 104, and IEC 61850, which were utilized for communication within substations.

### **2.2.2 Lateral Movement**

Lateral movement, the gradual spread throughout the targeted communication network, is a significant cyber threat. It starts with the most vulnerable host, serving as the entry point, and then advances through various hosts to reach the intended Operational Technology (OT) target. This attack often leverages user credentials to gain access to multiple hosts and navigate laterally within the IT-OT network. This technique can be observed in advanced persistent threats. Notably, lateral movement was a key tactic in the cyber attacks on the power grid in Ukraine during 2015 and 2016. In 2015, the attackers aimed to reach the SCADA system in the control centre through lateral movement to create a blackout. While network segmentation is one way to mitigate the risk of lateral movement, the attacks in Ukraine demonstrated its insufficiency. Network segmentation alone is not enough to protect against advanced persistent threats. Therefore, operators of power grids must urgently bolster network segmentation with additional security measures like next-generation firewalls and intrusion detection and prevention systems (IDPS) to effectively reduce the risk of lateral movement.

## **2.3 Phishing**

Phishing is a social engineering attack that takes advantage of human behaviour. Phishing attacks aim to acquire sensitive information or data and introduce malware into the corporate IT network, often acting as entry points for more complex cyber attacks. In phishing, attackers impersonate a credible source to convince victims to take specific actions. These actions include opening an email, clicking Uniform Resource Locator (URL) links, downloading files, and unknowingly divulging sensitive information. Emails are significant individual identifiers on the Internet and hold organizational importance as a formal means of communication. For these reasons, emails have become the primary medium for phishing attempts. Attackers can indiscriminately send phishing emails to any email address, hoping to persuade recipients to perform further actions, as noted earlier. Such actions can lead to harmful consequences, including severe data breaches, widespread malware installation, and significant financial losses, underscoring the urgency and seriousness of the issue.

Spear phishing is a specific type that focuses on an individual or organization. Before executing a spear phishing attack, an attacker collects extensive information about the target. Information gathering can occur through the Internet or social engineering methods. Using this preliminary data, the attacker tailors the content of the phishing email to be pertinent and closely aligned with the target, resulting in a higher success rate than generic phishing. As a result, spear phishing is a crucial entry point for advanced persistent threats. Strong organizational policies and corporate IT security measures are essential to defend against phishing attacks. These measures provide a sense of security and protection, as they involve verifying and scrutinizing the sources of email addresses, URL links, and file attachments in emails. Through such precautions, harmful emails can be identified and

filtered, serving as the first line of defence against phishing attacks. Nevertheless, the most vital defence strategy is enhancing user awareness. With adequate training and awareness, users can learn to identify phishing emails.

## **2.4 Denial-of-Service Attacks**

A Denial-of-Service (DoS) attack aims to hinder the legitimate access of users or network devices to vital system resources. These resources include network connections, computing power, and various application services. When several coordinated DoS attacks are launched simultaneously from multiple distributed sources, the term is distributed DoS (DDoS). This approach makes it significantly more challenging to track and identify the origin of the attacks, as simply blocking one attack source is insufficient for DDoS incidents. DoS attacks present a formidable threat to data availability in power grids. They can disrupt the flow of critical measurements and controls by jamming SCADA communication channels or compromising field devices to prevent data reporting. Attackers may also target routing protocols or inundate networks with excessive, illegitimate traffic.

DoS attacks can be classified primarily into bandwidth depletion attacks and resource depletion attacks. The first one focuses on saturating the bandwidth capacity of a target network. Attackers achieve this by flooding the communication channel with massive volumes of illegitimate traffic. They might also utilize amplification techniques, where third-party systems generate numerous legitimate requests simultaneously, again overwhelming the target's bandwidth. As a result, legitimate users experience significant disruptions in their communication, severely impairing overall network performance. The second one aims to overwhelm a targeted host's computing resources. Hackers exploit specific protocols and known response mechanisms to drain the resources. A common example involves the TCP/IP protocol, which uses a three-way handshake to establish communication between two hosts. By sending a multitude of malicious requests to the target host, attackers can create a situation where the host is overwhelmed with these requests, leaving it unable to process legitimate ones effectively.

DoS attacks pose significant risks to SCADA systems, especially those pertinent to power grid operations [13]. Extensive research has been conducted on the susceptibility of SCADA systems to these types of attacks. For instance, the adverse effects of DoS attacks on SCADA systems using the OPNET communication network simulator was presented in [13]. It showed a significant reduction in network throughput and processing capabilities. Moreover, how a DoS attack could exploit specific communication protocols used in substations, adversely affecting Remote Terminal Units (RTUs) processing and communication functions, can be found in [14]. Likewise, Carcano et al. highlighted vulnerabilities within the IEC communication protocols, showcasing how resource exhaustion attacks could expose critical cyber security weaknesses in power grid operations [15].

## 3 T5.2 Overview

### 3.1 Challenges Addressed by the Task

Task 5.2 recognized the challenge of developing separate digital twins for the transmission and distribution systems and their applications. Consequently, a unified, integrated digital twin was developed for the manageability and effectiveness of DT applications, as shown in Figure 3-1. Due to the significant computational resources and limited access required to accurately depict the complete Dutch electrical power system, dynamic model reduction techniques were applied. These methods were designed to refine the models, particularly to enhance details in key areas such as the integration points of significant variable RES.

To achieve comprehensive system models, the partners in T5.2 collaborated closely, beginning with the development of models for the transmission system. This was followed by the integration of dynamic, reduced models of the remaining system components, thereby providing a detailed and realistic representation of the physical power system. This involved the use of specialized equivalent models to effectively represent interconnections with adjacent networks, ensuring a cohesive and interconnected digital twin ecosystem. This task aimed to understand the operational dynamics of future power systems, particularly in evaluating the impact of cyberattacks and proposing methods to prevent cyberattacks. This was crucial for ensuring the resilience and reliability of power systems against evolving cyber threats.

### 3.2 Architecture of Digital Twin and Description

The architecture of the cyber-physical DT framework is shown in Figure 3-1. It enables synchronized interactions between the physical power system representation, communication network and its DT. The proposed framework establishes bidirectional data exchange through Open Platform Communications Unified Architecture (OPC UA) middleware and an emulated communication network, ensuring continuous state between the physical power grid and its virtual counterpart.

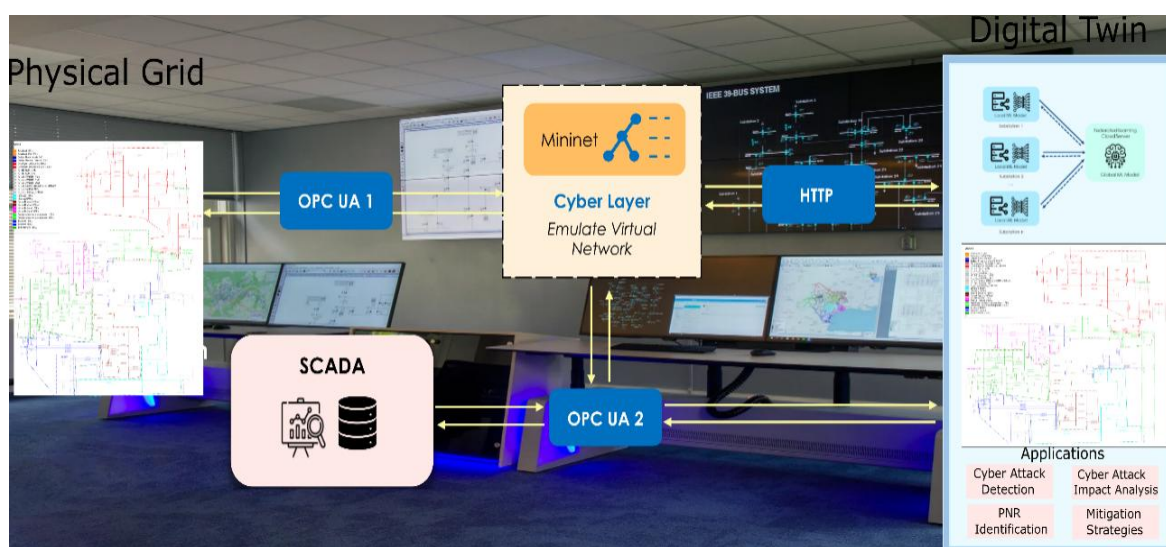


*Figure 3-1: Overall architecture of DT for cyber security assessment.*

## 3.3 Development Roadmap

### 3.3.1 Implemented Functions

The goal of the task was to develop and use a digital twin to assess cyber security of interconnected power grids. This task includes the functions as follows:

- **Conduct near Real-Time Cyber Attack Simulations on DT of Interconnected Power Grids:** Different cyberattack scenarios were designed and executed on the digital twins, aiming to understand their effects on power system stability and resilience. Mininet was utilized to simulate the network environment and to provide a realistic platform for network configurations and attack scenarios. Additionally, OPC UA was used as an interface between the physical and cyber-simulated layers for data exchange and interactions within the power grid, enhancing the realism of the simulation. OPC UA clients and servers were modelled as interacting components in the OPC UA architecture. Attack datasets were prepared to further enhance the realism of these simulations and to provide valuable data for further analysis.
- **Assess in near Real-Time the Impact on the Operation of Interconnected Power Grids:** Cyber attacks were simulated in near real-time on the DT of the interconnected power grids, resulting in the loss of generation and interconnectors, as well as the disconnection of multiple transmission lines. The impact on power system operations was evaluated by computing impact indices based on the loss of load, frequency deviations, voltage deviations, survived islands, and affected power system components.
- **Analyse how Cyber Attacks can Initiate Cascading Failures and Cause a Blackout:** Cyber attacks were recognized as capable of causing multiple contingencies, e.g., N-k. The probability of occurrence of such contingencies was considered to be almost negligible when caused by physical disturbances. However, such contingencies could be triggered simultaneously by cyber attacks. As a result, the point of no return was reached more rapidly, leading to cascading failures and blackouts. A computational method and tool were developed and demonstrated to assess the cascading failure mechanism and to analyse how cyberattacks could cause a blackout.
- **Anomaly Detection using Machine Learning:** ML methods were used to continuously monitor network traffic and operational data, enabling the rapid identification of deviations from normal patterns. By analysing deviations in communication network traffic, the system was able to promptly detect potential cyber threats and operational anomalies. This integrated approach, leveraging mininet for network simulation and an OPC UA server for protocol simulation, enhanced the ability to protect power grids from cyber attacks and ensured stable and reliable power system operations.

### 3.3.2 Software Platforms and Datasets Used for DT Development

To successfully execute the functions outlined above, a suite of advanced tools and datasets was employed throughout the project.

- **DigSILENT PowerFactory:** This software is essential for modelling the physical power system components and the digital twin. It allowed for in-depth power system analysis, providing a solid foundation for understanding how the physical infrastructure interacted with the cyber simulations.

- **Mininet:** This tool is crucial for simulating the network environment. It provides a realistic platform for creating network configurations and running various attack scenarios, thus enhancing the authenticity of our simulations.
- **Open Platform Communication Unified Architecture (OPC UA):** An OPC UA server is used to facilitate data exchange and interactions between the physical and cyber-simulated layers of the power grid. By modelling OPC UA Client and Server as interacting components, we can bolster the realism of our simulations and improve the accuracy of results.
- **Attack Datasets:** Preparing specific datasets that mimic potential cyber-attack scenarios is vital for the realism of the simulations and analysis. This dataset serves as a foundation for understanding training ML for anomaly detection.

### 3.3.3 Timeline and Milestones

| Month  |                                                                            | Jan | Feb | Mar | April | May | June | July | Aug | Sept | Oct | Nov | Dec | Jan | Feb | Mar | April | May | June | July | Aug | Sept | Oct | Nov | Dec |
|--------|----------------------------------------------------------------------------|-----|-----|-----|-------|-----|------|------|-----|------|-----|-----|-----|-----|-----|-----|-------|-----|------|------|-----|------|-----|-----|-----|
| Tasks  | Task Description                                                           | M13 | M14 | M15 | M16   | M17 | M18  | M19  | M20 | M21  | M22 | M23 | M24 | M25 | M26 | M27 | M28   | M29 | M30  | M31  | M32 | M33  | M34 | M35 | M36 |
| T5.2.1 | TwinEU Dutch system dynamic modelling                                      |     |     |     |       |     |      |      |     |      |     |     |     |     |     |     |       |     |      |      |     |      |     |     |     |
| T5.2.1 | Add protection mechanisms to Dutch transmission network                    |     |     |     |       |     |      |      |     |      |     |     |     |     |     |     |       |     |      |      |     |      |     |     |     |
| T5.2.1 | Communicate the powerfactory model with the OPC server                     |     |     |     |       |     |      |      |     |      |     |     |     |     |     |     |       |     |      |      |     |      |     |     |     |
| T5.2.2 | Cyberattack simulations and data collection                                |     |     |     |       |     |      |      |     |      |     |     |     |     |     |     |       |     |      |      |     |      |     |     |     |
| T5.2.3 | Develop and test federated learning algorithm                              |     |     |     |       |     |      |      |     |      |     |     |     |     |     |     |       |     |      |      |     |      |     |     |     |
| T5.2.4 | Quantify point of no return and develop defense against cascading failures |     |     |     |       |     |      |      |     |      |     |     |     |     |     |     |       |     |      |      |     |      |     |     |     |

*Figure 3-2: Timeline for the DT development for cyber security assessment.*

### 3.3.4 Demonstration Plan

To effectively illustrate the potential functionalities introduced in this task as shown in Figure 3-2, practical demonstrations of these capabilities were conducted within the innovative environment of the Control Room of the Future (CRoF) located at TU Delft.

- **Development of the Digital Twin:** A DT of interconnected transmission and distribution systems was developed using the tools described above. In the CRoF, the demonstration also included a communication layer and tools to simulate interactions with typical SCADA systems. This setting provided a real-world context for evaluating the effectiveness of the digital twin in simulating complex scenarios and devising proactive strategies to mitigate potential risks.
- **Executing Cyber Attack Simulations:** Controlled simulations were conducted using diverse cyber attack scenarios to evaluate their impacts on power system operations. These simulations generated an attack dataset to train the ML model for anomaly detection.
- **Analysing Results:** After each simulation, an analysis was performed to evaluate the operational impacts and cascading failures. This analysis provided insights into the implications of cyberattacks on power grids.
- **Reporting Findings:** Finally, the findings were compiled into comprehensive reports, including the cyber-attack implications on power grids for enhancing grid resilience and security.

## 3.4 Developed Framework and Results Demonstration

This chapter discusses in detail power system component modelling, interface challenges, and data flow for power system DT to assist researchers in developing analogous cyber-physical DT testbeds in the future. Figure 3-1, illustrates the overall architecture enabling synchronized interaction between the physical power system representation and its DT. The proposed framework establishes bidirectional data exchange through OPC UA middleware and an emulated communication network, ensuring continuous state alignment between the physical grid and its virtual counterpart.

### 3.4.1 Development of Integrated Digital Twin

#### 3.4.1.1 Power System Modelling

The modelling of power system components is one of the most important factors in any type of system analysis, future method development, and controller design. Digital twinning of a power system can be achieved at different levels of modelling fidelity, ranging from steady-state load flow models to full dynamic models that include detailed component dynamics, controllers, and protection schemes. A dynamic model of the Dutch 380 kV transmission network is modelled using publicly available data from TenneT and ENTSO-E. This Dutch transmission model features a high penetration of renewable energy, primarily from wind turbines, along with cross-border HVDC power exchange, the single line diagram of the Dutch 380kV transmission network shown in Figure 3-3. This setup facilitates the analysis of system behaviour under various types of disturbances. All synchronous generators, wind turbines, and HVDC links are equipped with dedicated controllers such as Automatic Voltage Regulators (AVR) for voltage regulation and improved dynamic response during disturbances, turbine-governors (GOV) for balancing mechanical input and electrical output power by regulating the turbine valves, and Power System Stabilizers (PSS) for damping electromechanical oscillations by providing a voltage feedback input signal to the AVR. Wind turbine generators are modelled using the standard WECC Type 4A model, which accurately represents both drive-train and converter dynamics to ensure system stability and to maintain grid voltage and frequency within prescribed operational limits. Various protection schemes have been incorporated into the network to replicate the behaviour of a physical power grid during system disturbances. All generating units, including synchronous machines, asynchronous machines, wind plants, and interconnectors, are equipped with voltage and frequency protection functions. These protections address both under/over-voltage (UV/OV) and under/over-frequency (UF/OF) and RoCoF events. In accordance with grid compliance requirements, wind plant protection settings are configured to support low-voltage ride-through capability. Transmission lines are protected using distance protection as the primary scheme, with overload protection serving as backup protection. In addition, under voltage (UVLS) and under frequency (UFLS) load shedding protection is implemented to maintain system stability as tabulated in Table 1.

Furthermore, the distribution network consists of six sites containing asynchronous generators and three synchronous generators. It is configured as a ring-main distribution system and incorporates transformers with voltage levels up to 11 kV to improve overall power system reliability, as depicted in Figure 3-6. The network represents a synthetic model of the Zeeland region and is integrated with the associated transmission system. For analytical convenience and to reduce the complexity of grid operation studies, the integrated transmission and distribution network has been partitioned into four regions, as illustrated in Figure 3-5. The geographical representation of the transmission and distribution system is shown in Figure 3-4.

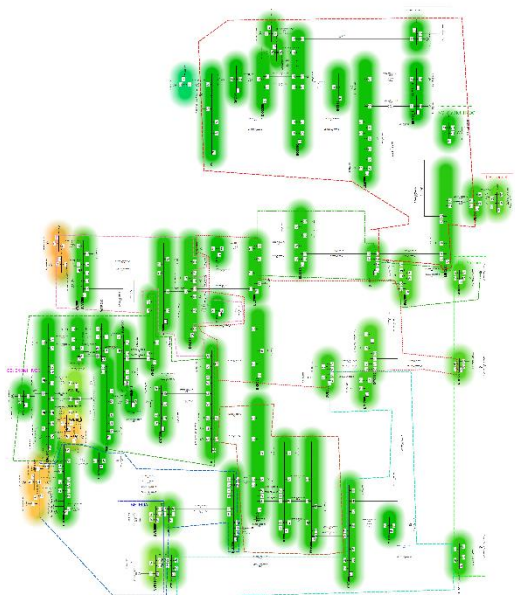


**Figure 3-3: SLD of 380kV Dutch transmission network.**



**Figure 3-4: Geography of synthetic Dutch transmission and distribution network.**

**Table 1: Overview of the dynamic model and coordinated protection schemes for the integrated Dutch transmission and distribution network.**

| Component                            | Models/Controllers                              | Protection                                                             |
|--------------------------------------|-------------------------------------------------|------------------------------------------------------------------------|
| Synchronous /Asynchronous Generators | AVR, GOV, PSS                                   | UF/OF, UV/OV, RoCoF, OOS                                               |
| Interconnectors                      | 1. Generator + Load<br>2. HVDC control terminal | 1. UF/OF, UV/OV, RoCoF<br>2. UF/OF, UV/OV, RoCoF, Voltage Ride through |
| Wind plants                          | WECC Type 4A model                              | UF/OF, UV/OV, RoCoF, Voltage Ride through                              |
| Loads                                | General load model                              | UFLS, UVLS                                                             |
| Lines                                | -                                               | Distance, Over loading                                                 |

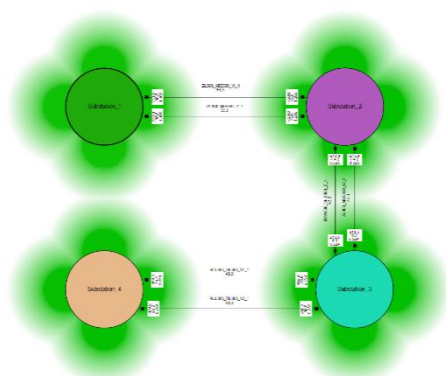


**Figure 3-5: Integration of Dutch transmission and distribution network.**

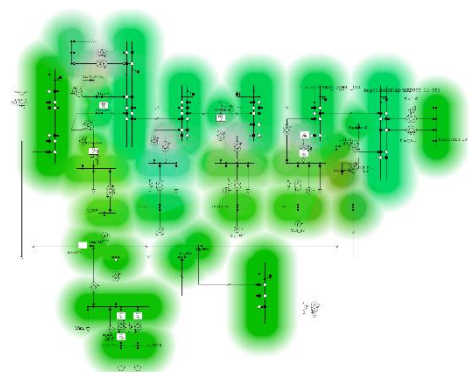


**Figure 3-6: SLD of Dutch distribution network.**

Overall, the developed dynamic model of the Dutch transmission and distribution network effectively captures the transient behavior of the system and facilitates the assessment of the system's response under various disturbance scenarios, including physical and cyber induced events such as load or generation loss and line tripping.

### 3.4.1.2 External Measurements

For DT RMS simulations, information must be exchanged between the physical grid and the twin network. This exchange is achieved by incorporating external measurement blocks for each component, including lines, buses, loads, generators, and transformer tap changers. In this testbed, measurements and control commands are continuously exchanged between the physical system and the twin network. At the substation level, measurements such as bus voltage magnitude, voltage angle, active power, reactive power, and circuit breaker status are monitored. For generators, voltage magnitude, voltage angle, current, loading, active power, and reactive power are measured, while voltage setpoints from the AVR and power setpoints from the governor are communicated for control purposes. Transformer tap-changer control commands are also modelled. Similarly, measurements and control signals for other network components are incorporated. All measurement signals and control commands are interfaced through OPC UA to enable near real-time information exchange during Root Mean Square (RMS) simulations. Two types of external measurement interfaces are used for circuit breaker status, setpoint control, tap-changer operations, and other control commands. One interface provides inputs to power factory from the OPC UA server, DT platform, or physical grid, while the other updates the current measurement status within the simulation environment. Each external measurement is assigned a unique foreign key identifier in the format  $\%S.\%B.\%E.\%N.\%C$ . In this structure,  $S.B$  denotes the substation number and bus name within the network,  $E$  represents the element name,  $N$  specifies the measurement name, and  $C$  indicates whether the signal corresponds to a control command or a measurement.

### 3.4.1.3 Cyber Layer Modelling

**Cyber Layer Modelling** The cyber layer acts as the interface for data acquisition, communication, storage, and supervisory control within the proposed framework. It integrates OPC UA servers, an emulated communication network implemented in Mininet, a database, and a Human-Machine

Interface (HMI), acting as SCADA, to enable synchronized interaction between the physical power system model and its digital counterpart.

- 1) **Open Platform Communications Unified Architecture (OPCUA):** OPC UA serves as the middleware that enables standardized and platform-independent communication between the power system model (Power Factory) and the DT. In the proposed framework, two independent OPC UA servers are deployed:
  - **OPC UA server 1 (Physical system interface):** It establishes a connection with the power factory physical power system model. It is configured to extract real-time power system measurements, including bus voltages, line currents, active and reactive power flows, circuit breaker status, and frequency values. The server is implemented using the OPC UA Python SDK and dynamically generates nodes corresponding to physical components (buses, transformers, circuit breakers, and transmission lines) based on the physical system model. Measurements are then extracted at 500 ms intervals to ensure near-real-time synchronization between the power system simulation and the cyber layer. These values are then made available to the communication network layer via subscribed OPC UA clients (hosts) inside the Mininet.
  - **OPC UA server 2 (DT interface):** This acts as the interface between the communication network (Mininet) and the DT. It receives manipulated or delayed data from the cyber layer and updates the DT model accordingly. Similar to OPC UA server 1, it updates OPC UA server node values every 500 ms. The OPC UA layer, therefore, acts as a bidirectional bridge that collects measurements from the physical model, transfers commands or modified data to the DT, and also interfaces with Mininet hosts and SCADA systems.
- 2) **Database:** A MongoDB database is integrated within the proposed framework to function as the SCADA system. It is an open-source, NoSQL document-oriented database designed for scalability, flexibility, and modern distributed applications. It stores power system measurements, including voltage magnitudes, current values, breaker states, power flows, and timestamped event logs. Within the proposed architecture, MongoDB is deployed as the backend database of the SCADA and is logically connected to OPC UA server 2, which interfaces with the DT environment. The modular database design allows future extension toward cloud-based synchronization, distributed DT coordination, or federated analytics platforms, although these extensions are beyond the scope of the present study. To provide real-time visualization and validation of OPC UA data exchange, the UA Expert client tool is incorporated into the framework as a lightweight HMI. UA Expert connects to both OPC UA servers and enables real-time monitoring of measurement nodes (e.g., voltage, current, breaker status) and visualization of data updates. Although UA Expert is not used for active control within the experiment, it serves as a supervisory monitoring interface.
- 3) **Communication Network (Mininet):** The communication layer is implemented using Mininet to emulate realistic communication network behaviour and enable controlled attack execution. Mininet provides software-defined network emulation that can replicate realistic communication latency and packet-level interactions. The communication network topology in Mininet is automatically generated from a configuration file derived from the physical model topology. Based on this topology, corresponding Mininet hosts are instantiated to represent substation IED hosts, gateway hosts, control operator hosts, and a dedicated host

acting as an attacker. Each host is connected via virtual switches and routers that reflect inter-substation and control centre connectivity and mirror the hierarchical structure of the actual power system communication architecture. This automated mapping ensures consistency between the physical grid topology and the cyber network topology. A dedicated attack host within Mininet simulates realistic cyber threats by modifying measurement values of targeted hosts, for example, false circuit breaker status (open/closed), modified voltage, or power flow values. The manipulated data is then forwarded through the OPC UA server 2 to the DT model. As a result, the DT updates breaker states incorrectly, power flow is recalculated, and line overloads or voltage instability may occur, which can trigger cascading failure sequences.

### **3.4.2 Executed Cyber Attack Scenarios within DT Testbed**

#### **3.4.2.1 Data Manipulation Attack**

This paper focuses on data manipulation attacks targeting power system measurements within the emulated communication network. We assume that the attacker has already gained access to the network (e.g., via compromised credentials, lateral movement, or exploitation of a vulnerable host). It has performed prior reconnaissance to identify vulnerable assets, including IP addresses, communication ports, and services of target devices such as Mus. Thus, this work does not focus on intrusion techniques but instead evaluates the impact and propagation of maliciously modified measurement data within the proposed framework. A dedicated attacker host is included inside the emulated environment that interacts with the system through an xterm terminal. It provides a real-time command-line interface connected to selected virtual hosts. It can enable controlled and repeatable execution of attack scenarios. From the interface, the attacker targets specific substations and MU instances based on previously acquired network knowledge (e.g., IP address of the targeted host). Fig 4 shows the attacker's interaction via the emulated xterm interface. The attacker selects a target MU (e.g., S10m9), establishes a connection using known IP/port information, and performs data manipulation by modifying a specific node value (e.g., Node 616  $\rightarrow$  1), thereby demonstrating a switching attack on measurement data within the system. In this case, the attacker emulates switching attacks by altering breaker status values (e.g., forcing a state change from open to closed or vice versa).

#### **3.4.2.2 Switching Attack**

In this scenario, a time-coordinated cyber attack is implemented, which replicates the Ukrainian substation cyber attack by disconnecting transmission lines connected to a targeted substation. Based on the latest available measurements from the physical grid network, the cyber attack use case is initiated at 15 s. The attack begins by disconnecting the circuit breakers of lines connected to the substation within 0.5 s and is fully executed by 18 s. This results in an N-k contingency condition, leading to severe instability across the entire grid. Consequently, power is redistributed to parallel transmission lines, causing overloading and triggering protection mechanisms; this is considered a slow-cascading stage. This leads to cascading tripping of transmission lines in neighbouring zones. The initial cyber attack event, combined with the cascading failures, results in unintentional and uncontrolled islanding of the grid, dividing it into two islands, referred to as Area 1 and Area 2.

#### **3.4.2.3 Network Scanning Attack**

To emulate network reconnaissance activities, TCP SYN-based scanning attacks were generated using the Nmap network scanning tool. Nmap is a widely used network discovery and security auditing tool capable of identifying active hosts, open ports, and running services within communication

networks. In this work, it was used to emulate stealth and aggressive network scanning activities targeting multiple substations in the OT communication layer. We perform a TCP SYN stealth scan, which scans all available ports and increases the scan aggressiveness and transmission rate. The generated reconnaissance traffic was captured by the DT integrated monitoring framework using the Wireshark tool and incorporated into the OT traffic dataset. The resulting traffic patterns were subsequently used to train the Federated Learning (FL)-based intrusion detection models deployed at distributed substation DT clients.

#### 3.4.2.4 DoS Attack

Multiple SYN-based DoS attack scenarios were also generated within the mininet-based communication network using the hping3 packet generation tool. Hping3 is a network packet crafting and traffic generation tool that allows customized TCP/IP packet generation for security testing and attack emulation. We emulated stealth SYN probing, high-rate SYN transmission, and SYN flood attacks targeting substations in the OT communication network.

#### 3.4.3 Anomaly Detection Using Federated Learning

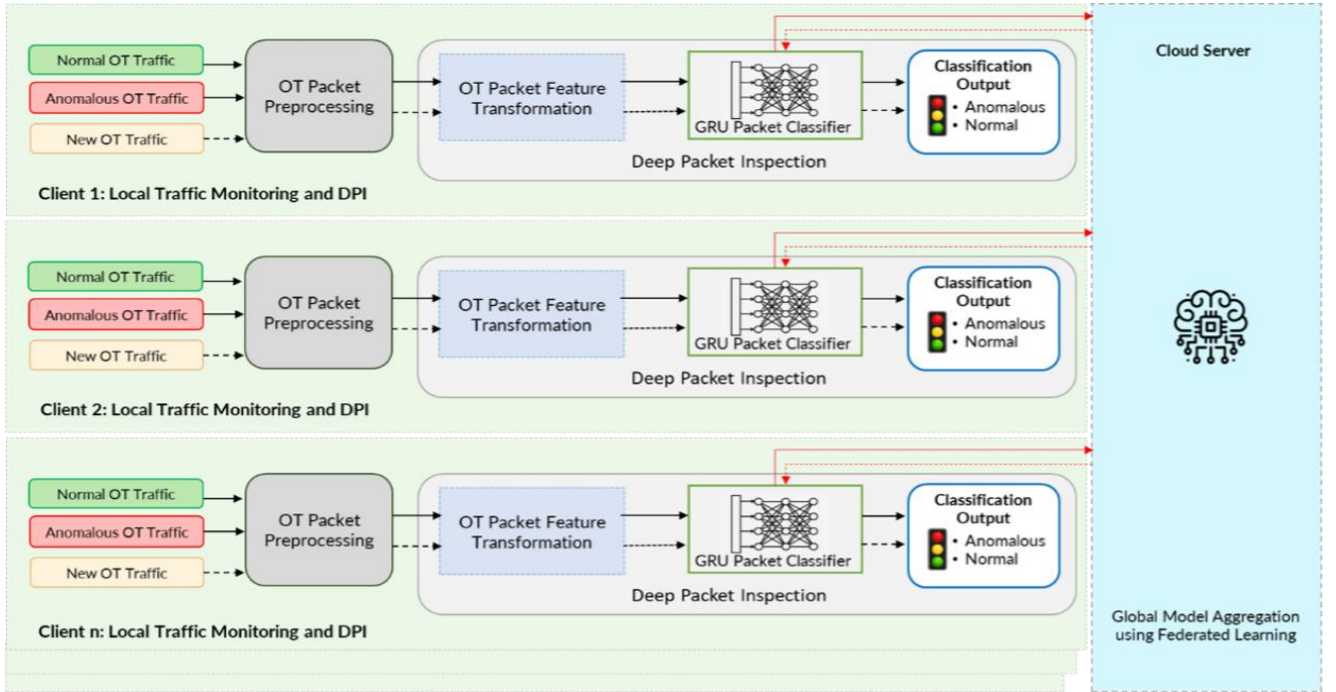


**Figure 3-7: Digital twin module for attack detection using federated deep packet inspection**

The DT attack detection module captures OT protocol-level traffic (e.g., TCP/IP, IEC 61850, IEC 104, DNP3, and Modbus) under both normal and anomalous operating conditions. The cyber physical power system co-simulation generates packet-level Operational Technology (OT) network traffic, producing high-dimensional datasets that represent both benign and cyber attack scenarios. The generated data from our testbed, together with OT protocol data from public datasets, is pre-processed into structured numerical representations. Figure 3-7 illustrates the architecture of the federated DPI within the DT attack detection module. Principal Component Analysis (PCA) is applied to reduce the dimensionality and transformation of packet features while preserving dominant traffic characteristics. Given a dataset  $X \in \mathbb{R}^{(N \times d)}$ , the covariance matrix is computed as in (1).

$$C = \frac{1}{N-1} (X - \bar{X})^T (X - \bar{X}), \quad (1)$$

where  $\bar{X}$  denotes the mean feature vector. The top- $m$  principal components are selected based on variance retention, producing a reduced feature matrix  $Z = XU_m$ .

Each substation is emulated as a distributed client within the DT environment, enabling local traffic monitoring and attack detection. Each client trains a local deep learning-based DPI model using a Gated Recurrent Unit (GRU) classifier to capture inter-feature dependencies in packet payloads. The local training objective minimizes the cross-entropy loss as in (2):

$$L_k = -\frac{1}{N_k} \sum_{i=1}^{N_k} \sum_{c=1}^C y_{i,c} \log(\hat{y}_{i,cl}) \quad (2)$$

where  $\hat{y}_{i,c}$  represents the predicted class probability. Model updates are shared with a central aggregator and combined using federated averaging as in (3):

$$w^{(t+1)} = \sum_{k=1}^K \frac{n_k}{n} w_k^t, \quad (3)$$

where  $n_k$  is the local dataset size and  $n = \sum_{k=1}^K n_k$ . DT provides simulation and evaluation of cyber attack scenarios, including DoS, network scanning, malware injection, and exploitation attacks, by replicating the communication behavior of distributed substations and control centres. These attacks can introduce subtle deviations in the semantics of packet payloads.

To address data privacy and regulatory constraints, the DT attack detection module adopts a cross-silo FL paradigm. In this setup, substation clients locally train intrusion detection models using their own traffic data and share only model parameters with a central aggregation server. The global model is iteratively updated using the Federated Averaging (FedAvg) algorithm, enabling the learning of system-wide cyber intrusion patterns without centralizing sensitive OT data. The trained global model is then redistributed to substation clients for real-time inference, allowing continuous detection of anomalous traffic across the network. In this way, the DT attack detection module provides a cyber security validation and learning environment that supports data generation, distributed model training, and intrusion detection. This architecture enhances scalability and ensures privacy-preserving intrusion detection in large-scale OT networks of power systems.

The experiment uses different attack datasets Malware, exploit scenarios, DoS attacks, and network scanning are types of attacks included. To represent protocol diversity, the dataset includes other OT protocols such as IEC 61850, IEC 104, DNP3, and Modbus. For intrusion detection, every packet that is collected is converted into a numerical feature vector encoding header and payload properties. Two scenarios are simulated to assess the consequences of various local data distributions (how data varies between clients):

- Independent and Identically Distributed (IID): The dataset is randomly and uniformly divided, guaranteeing that every client receives a fair distribution of all attack and traffic types.
- Non-IID (Non-Independent and Identically Distributed): This type of dataset is divided using quantity and label skew to simulate actual substation situations. In addition to regular traffic, each substation receives samples of two distinct attack types, which leads to an unequal distribution of classes and data sizes. This setup mimics real OT networks, where substations are vulnerable to attacks and encounter localized traffic as a result of different protocols.

Each client uses PCA to reduce dimensionality before training, keeping 95% of the variation. This procedure stabilizes local learning on high-dimensional data, removes redundancy, and lowers communication overhead during aggregation. As depicted in Figure 3-8, the effectiveness of federated DPI was assessed in two data distribution scenarios: IID and non-IID. The centralized method outperforms the centralized DPI in terms of accuracy (97.61%), precision (99.46%), recall (93.72%),

and F1 score (96.2%), due to access to the complete dataset. Each client in the IID scenario received a representative and well-balanced combination of attack and normal packets. After 10 communication rounds, it still attains nearly the same accuracy of 97.55% (with less training time), precision of 96.11%, recall of 91.88%, and an F1-score of 93.14%. These results show that the global model effectively learns discriminative features of OT traffic by utilizing the GRU's ability to capture inter-feature correlations when client data distributions are uniform. The non-IID setup, on the other hand, restricted each substation to a specific subset of attack types. With an accuracy of 95.58%, a precision of 52.07%, a recall of 58.69%, and an F1-score of 54.62%, it led to a decrease in performance. Non-IID distributions cause this performance degradation, as they cause client drift. The results obtained using the default FedAvg approach indicate that standard aggregation algorithm is not sufficient to achieve reliable attack detection under heterogeneous, non-IID conditions. In particular, when attack behaviours are unevenly distributed across substations, the global model may be biased toward locally dominant patterns and may therefore struggle to generalize to attack behaviours that are underrepresented or absent at some substations. These findings highlight the need for aggregation strategies to address this non-IID challenge. Future work will be to improve the global model's ability to learn from unevenly distributed attack behaviours while maintaining reliable detection performance across participating substations and to incorporate privacy-preserving mechanisms to secure the shared training weight updates.

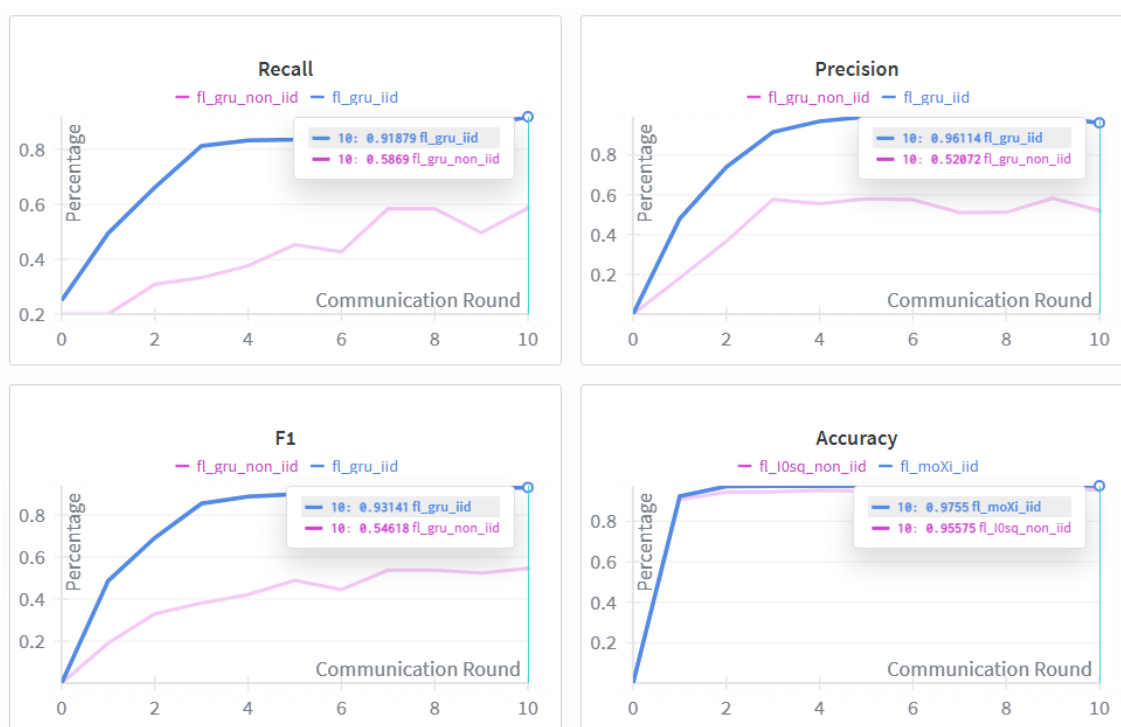


*Figure 3-8: Performance of federated DPI under IID and non-IID setting*

### 3.4.4 Impact and Cascading Failure Analysis on the Operation of Interconnected Power Grids

The developed digital twin of the integrated Dutch transmission network can be used to analyse the detailed dynamic response of the power grid in near real time. Based on the current grid state, the digital twin operator can evaluate multiple use-case scenarios, such as voltage stability, frequency stability, and load shedding, and determine the necessary control actions in response to natural events. Furthermore, the system can use real-time grid data to predict potential cyber attack scenarios

and analyse their impact on the network, including the grid's dynamic response prior to an attack on the actual system.

The developed cyber-physical digital twin framework is employed to investigate various cyber attack scenarios, namely switching attacks and spoofing attacks, across different network locations. The switching attack scenarios are further divided into two categories: (i) the simultaneous abrupt tripping of circuit breakers associated with multiple transmission lines and (ii) the sequential tripping of multiple circuit breakers in a random order. Subsequently, a comprehensive impact assessment is performed to evaluate the propagation dynamics of cascading failures and to quantify the critical threshold, referred to as the point of no return. The outcomes of the dynamic cascading failure analysis and impact assessment serve as the basis for developing advanced methodologies aimed at improving power system resilience against cyber-induced disturbances.

#### 3.4.4.1 Switching Attack

The DT operator can simulate different cyber attack use cases, with a specific focus on vulnerable areas identified by the cyber security team during the early stages of attack detection. Using this information, the DT operator can forecast potential cyber attack events and evaluate their impact on the grid. In this study, multiple circuit breakers were opened for the bus DIM380 to replicate a scenario similar to the Ukrainian cyber attack, and the resulting system dynamics and cascading failures were analysed. The cyber attack was initiated at 15 seconds, leading to the disconnection of multiple transmission lines in the network. This initial disturbance caused overloading in several remaining lines, which were subsequently tripped by secondary line overload protection mechanisms. The cascading tripping of lines resulted in uncontrolled islanding, further leading to system-wide instability.

*Table 2: Cascading events caused by switching cyber attack.*

| S.No | Time (sec) | Event description                                                                                                                                         |
|------|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | 15         | Multiple transmission lines connected to Bus DIM380 were disconnected due to a cyber attack.                                                              |
| 2.   | 15.5       | The gas generator at bus DIM15 was disconnected by the RoCoF protection scheme.                                                                           |
| 3.   | 18.5       | Multiple transformer tap-changing operations were performed to stabilize the system voltage.                                                              |
| 4.   | 23         | The MBT380–DOD380 kV transmission line was disconnected by overload protection, resulting in the formation of uncontrolled islands.                       |
| 5.   | 33         | The system reached the PNR due to severe voltage and frequency instability.                                                                               |
| 6.   | 33-34      | Multiple under-frequency load-shedding actions were executed at various substations including IC_150kV-007, IC_150kV-005, and IC_150kV-004, among others. |
| 7.   | 36         | Several wind turbines were disconnected by over-frequency and under-frequency protection schemes, leading island blackout.                                |

|    |      |                                                                                                                                                                         |
|----|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8. | 36.5 | Automatic transformer tap-changing operations were performed to regulate the voltage profile.                                                                           |
| 9. | 40   | Islanding Area 2 reached a stable operating condition, resulting in a total generation loss of approximately 1 GW out of the original 25 GW system capacity (40% loss). |

Following this cascading sequence, multiple lines and generators were disconnected by various protection schemes, as illustrated in Figure 3-9. It can be observed that *Gen\_Gas\_DIM15* was disconnected due to ROCOF protection, while a wind turbine was disconnected by an over-frequency protection relay. The corresponding power output variations are also shown in Figure 3-9. The sequence events are tabulated in Table 2. The cascading failure dynamics generation tripping, bus voltages, voltage angles, frequencies and total load is show in Figure 3-9, Figure 3-10 and Figure 3-11.

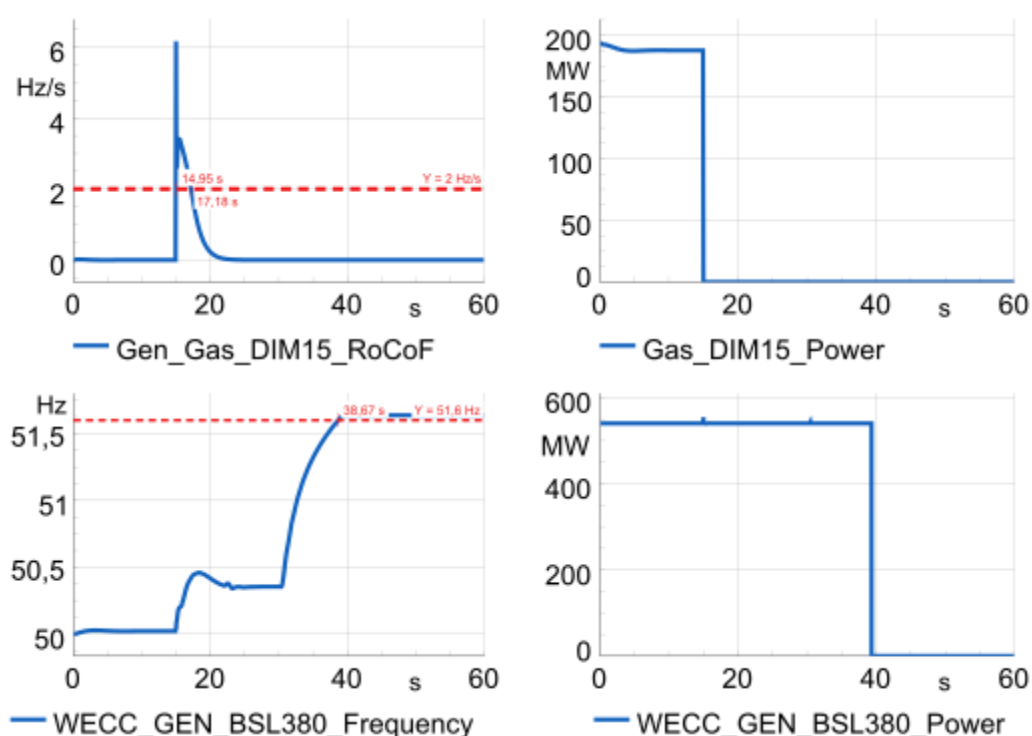


*Figure 3-9: Cascading failure caused by the initial cyber attack events.*

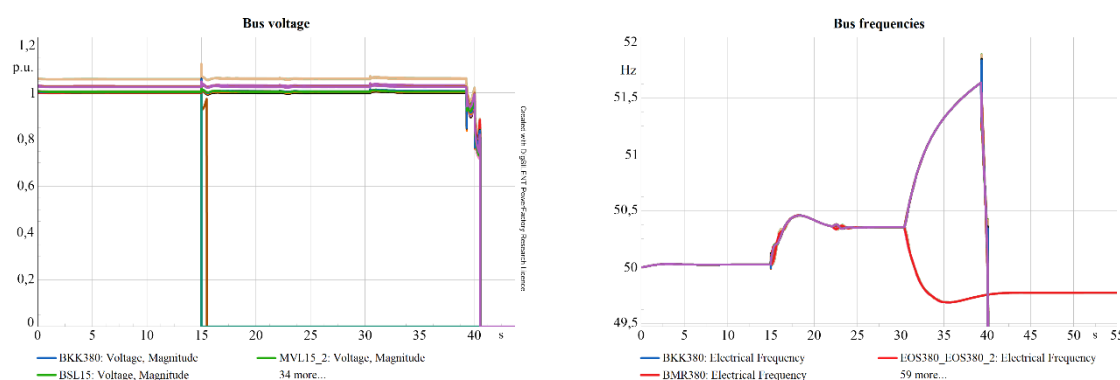


*Figure 3-10: Bus voltages and frequency.*

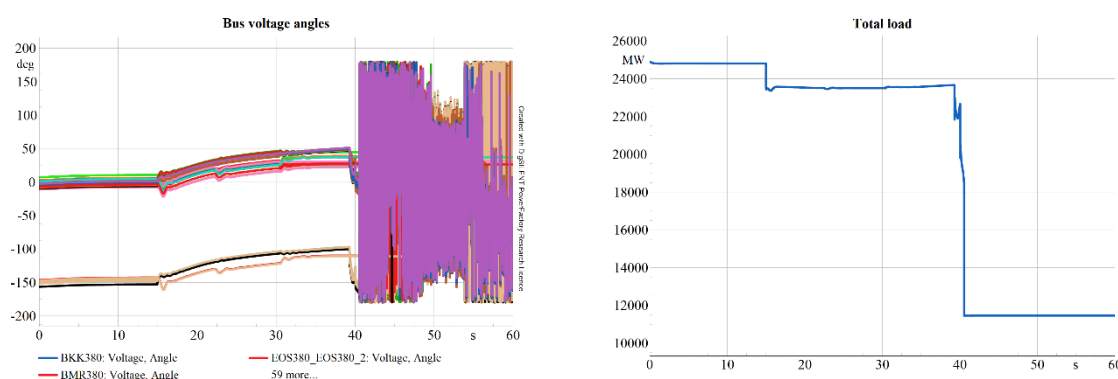


**Figure 3-11: Bus voltage angles and total load.**

### 3.4.4.2 Load Cyber Attack

Specifically, a high-load circuit breaker (1.4 GW) is disconnected from the grid. Compared to the previous scenario, this targeted attack is more severe and is executed at a faster rate. The initial disconnection leads to subsequent outages of neighbouring and inter-zonal transmission lines due to overloading, triggered by protection schemes, resulting in a slow cascading failure. This sequence of events further causes unintentional islanding, forming two separate areas, namely Area 1 and Area 2. In this scenario, Area 1 operates at an elevated frequency that gradually increases, while Area 2 operates at a frequency slightly below 50 Hz.

After a few seconds, wind turbines and other generators in Area 1 begin to disconnect due to frequency and RoCoF protection mechanisms, as shown in Figure 3-12 and overload line tripping and under frequency load shedding is illustrated in Figure 3-13, leading to fast cascading events and the PNR. Ultimately, this results in a load loss of 54.2%, as illustrated in Figure 3-11- Figure 3-15 , occurring approximately 55 seconds after the cyber attack event. The sequence of events is summarized in Table 3.

Furthermore, the digital twin testbed not only facilitates the analysis of cascading failures and the impact of physical or natural disturbances but also enables the identification of root causes associated with both slow and fast cascading failures, identifying and quantifying the PNR. This, in turn, supports the development of reactive and preventive control strategies based on real-time grid conditions.

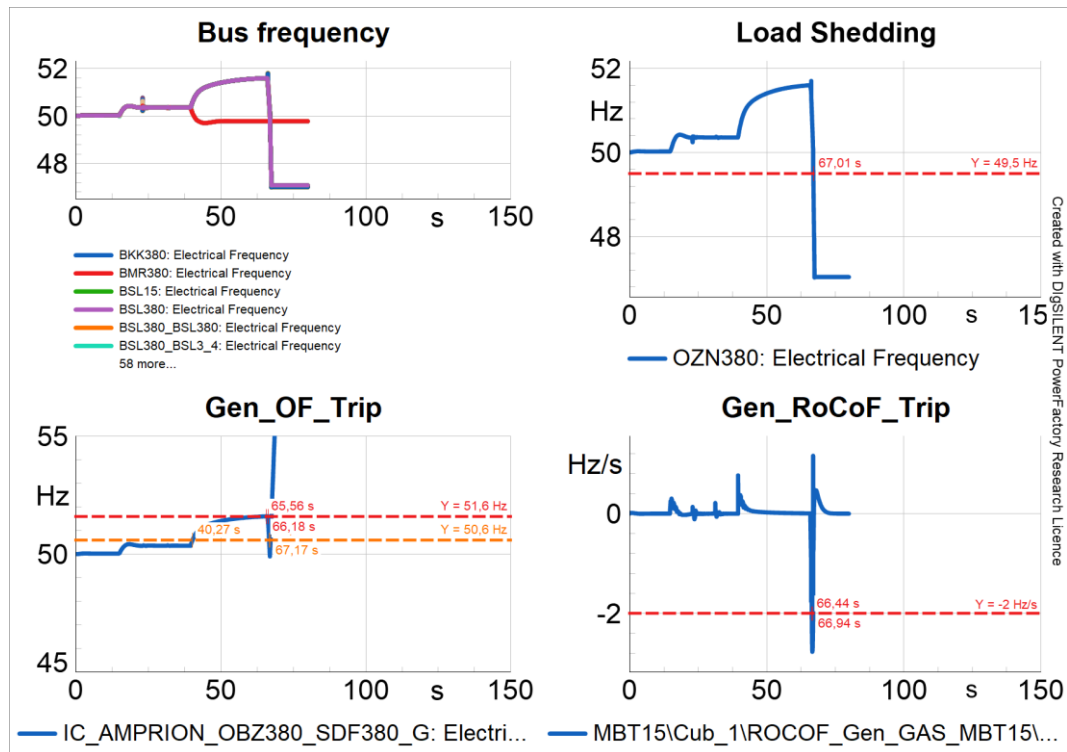


Figure 3-12: Impact of a cyber attack on Dutch transmission network.

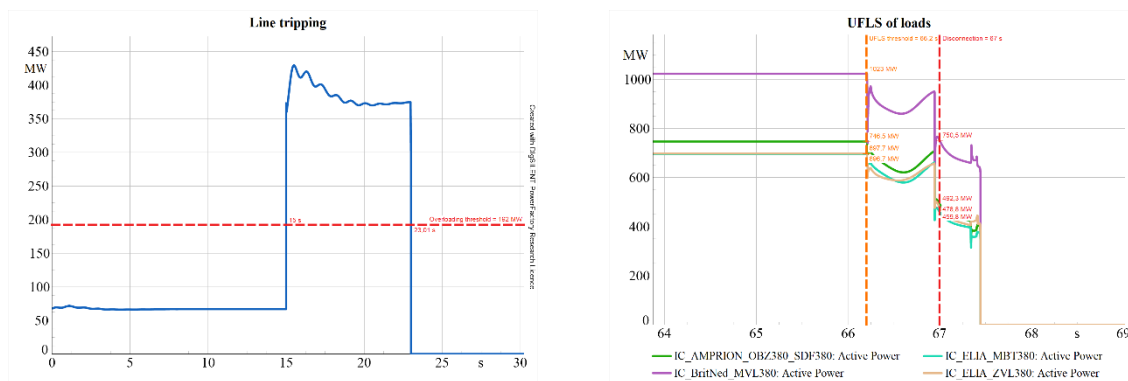


Figure 3-13: UFLS of loads and line over load tripping

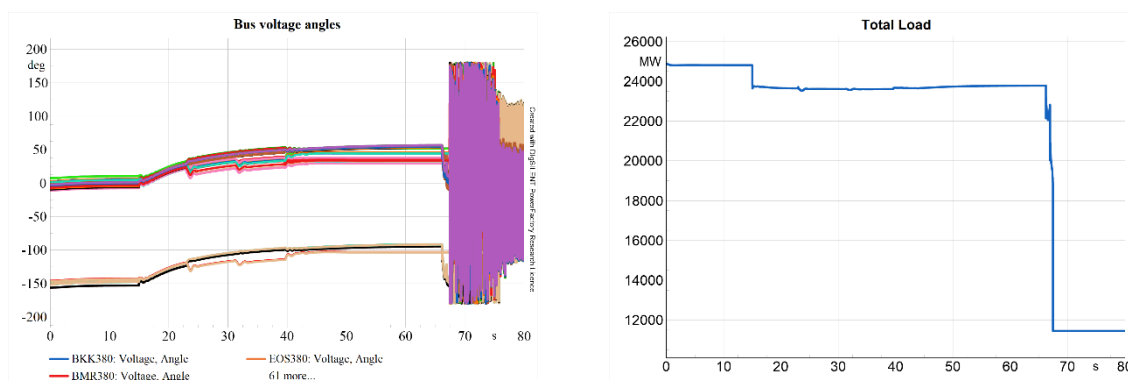


Figure 3-14: Bus voltage angles and total active load.

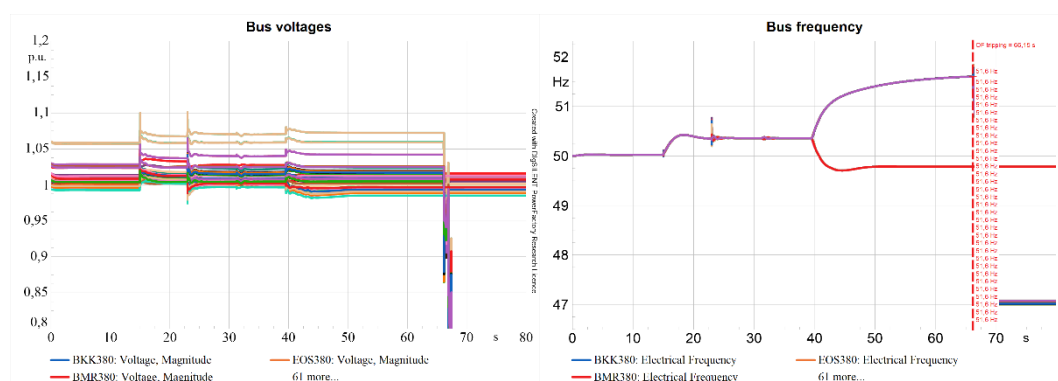


**Figure 3-15: Bus voltages and bus frequencies.**

**Table 3: Cascading events caused by cyber attack load event.**

| Time (S) | Event and Remark                                                                                                                    |
|----------|-------------------------------------------------------------------------------------------------------------------------------------|
| 15       | Cyber attack load event, disconnection of 1.4GW of load                                                                             |
| 23       | Two neighbouring parallel lines are disconnected by the overload protection                                                         |
| 31-39    | Two more parallel lines are disconnected because of stress on the network by the overloading protection. Formation of two islanding |
| 66.15    | OF tripping of wind turbines in islanding area 1                                                                                    |
| 66.88    | Slack generators and other synchronous generators disconnected by RoCoF protection in islanding area 1                              |
| 67       | UFLS activated and performed load shedding in the islanding area 1 and 2                                                            |
| 68       | System stabilizes with the load loss of 54.2%                                                                                       |

### 3.4.4.3 Spoofing attack

In this attack scenario, the attacker gains unauthorized remote access to the digital substation and automation systems by exploiting system vulnerabilities. With this access, the attacker can maliciously alter the set points of various controllers, such as HVDC terminal set points, generator AVR set points, or load-frequency controller set points, to create instability in the network. In this use case, the active power set point of EOS380\_HVDC\_Cobra is changed to 0.5, and the AVR set point of the NDR380 generator is changed to 0.9. In this type of attack, no network elements are disconnected at the instant the cyber attack is executed. From the sequence of events, it can be observed that no significant actions occur during the first few seconds. However, the changes in these set points cause several transmission lines to become overloaded and subsequently trip. Following these initial line disconnections, the targeted generator is disconnected by the undervoltage protection scheme. This tripping is followed by automatic under-frequency load shedding throughout the network. These events create further instability, causing the system to reach the Point of No Return (PNR). Beyond this point, continuous disconnections of network elements occur, representing a rapidly propagating cascade that results in a complete system-wide blackout, with generation dropping from 25 GW to 0

GW. The sequence of events is summarized in Table 4, while the element tripping sequence, voltage profiles, frequency profiles, and protection operations are illustrated in Figure 3-16-Figure 3-22.

**Table 4: Cascading events caused by spoofing cyber attack event.**

| Time (s) | Event and remark                                                                                                  |
|----------|-------------------------------------------------------------------------------------------------------------------|
| 15       | The set point of Cobra_EOS380_G is changed to 0.5, and the AVR set point of NDR380_G is changed to 0.9.           |
| 25       | Multiple transmission lines are disconnected by the overload protection at the DOD380 substation.                 |
| 32.4     | NDR380_G is disconnected by the undervoltage protection scheme.                                                   |
| 33       | Under-frequency load shedding is activated, shedding 7% of the load across the entire system.                     |
| 41       | EOS380_G is tripped by the under-frequency protection relay.                                                      |
| 42       | The system reaches the PNR.                                                                                       |
| 43-44    | Multiple wind plants are disconnected by frequency and voltage protection, and the system is under severe stress. |
| 45       | Multiple synchronous plants are disconnected by ROCOF protection.                                                 |
| 45.2     | Multiple transmission lines are disconnected by overload and distance protection.                                 |
| 90       | Interconnectors are disconnected by over-frequency protection.                                                    |
| 92       | The entire grid experiences a severe blackout, with a 100% load loss.                                             |

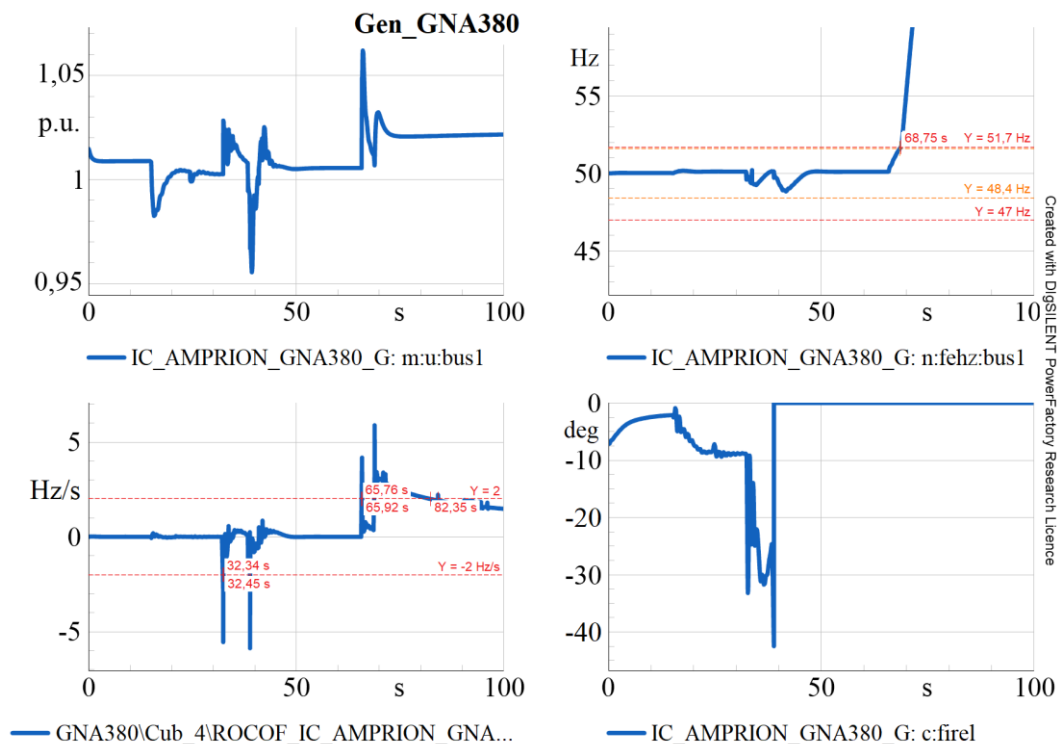


**Figure 3-16: Generator GNA380 tripping**

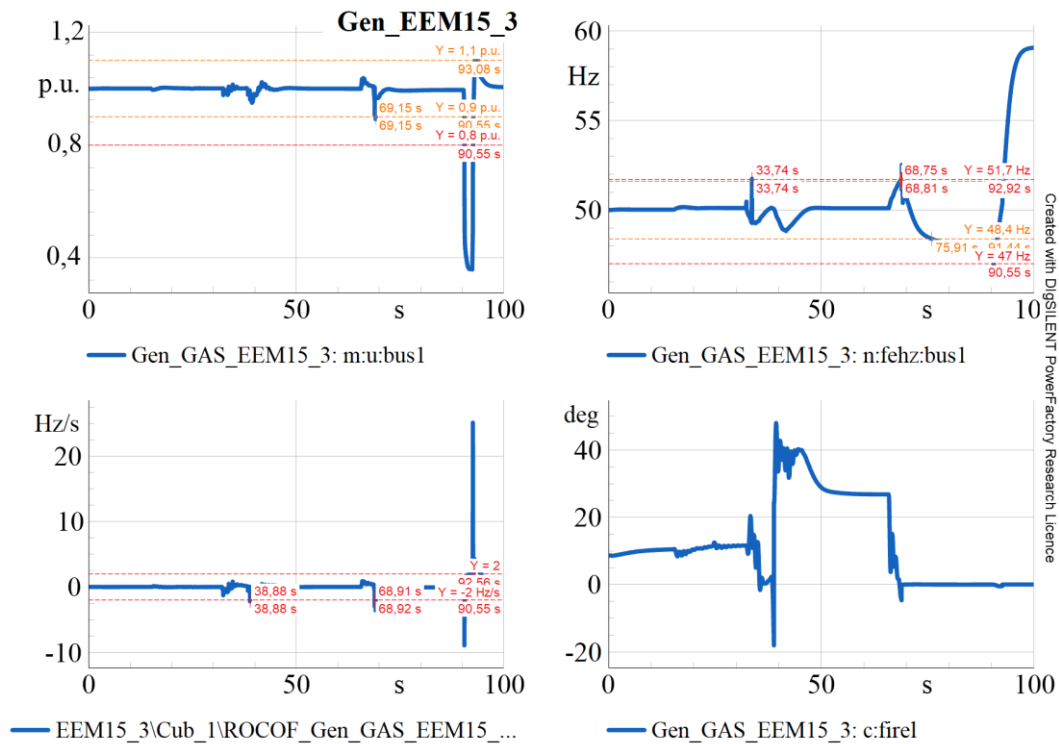


Figure 3-17: Generator EEM15\_3 tripping.

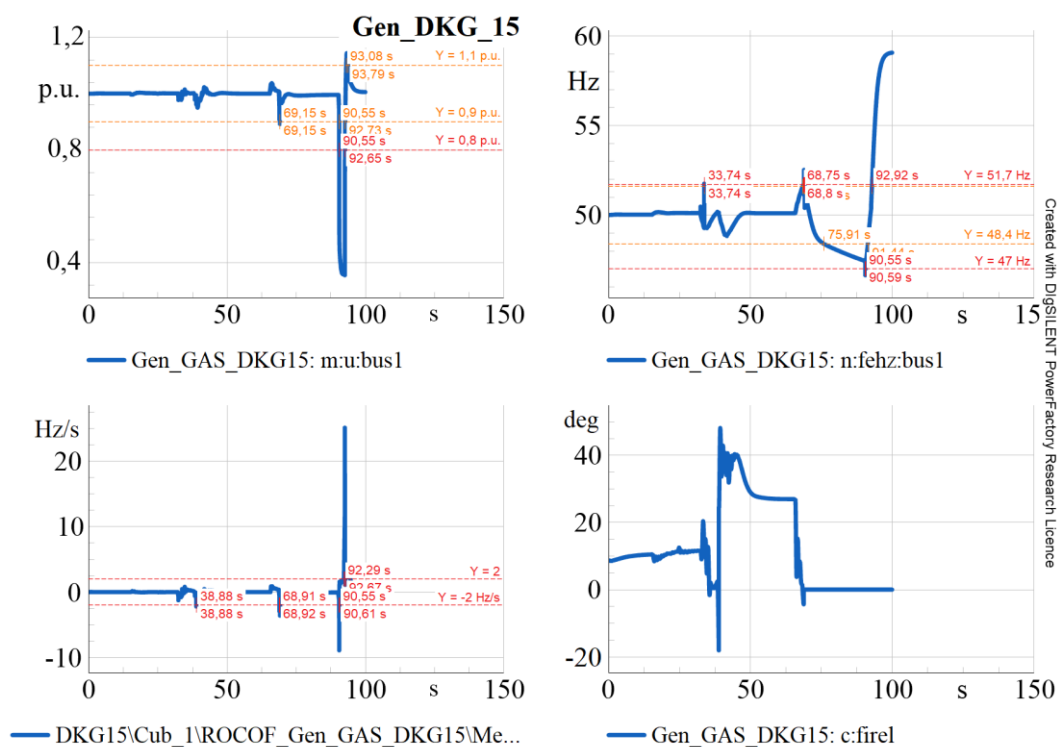


Figure 3-18: Generator DKG\_15 tripping.

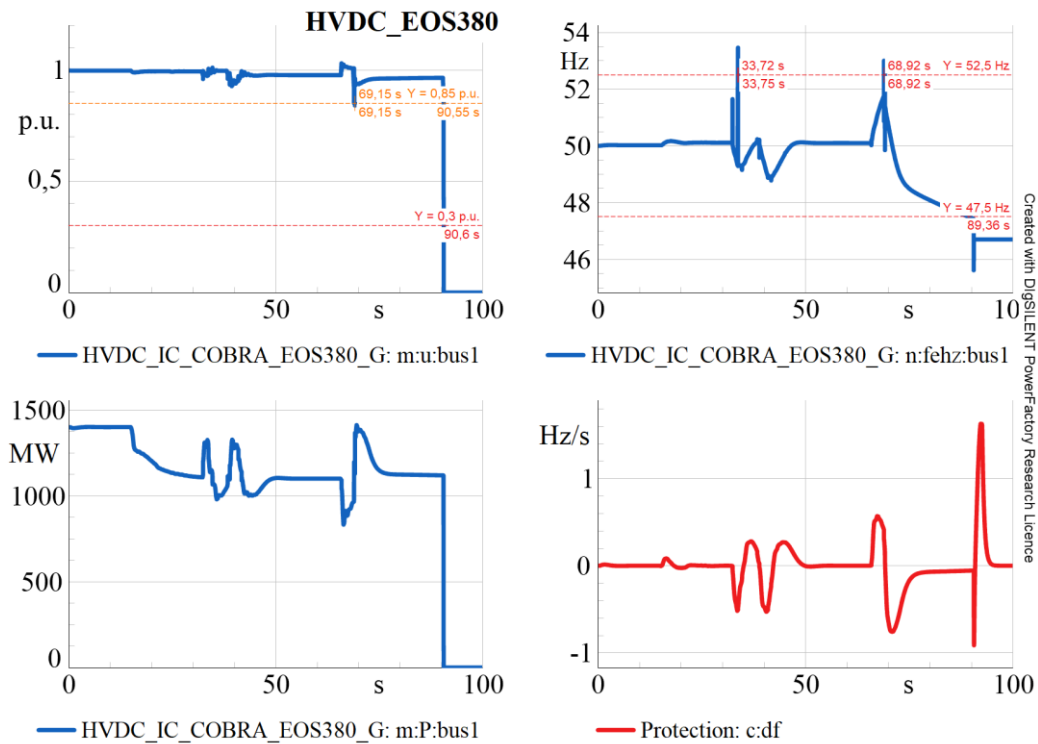


Figure 3-19: HVDC interconnector tripping.

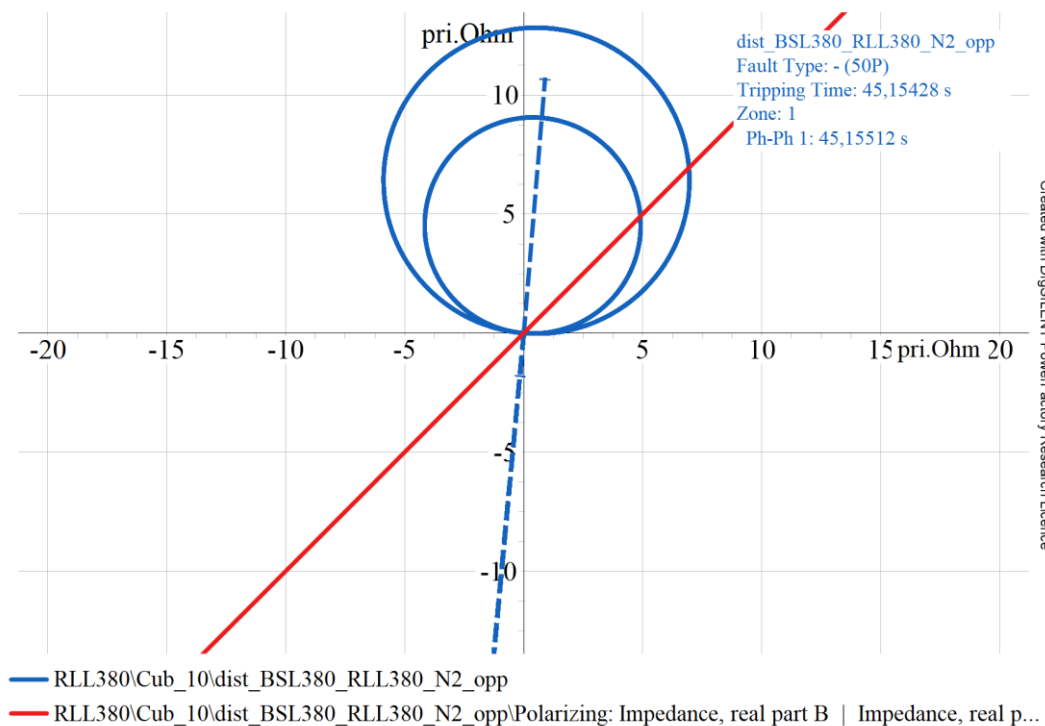


Figure 3-20: Line tripping by out of zone distance protection.

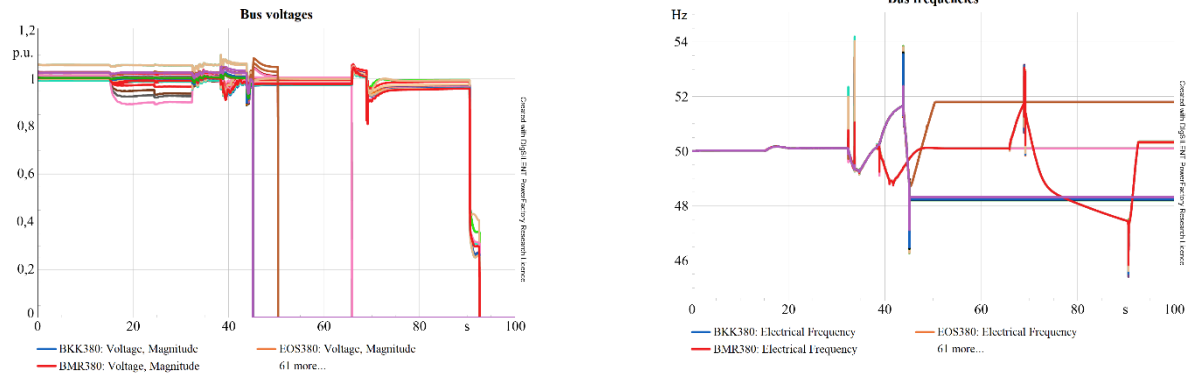


**Figure 3-21: Bus voltages and frequency dynamics.**

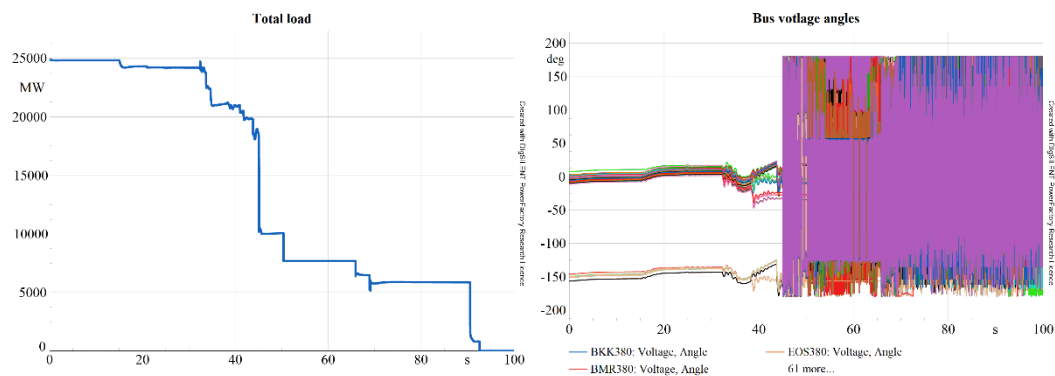


**Figure 3-22: Bus voltage angles and total load.**

#### 3.4.4.4 Impact assessment

The cyber attack use-case scenarios discussed above were generated for the entire Dutch power grid. Two types of cyber attack scenarios were considered for the impact assessment: (1) switching attacks and (2) spoofing attacks. The objective of the analysis is to identify the buses that experience the highest impact and result in significant load loss.

The switching attacks are further classified into multiple categories: (1) disconnection of synchronous generators, (2) disconnection of wind power plants and HVDC interconnectors, (3) disconnection of loads, and (4) disconnection of elements connected to a substation, such as transmission lines, shunt elements, and other associated equipment.

The disconnection of substation elements is further divided into two categories: (1) simultaneous disconnection of all selected substation elements at the same time, and (2) coordinated sequential disconnection of substation elements. The second category is designed to capture cascading failure dynamics under different attack coordination strategies and attack sequences.

In all switching attack scenarios, only a single substation, generation source, or load is selected for the impact assessment. Considering multiple substations simultaneously would effectively result in a large N-k contingency, which would likely lead to widespread cascading failures and potentially cause a system-wide blackout immediately.

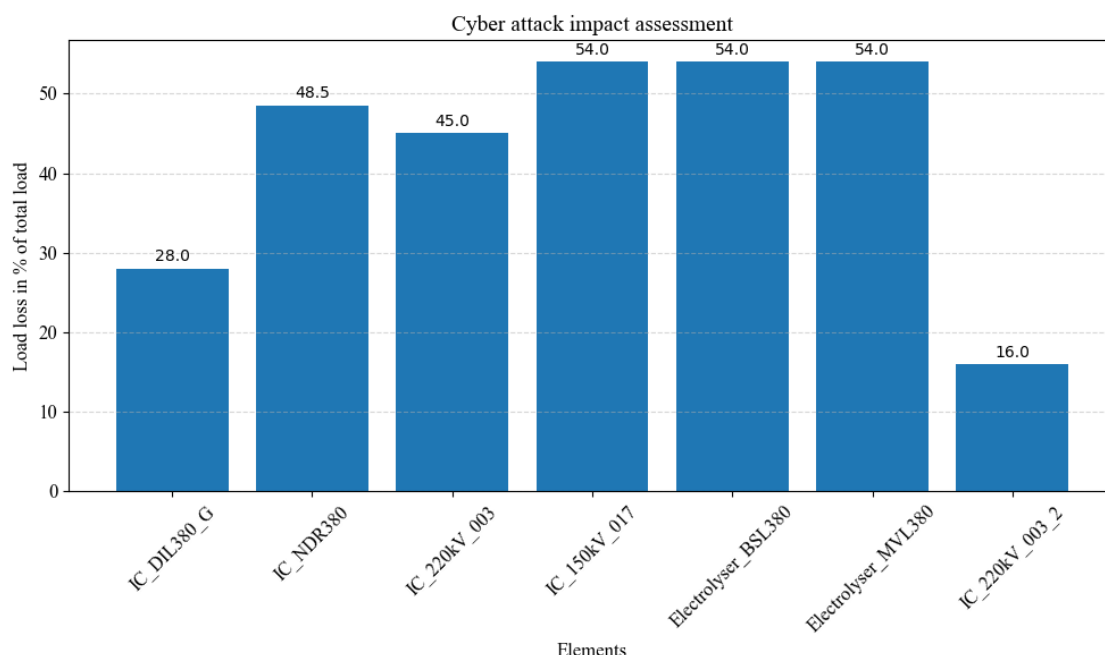


**Figure 3-23: Cyber attack impact assessment caused by element switching attack.**

Figure 3-23 illustrates the system load loss caused by the disconnection of individual elements under the switching attack category. The elements IC\_DIL380\_G and IC\_NDR380 represent interconnection generation sources, while the remaining elements on the x-axis represent loads.

The Dutch power system has a relatively high generation capacity compared to its load demand. Therefore, the disconnection of a small generating unit, such as a wind power plant or a small synchronous generator, can generally be compensated for by the remaining generating sources, thereby maintaining system stability.

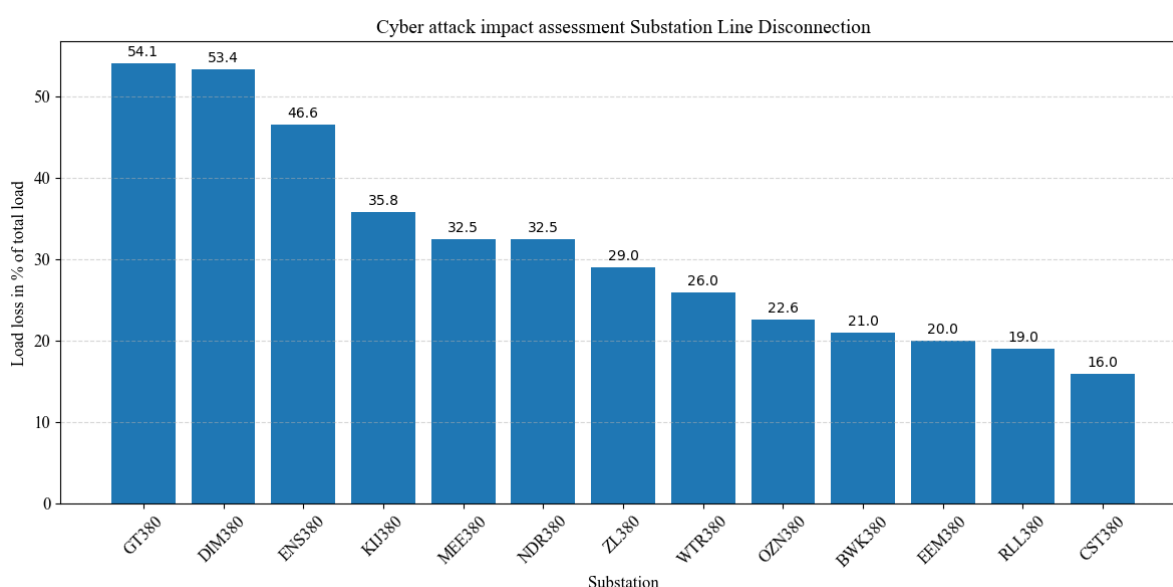


**Figure 3-24: Cyber attack impact assessment caused by substation switching attack.**

Figure 3-24 presents only the cases in which the load loss exceeds 15%. It can be observed that the disconnection of generation sources is largely compensated for by the remaining generators. In

contrast, the disconnection of certain loads results in severe voltage and frequency instability in the affected region. As discussed in the previous chapter, this instability propagates to neighboring substations, leading to cascading failures and ultimately causing a blackout over approximately half of the grid. In total, 70 use cases were generated by considering single-element disconnections. The switching attack is started at 15 seconds and simulation run time is 150 seconds.

Figure 3-24 presents the impact assessment of the substation switching attack. For each substation, a maximum of 11 attack scenarios are generated. In the first scenario, all the substation elements are disconnected simultaneously by the cyber attacker. In the remaining scenarios, the substation elements are disconnected sequentially, with a time interval of 0.5 s between consecutive disconnections.

For a substation containing three elements, the total number of possible attack scenarios is  $(3! + 1) = (6 + 1)$ , where the additional case corresponds to the simultaneous disconnection of all elements. In general, for a substation with  $n$  elements, the total number of attack scenarios is  $(n! + 1)$ . To maintain computational feasibility, a maximum of 10 sequential attack combinations, along with one simultaneous disconnection case, are generated for each substation.

If a substation exhibits similar levels of load loss across all generated attack combinations, it is identified as a highly critical substation for further analysis. Overall, 504 use-case scenarios were generated for the impact assessment.

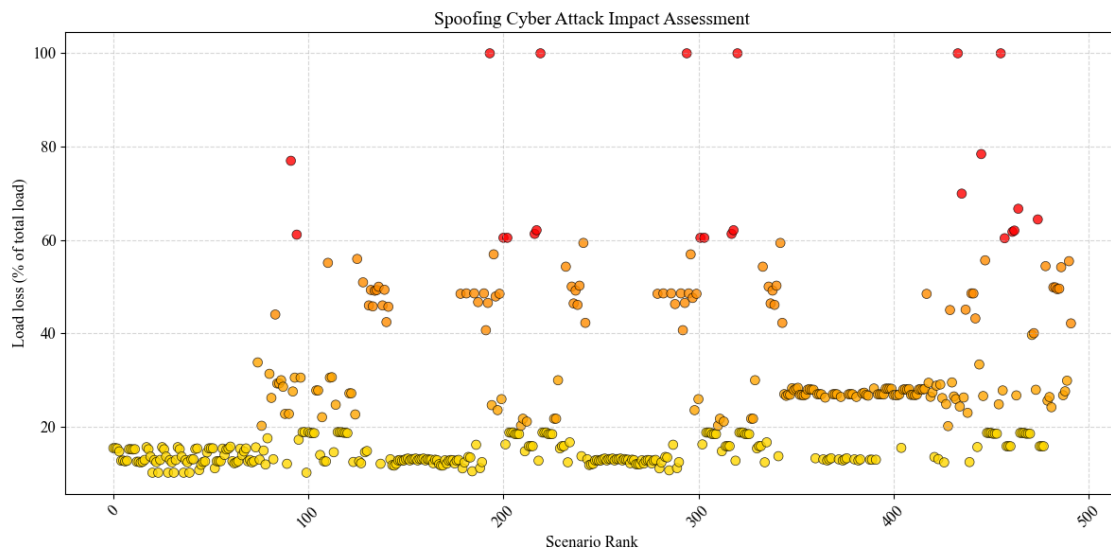


**Figure 3-25: Cyber attack impact assessment caused by substation spoofing attack.**

In the spoofing attack use-case scenario, it is assumed that the attacker has remote access to a digital substation, enabling the attacker to manipulate the reference set points of generator controllers. For example, the attacker can modify the voltage reference of the Automatic Voltage Regulator (AVR) or alter the active power reference ( $P_{set}$ ) of the HVDC interconnectors to introduce disturbances into the network and compromise the stability of the entire power system.

Unlike the switching attack scenarios, the targeted generator, controller, or bus is not immediately disconnected from the network after the attack is launched. Instead, the spoofed control signals first introduce instability into the system. Subsequently, the protection schemes associated with the affected component operate and disconnect the targeted generator or substation from the network, resulting in significant load loss.

The attack is implemented by varying the HVDC active power reference ( $P_{set}$ ) from 1 p.u. to -1 p.u. in increments of 0.5 p.u., taking advantage of the bidirectional power transfer capability of HVDC converters. Simultaneously, the voltage reference of the synchronous generator AVRs is varied from 0.90 p.u. to 1.10 p.u. in increments of 0.05 p.u. These parameter combinations result in a total of 1,120 use-case scenarios.

During the simulations, cases that resulted in simulation errors or negligible load loss were excluded from the analysis. After the cyber attack use cases were executed, there was significant divergence, an inadequate power mismatch, and unsolvable controller equations, which resulted in simulation crashes or produced a simulation error or calculation error within the software tool; this is not related to the developed model or methods, but rather to the system's algebraic calculations. Consequently, Figure 3-25 presents only the scenarios in which the load loss exceeds 15%. The attack is initiated at 15 s, and each simulation is performed for a total duration of 150 s.

As shown in Figure 3-25, the spoofing attack is considerably more severe than the switching attack. Several attack scenarios result in a complete system-wide blackout (100% load loss), while many other scenarios lead to the blackout of approximately half of the power grid. These results demonstrate the significant impact that coordinated spoofing attacks on controller reference signals can have on the stability and resilience of the Dutch power grid.

#### 3.4.4.5 Point of No Return (PNR)

The PNR is defined as the operating point beyond which the power system enters a state of global instability, making system collapse inevitable. The anatomy of a cascading failure typically consists of two distinct phases. The first is a slow cascading phase, which may last from several minutes to a few hours and is characterized by the gradual propagation of disturbances throughout the network. As the system deteriorates, it reaches a critical point known as the PNR where the overall system loses its ability to recover to a stable operating condition, even if corrective control actions are applied. Beyond the PNR, the system enters a fast cascading phase, which lasts only a few seconds and results in rapid disconnection of system components through protection mechanisms, eventually leading to a partial or complete blackout. Therefore, identifying the PNR is essential for detecting the onset of global instability and enabling preventive control actions before irreversible cascading failures occur.

In this work, the PNR is identified using synchronized voltage measurements obtained from Phasor Measurement Units (PMUs). The methodology utilizes bus voltage signals to quantify the transition from a stable operating state to global instability.

The acquired PMU voltage signals are first processed using an autocorrelation function to identify persistent oscillatory behavior while suppressing measurement noise. The autocorrelation analysis enhances the oscillatory characteristics of the signal, allowing sustained voltage oscillations or dynamic changes to be detected effectively. A high autocorrelation value indicates the presence of persistent oscillations during the corresponding time interval. Once oscillatory behavior is detected, the processed signals are analysed using the Empirical Wavelet Transform (EWT) to obtain localized frequency components in the form of Intrinsic Mode Functions (IMFs) [16]. Considering a mother wavelet, dilation parameter  $s$  and translation parameter  $u$ , the wavelet dictionary is defined as follows (4),(5):

$$\psi_{u,s}(t) = \frac{1}{\sqrt{s}} \psi\left(\frac{t-u}{s}\right) \quad (4)$$

$$f(t) = w(0, t) \star \phi_1(t); f_k(t) = w(k, t) \star \psi_k(t) \quad (5)$$

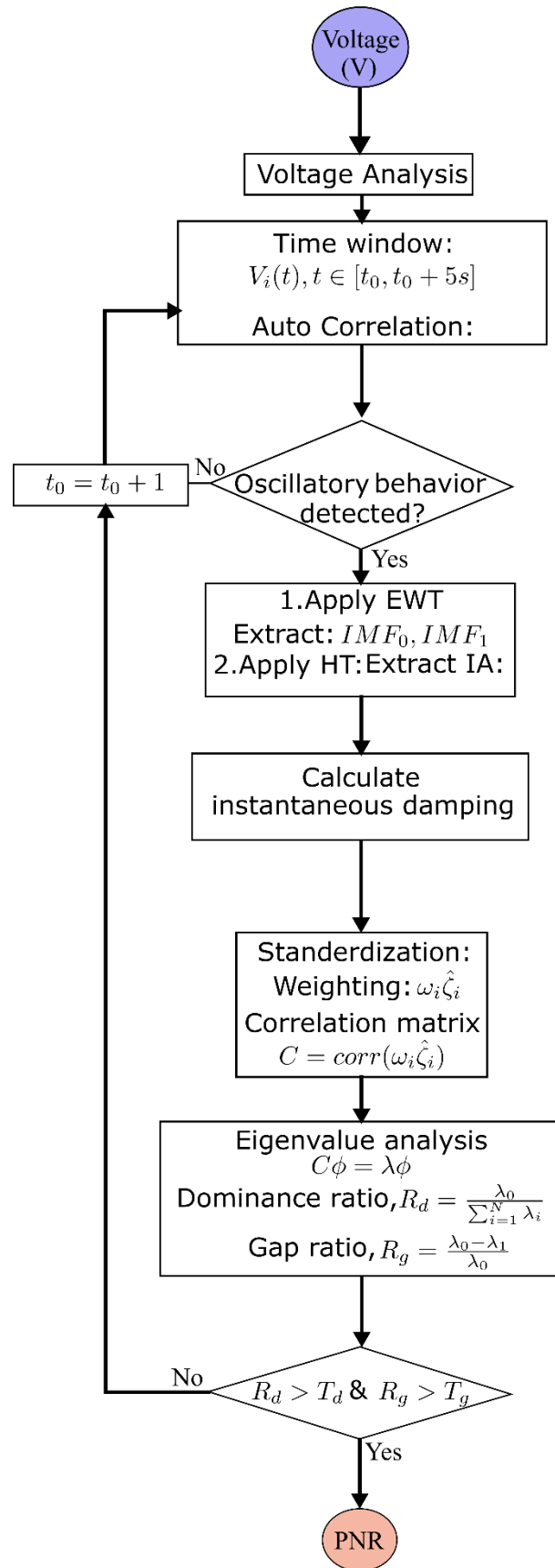


Figure 3-26: Flow chart of PNR quantification method.

The wavelet transform of a signal ( $f$ ) is defined as the inner product between the signal and a wavelet function, expressed as  $\langle \omega_f = f, \psi \rangle$ . The EWT, first proposed by Gilles [16], is an adaptive signal decomposition technique that constructs wavelets based on the spectral characteristics of the input signal. Unlike conventional wavelet transforms that employ predefined basis functions, EWT develops a set of adaptive wavelets whose frequency supports are determined directly from the signal spectrum. This approach can be interpreted as constructing a bank of adaptive band-pass filters, where each filter corresponds to a specific frequency scale.

The construction of empirical wavelets begins by estimating the local maxima of the Fourier spectrum of the processed signal. The boundaries between adjacent frequency bands are then determined as the midpoints between two successive spectral maxima. Consequently, the Fourier support  $[0, \pi]$  is partitioned into ( $N$ ) contiguous segments. To ensure smooth transitions between adjacent frequency bands, a transition region of width ( $2\tau_m$ ) is introduced around each boundary ( $\omega_m$ ). The detailed procedure for selecting ( $\tau_m$ ) is described in [16].

Based on these adaptive frequency partitions, the empirical wavelets are constructed as one low-pass filter, ( $\widehat{\phi}_m$ ), representing the approximation component, and ( $N-1$ ) band-pass filters, ( $\widehat{\psi}_m$ ), representing the detail components associated with each frequency segment. These adaptive filters decompose the PMU measurements, including frequency and Positive-Sequence Voltage Magnitude (PSVM), into localized frequency bands.

Subsequently, the Hilbert Transform (HT) is applied to the extracted IMFs to analyze their temporal modal characteristics. The combination of the EWT and the Hilbert Transform enables a detailed time-frequency analysis of nonlinear and non-stationary power system signals. For a given time-series signal ( $u(t)$ ), the dominant first two IMF first extracted using the decomposition technique. The conventional Hilbert–spectral analysis (HSA) suffers from two well-known limitations: mode mixing, which occurs when frequency components with similar frequencies appear within the same IMF, and the presence of low-frequency components that may degrade the decomposition quality. To overcome these limitations, IMFs are utilized. This approach automatically identifies the optimal masking signal frequencies according to the inherent dynamics of the input signal, thereby improving the separation of oscillatory modes and enhancing the accuracy of the decomposition.

Using the Hilbert transform, the analytic signal corresponding to each IMF is obtained and expressed in exponential form as (6)-(8)

$$H[u(t)] = -\frac{1}{\pi} \int_{\epsilon}^{\infty} \frac{u(t + \tau) - u(t - \tau)}{\tau} d\tau \quad (6)$$

$$z(t) = A(t)e^{j\phi(t)} = u(t) + jH[u(t)] \quad (7)$$

$$A(t) = \sqrt{u^2(t) + H^2[u(t)]} \quad (8)$$

where ( $A(t)$ ) and ( $\phi(t)$ ) denote the instantaneous amplitude and instantaneous phase, respectively.

The analytic signal provides direct access to important instantaneous parameters, including the amplitude, phase, and frequency of the oscillatory modes. Among these quantities, the instantaneous amplitude provides valuable information regarding the growth or decay of system oscillations.

The instantaneous amplitude and phase are subsequently utilized to estimate the instantaneous damping, which serves as an important indicator of power system stability (9). The damping is calculated as the ratio of the time derivative of the instantaneous amplitude to the amplitude itself, i.e.,

$$\alpha(t) = -\frac{\dot{A}(t)}{A(t)} \quad (9)$$

where ( $\dot{A}(t)$ ) represents the derivative of the instantaneous amplitude with respect to time.

The estimation of instantaneous damping provides deeper insight into the dynamic response of the power system while preserving the temporal characteristics of the measured signals. Consequently, this methodology enables accurate tracking of oscillation growth and decay, facilitating early detection of instability and identification of the PNR during cascading failures. The application of these instantaneous parameters for stability assessment is discussed in the subsequent sub-chapters.

Once the analytic signal has been obtained from the Hilbert transform, several instantaneous characteristics of each IMF can be extracted. These include the Instantaneous Amplitude (IA) and Instantaneous Frequency (IF). The instantaneous frequency provides information about the oscillatory modes present in the measured signal, whereas the instantaneous amplitude is utilized to quantify the dynamic behavior of the oscillations as shown in Figure 3-26.

The instantaneous amplitude is subsequently employed to estimate the Instantaneous Damping (ID) using (9). The damping profile indicates the evolution of system stability following the initiating disturbance. Positive or increasing damping values correspond to a decaying oscillatory response, whereas decreasing or negative damping values indicate growing oscillations and the onset of instability.

For each bus  $i$  in the analysis window, computed a normalized damping sequence  $d_i$  derived from the dominant intrinsic mode functions IMF0, IMF1, and scale it by the short circuit MVA rating of that particular bus,  $w_i$ , to obtain  $\tilde{d}_i = w_i d_i$ . This scaled quantity is used solely to determine whether a bus exhibits meaningful oscillatory content. A bus is retained for further analysis only if  $\text{std}(\tilde{d}_i) > \tau$ , where  $\tau = 10^{-6}$ . Since  $w_i$  is a positive constant, this condition is equivalent to requiring  $\text{std}(d_i) > \tau/w_i$ , meaning the effective variance threshold is inversely scaled by inertia higher-inertia buses require less raw damping variance to be classified as oscillating, while lower-inertia buses require more, consistent with the physical expectation that smaller buses must show proportionally larger relative variation to represent genuine oscillatory behavior rather than noise. Once the retained bus set is determined, the coherency structure among these buses is computed using standard Pearson correlation on the unscaled damping sequences  $d_i$ , not on the weighted sequences  $\tilde{d}_i$ . This is a deliberate methodological choice rather than an oversight, because Pearson correlation normalizes by the standard deviation of each input, it is invariant to positive rescaling, so  $\rho(w_i d_i, w_j d_j) = \rho(d_i, d_j)$  for any positive  $w_i, w_j$  and applying the inertia weighting directly within the correlation calculation would have no numerical effect on the resulting coefficients. The correlation matrix used for the subsequent eigen-decomposition therefore captures oscillatory shape and pattern similarity among buses independent of their inertia, while inertia instead governs which buses are admitted into that matrix in the first place. Since the damping signals obtained from different buses have varying magnitudes, all ID signals are first normalized to establish a common scale for comparison. To account for the electrical significance of each measurement location, a weighting factor is assigned based on the short-circuit MVA of the corresponding bus as shown in Figure 3-26. Buses with higher short-circuit

capacity generally have a stronger influence on voltage dynamics; therefore, incorporating this weighting improves the representation of the overall system response.

The normalized and weighted damping signals are then used to construct a weighted correlation matrix. Unlike individual bus measurements, the correlation matrix captures the collective interaction among voltage responses throughout the network,  $C$  is the correlation matrix ( $C \in \mathbb{R}^{N \times N}$ ) where  $N$  is the total number of bus voltages,  $(\lambda)$  is the eigen matrix (10) and  $(\phi)$  is the eigen vector. Consequently, it enables the distinction between localized disturbances and disturbances that propagate across the entire system, thereby providing an indication of global voltage instability.

$$\lambda = \begin{bmatrix} \lambda_0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{bmatrix} \quad (10)$$

Where  $\lambda_0 > \lambda_1 > \lambda_2 > \cdots > \lambda_n$

Finally, PNR is computed from the weighted correlation matrix using two complementary metrics: the system dominance ratio (11)

$$R_d = \frac{\lambda_0}{\sum_{i=1}^N \lambda_i} \quad (11)$$

and the eigenvalue gap ratio (12)

$$R_g = \frac{\lambda_0 - \lambda_1}{\lambda_0} \quad (12)$$

where  $(\lambda_0)$  and  $(\lambda_1)$  denote the largest and second-largest eigenvalues of the weighted correlation matrix, respectively. The point of no return (PNR) is identified when both the system dominance ratio ( $R_d$ ) and the eigenvalue gap ratio ( $R_g$ ) exceed their respective threshold values ( $T_d$ ) and ( $T_g$ ). At the PNR, the dominant eigenvalue ( $(\lambda_0)$ ) approaches unity ( $(\lambda_0 \approx 1)$ ), indicating that a single dominant mode governs the system dynamics. The dominance ratio quantifies the contribution of the principal eigenvalue to the overall system dynamics, while the eigenvalue gap ratio measures the degree of separation between the dominant mode and the remaining modes. By combining these two quantities, characterizes the dominant voltage dynamics of the power system and provides a reliable indicator of oscillatory behavior, loss of stability, and progression toward the PNR as shown in Figure 3-27.

From the generated use cases the  $T_d$  is selected as 95% and  $T_g$  as 50. The proposed method successfully able to capture and quantify the PNR in the system by observing the voltage oscillations in the network.

The proposed method is validated using various cyber attack scenarios. One of the case studies considers a switching attack on the Dutch transmission network at the DIM 380 kV substation bus. The attack scenario and the corresponding sequence of events are described in Table 2.

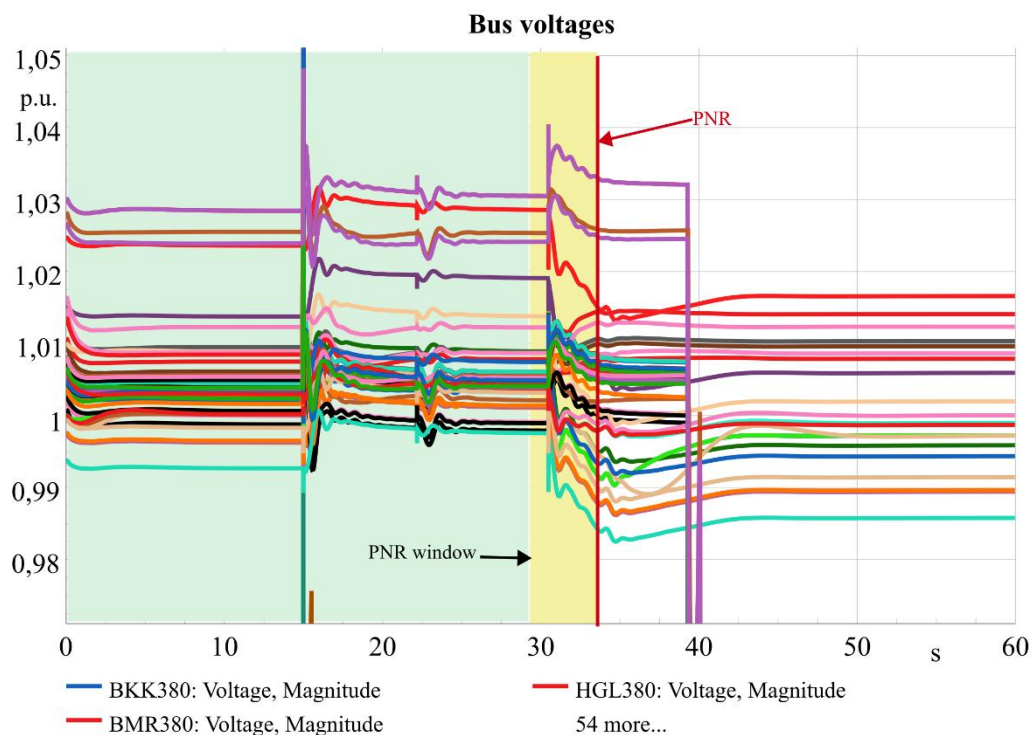


Figure 3-27: Bus voltages dynamics and PNR caused by switching cyber attack scenario.

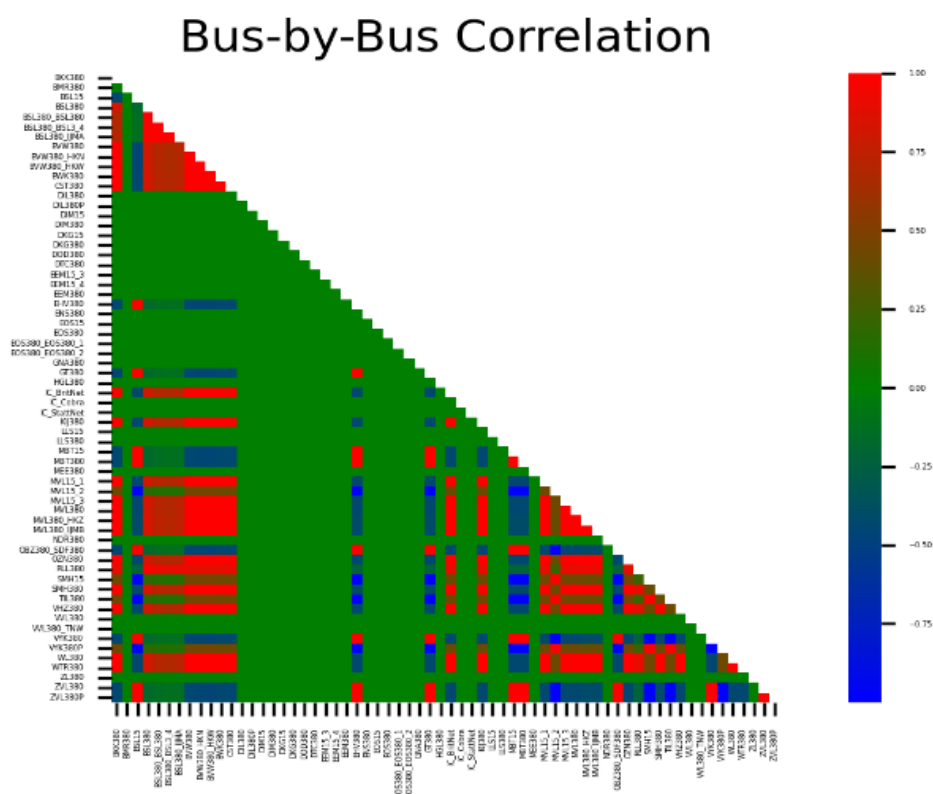


Figure 3-28: Weighted correlation matrix before reaching the PNR.

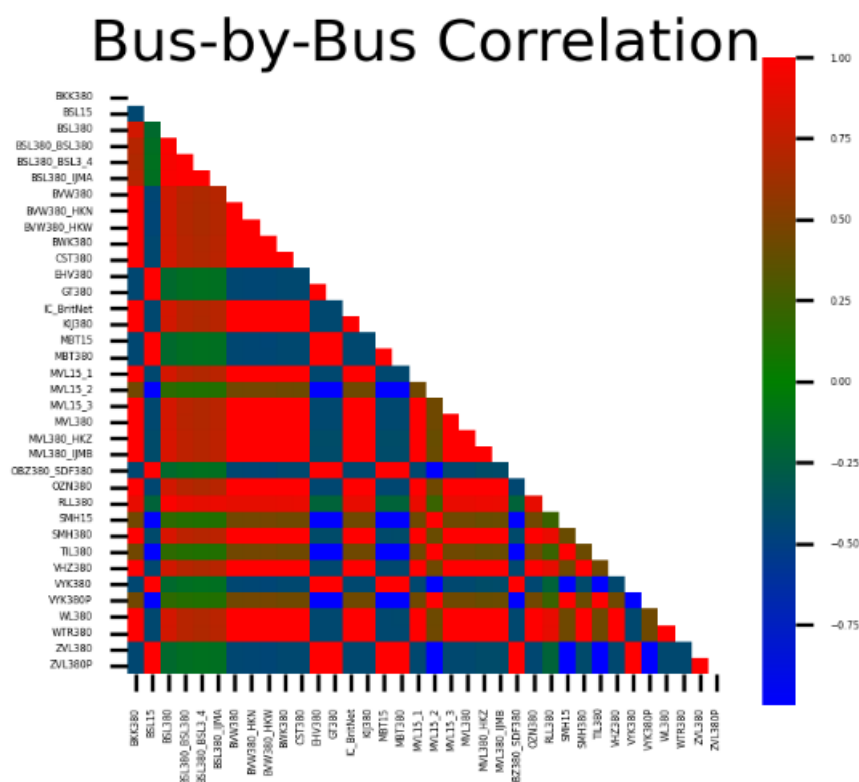


**Figure 3-29: Weighted correlation matrix during the PNR.**

The cyber attack is initiated at 15 s, after which the system begins to exhibit oscillations that are initially damped by the controllers and power system stabilizers. However, following the initial attack, the system experiences cascading tripping, resulting in severe oscillations and a partial blackout.

Using the proposed method, the PNR window between 28 s and 33 s identifies the onset of severe instability, and at 33 s the system is classified as having reached the PNR, as shown in Figure 34. Prior to reaching the PNR, the cross-correlation matrix is predominantly green, indicating normal system behavior without severe oscillations as shown in Figure 3-28. During the PNR time window, however, the correlation matrix reveals that the bus measurements across the entire grid become highly as shown in

Figure 3-29, correlated due to the severe oscillatory behavior, clearly indicating the system's approach to the PNR. This correlation matrix provides an effective visual representation of the evolving grid dynamics.

Immediately after the PNR is reached, several system elements become disconnected because of cascading outages, as illustrated in Figure 3-30, resulting in a partial blackout at approximately 40 s. In the current study, PNR is validated using an implicit recovery criterion the method is tested against blackout scenarios, in which the system is confirmed via full simulation to progress into the fast cascading phase, and PNR is correctly detected before that phase begins in every such case, as a complementary check, in scenarios where the system does not experience fast cascading failure or blackout, the model correctly without pointing the PNR, indicating no fast cascading conditions. However, that the current test scenarios do not include cases with corrective control actions or recoverable disturbances, where the system experiences oscillatory stress but is subsequently stabilized rather than progressing to blackout. This reflects the current scope of the study, which focuses on characterizing the dynamics and detectability of uncontrolled cascading failure rather than

evaluating corrective-action effectiveness. After the corrective actions the system is stabilized without any cascades as presented in the next sections.

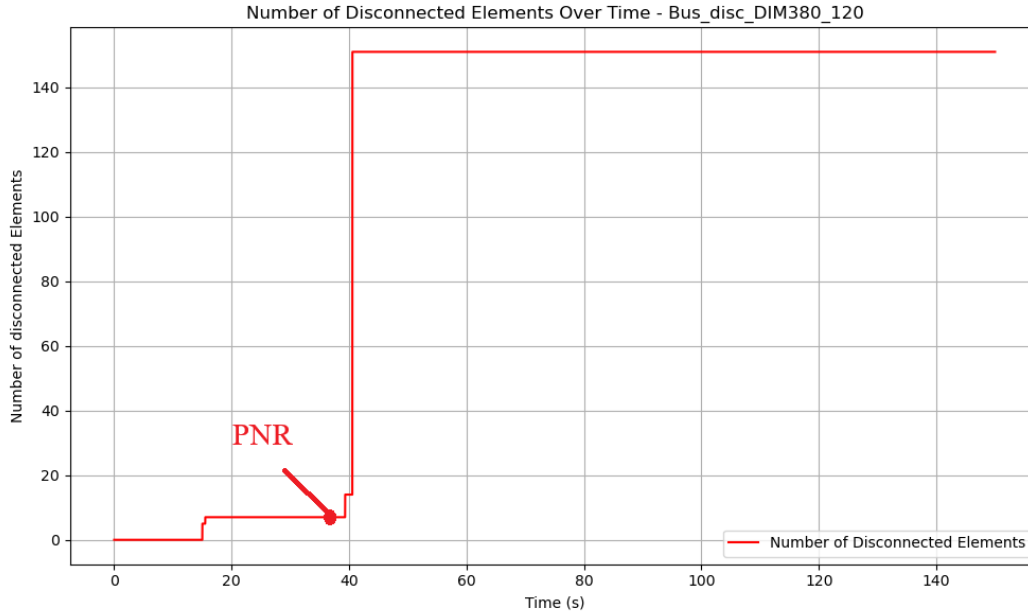


*Figure 3-30: Elements disconnected caused by switching cyber attack scenario.*

#### 3.4.4.6 Cyber Attack Mitigation

The DT can be used by the operator to simulate a range of cyber attack scenarios, with particular emphasis on weak zones identified by the cyber security team during the early stages of intrusion detection. Leveraging this information, the DT operator can predict potential cyber attack events and their locations, and assess their impact on power system stability and grid operation. The occurrence of a disturbance disrupts the equilibrium between generation and demand within the affected portion of the power system, resulting in a local power imbalance. In the above section have demonstrated that the post-disturbance network can be partitioned into generator-dominant and load-dominant regions, thereby facilitating the analysis of interregional power exchange. Building upon this concept, the proposed framework first partitions the power network into a set of clustered regions using the initial power flow solution, such that each region exhibits a locally balanced power-flow distribution. To enable efficient exploration of the network topology, the Breadth-First Search (BFS) algorithm is employed as the graph traversal strategy throughout the clustering process [17]. Based on the resulting post-fault clustered network, a generalized classification of generator-rich and load-rich regions is subsequently established. Specifically, the net power imbalance of each clustered region is computed using the methodology described in the previous section. According to the sign of the resulting net power balance, each clustered region is classified as either load-rich as in (13) or generator-rich as in (14), as defined by

$$\sum_{i \in W_k} P_{G_i} + \sum_{i \in \delta_k} \eta_{L_i}^k P_{L_i} < 0, \quad (13)$$

for a load-rich region, and

$$\sum_{i \in W_k} P_{G_i} + \sum_{i \in \delta_k} \eta_{L_i}^k P_{L_i} > 0, \quad (14)$$

for a generator-rich region.

Where  $P_{G_i}$  and  $P_{L_i}$  denote the active power generation and active power demand at node  $i$ . Moreover, for each node  $i$ ,  $\eta_{L_i}^k$  denotes the proportion of the nodal power flow attributed to clustered region  $k$ . This factor is utilized to determine the regional net power imbalance.

Furthermore, excessive loading of transmission lines following a disturbance increases the likelihood of relay tripping, thereby escalating the risk of cascading failures. The subsequent evolution of a cascading failure is primarily governed by two factors. The first is the overall severity of line overloading across the network, while the second is the spatial extent to which the disturbance propagates beyond the faulted area. Owing to communication and control delays, system operators responsible for geographically distant regions may have insufficient situational awareness and limited time to implement corrective actions. Consequently, evaluating both the local and nonlocal impacts of a disturbance is essential for assessing the vulnerability of the post-fault system.

To quantitatively characterize these effects, three overload performance indices are utilized. Let ( $E_{\text{fault}}$ ) denote the set of transmission branches located within the fault-affected region, and let ( $E_{\text{left}}$ ) represent the set of all remaining branches in the network. These sets satisfy as in (15)

$$E_{\text{fault}} \cup E_{\text{left}} = E, \quad E_{\text{fault}} \cap E_{\text{left}} = \emptyset, \quad (15)$$

where  $E$  is the complete branch set of the transmission network. For a power system with branch capacity scaling factor  $\alpha$ , the overload ratio associated with each branch is defined as in (16)

$$OV_e = \begin{cases} \frac{f_e - \alpha f_e^0}{\alpha f_e^0}, & \text{if } f_e > \alpha f_e^0, \\ 0, & \text{otherwise,} \end{cases} \quad (16)$$

where  $f_e$  and  $f_e^0$  denote the post-fault and reference (pre-fault) power flows of branch  $e$ , respectively. Based on the branch overload ratio, three system-level indices are given as follows (17). The overload index within the fault-affected region is

$$OVI = \sum_{e \in E_{\text{fault}}} OV_e \quad (17)$$

whereas the overload index corresponding to the unaffected portion of the network as (18)

$$OO = \sum_{e \in E_{\text{left}}} OV_e \quad (18)$$

Finally, the overall system overload index is defined as (19)

$$OVT = \sum_{e \in E} OV_e \quad (19)$$

Collectively, these indices provide a comprehensive assessment of post-disturbance system stress by quantifying overload severity within the faulted region, its propagation to remote areas, and the cumulative loading condition of the entire transmission network.

### 3.4.4.6.1 Attack mitigation for Load cyber attack

In this cyber attack scenario, the adversary targets a high-load circuit breaker supplying approximately 1.4 GW of demand, with the objective of disconnecting it from the transmission network. If the attack is successful, the initial outage causes a redistribution of power flows, leading to the overloading of neighbouring and inter-zonal transmission lines. These overloads activate protection schemes, resulting in successive line outages and initiating a slow cascading failure. As the cascade progresses, the system experiences unintentional islanding and significant operational disturbances, as discussed in the previous section.

To mitigate this attack, the DT of the power system was employed to perform multiple contingency and operational analyses. The disconnected load is located in the Noord-Holland 380 kV zone and is connected to the DIM380 bus. The application of the mitigation strategy demonstrates that reducing generation within the affected zone alleviates transmission line loading and limits the redistribution of power flows following the circuit breaker outage. Consequently, the likelihood of protection-induced transmission line trips is reduced, effectively mitigating the propagation of the cascading failure. The single-line diagrams of the system before and after the implementation of the mitigation strategy are presented in Figure 3-31. As shown in the figure, the cyber attack causes the disconnection of a significant portion of the system load under the baseline scenario. In contrast, after the mitigation strategy is applied, the cascading outage is effectively contained, enabling the power system to maintain stable operation while supplying the majority of the connected load.

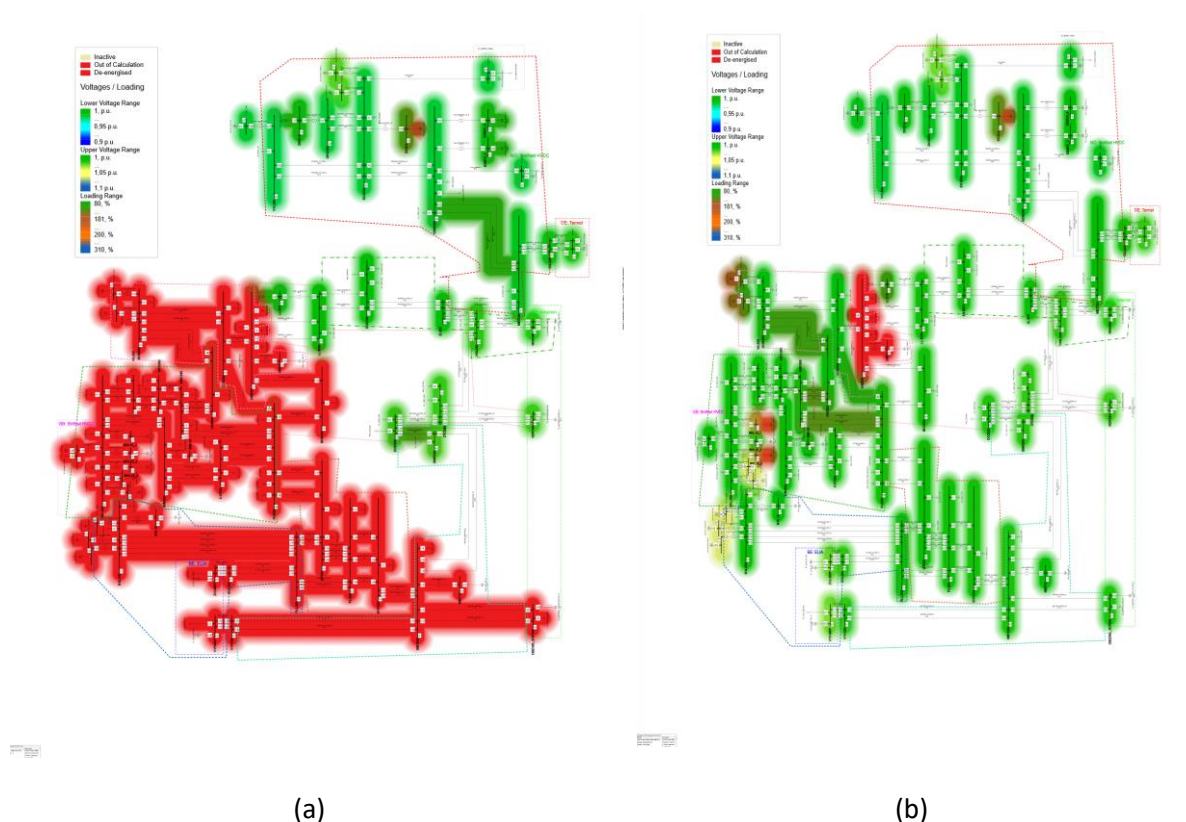


**Figure 3-31: The SLD of the synthetic digital model of the Dutch power system (a) without and (b) with the mitigation strategy. Different colours indicate the voltage levels and loading.**

The dynamic response of the system under the cyber attack and after the implementation of the mitigation strategy is presented in Figure 3-32–Figure 3-34. The bus voltage profiles, shown in Figure 34, demonstrate that the system voltages remain within acceptable operating limits. Similarly, the bus voltage angle responses, presented in Figure 3-32, indicate improved system stability. The bus frequency responses, illustrated in Figure 3-34., remain within the permissible operating range, confirming the effectiveness of the control actions. Finally, Figure 3-35 shows that the available generation is sufficient to meet the remaining system demand, demonstrating that the load is supplied reliably while maintaining a stable operating condition.

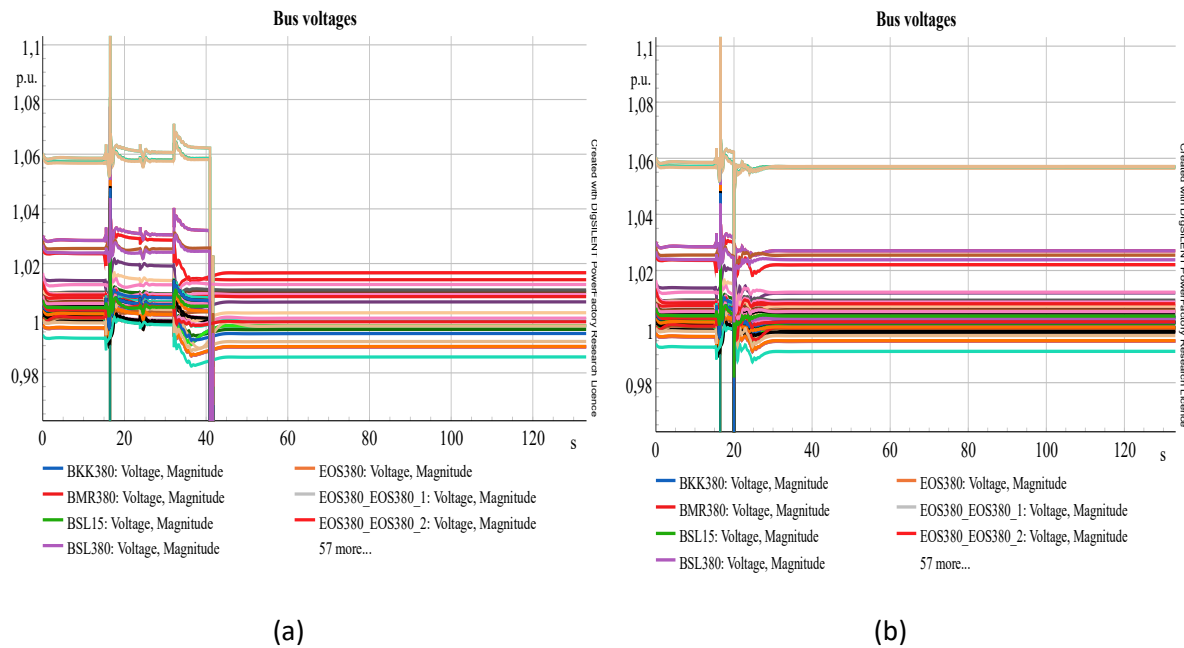


**Figure 3-32: Bus voltages (a) before and (b) after applying the mitigation strategy.**

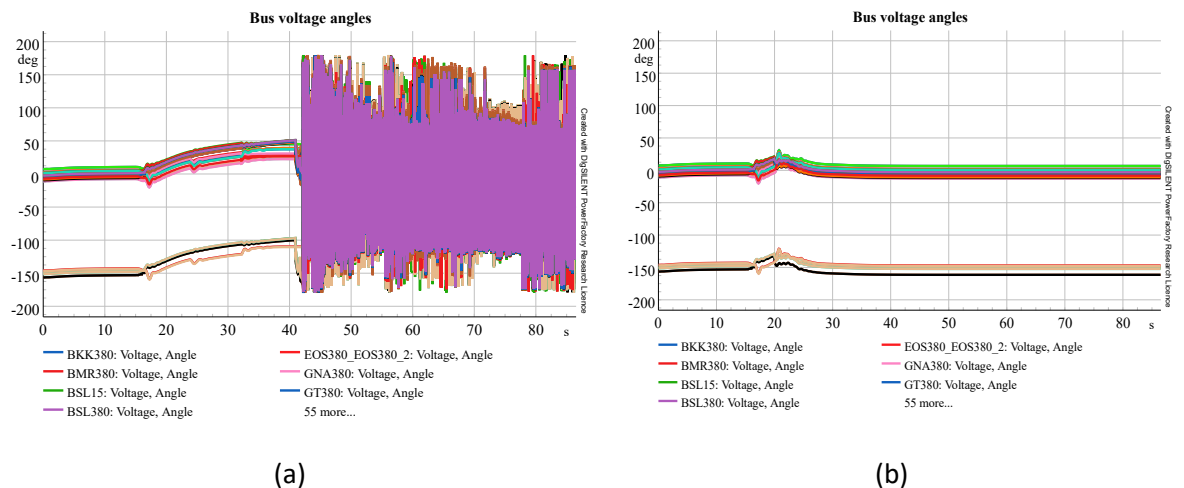


**Figure 3-33: Bus voltage angles (a) before and (b) after applying the mitigation strategy.**

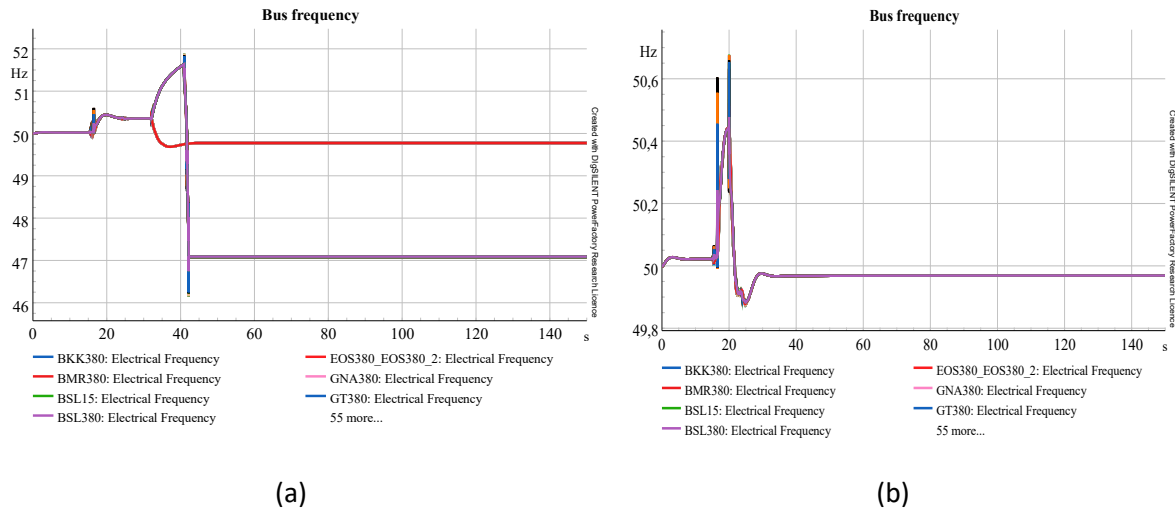


**Figure 3-34: Bus frequency (a) before and (b) after applying the mitigation strategy.**

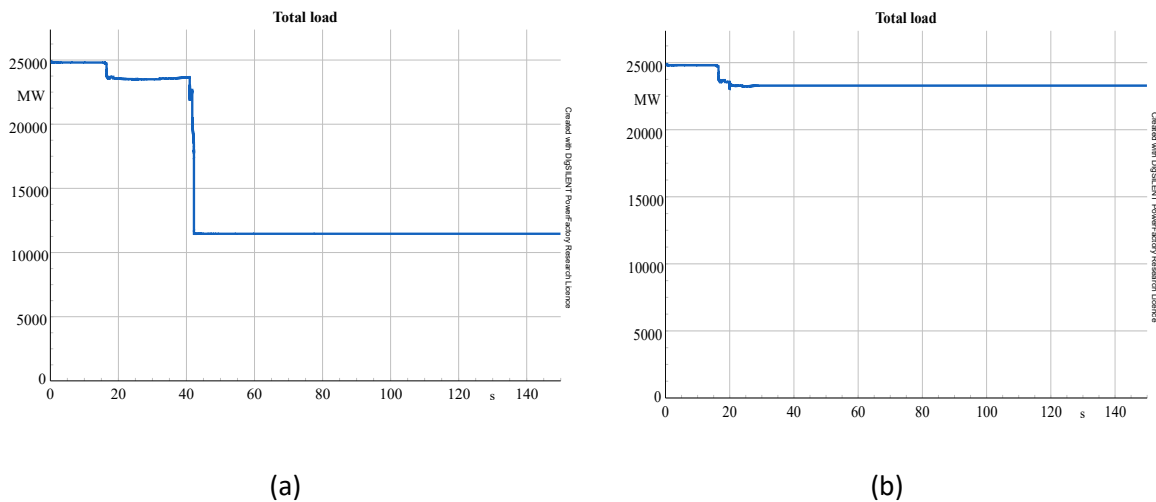


**Figure 3-35: Total load (a) before and (b) after applying the mitigation strategy.**

### 3.4.4.6.2 Attack mitigation for switching attack

In this case, multiple circuit breakers associated with the MEE380 bus were intentionally opened to emulate a cyber-induced contingency. The attack results in the disconnection of several transmission lines, causing severe power flow redistribution and overloading of the remaining corridors. This condition subsequently triggers protective relay operations, leading to unintended system islanding and loss of synchronism.

To mitigate this attack, the DT operator simulates and evaluates multiple contingency and operational scenarios. The analysis identifies that the disconnected elements are located in the Groningen–Drenthe 220/380 kV zone. The mitigation strategy is implemented and controlled load curtailment implemented in the affected area, thereby relieving transmission congestion and redistributing power flows in a stable manner. As a result, the protection-induced transmission line tripping is reduced, effectively arresting the progression of the cascading failure.

The single-line diagrams of the system before and after the implementation of the mitigation strategy are presented in Figure 3-36. As observed, the cyber attack scenario leads to widespread load

loss and significant network disruption. In contrast, the application of the mitigation strategy effectively contains the cascading outage, allowing the system to maintain secure and stable operation while supplying the majority of the connected demand.

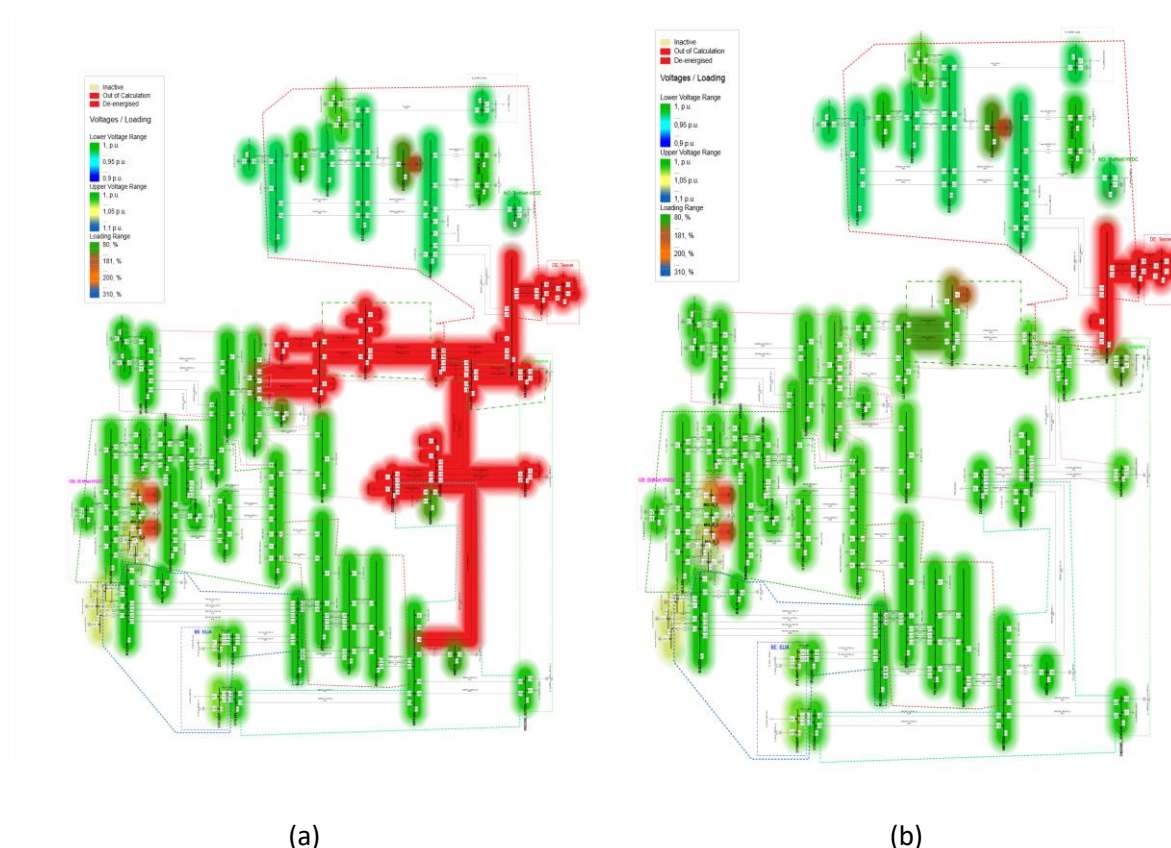


**Figure 3-36: The SLD of the synthetic digital model of the Dutch power system (a) without and (b) with the mitigation strategy. Different colours indicate the voltage levels and loading.**

The dynamic behaviour of the power system under the cyber attack scenario and following the application of the mitigation strategy is illustrated in Figure 3-37–Figure 3-40. Figure 3-37 presents the bus voltage profiles, which confirm that voltage magnitudes are effectively regulated and remain within statutory operating limits despite the disturbance. The corresponding bus voltage angle dynamics is depicted in Figure 3-38, indicating improved rotor-angle stability. Frequency evolution, shown in Figure 3-39, remains bounded within the allowable deviation band, reflecting effective active power balancing and control response. Finally, Figure 3-40 demonstrates that post-mitigation generation adequacy is maintained, ensuring secure load supply and overall system stability under the restored operating condition.

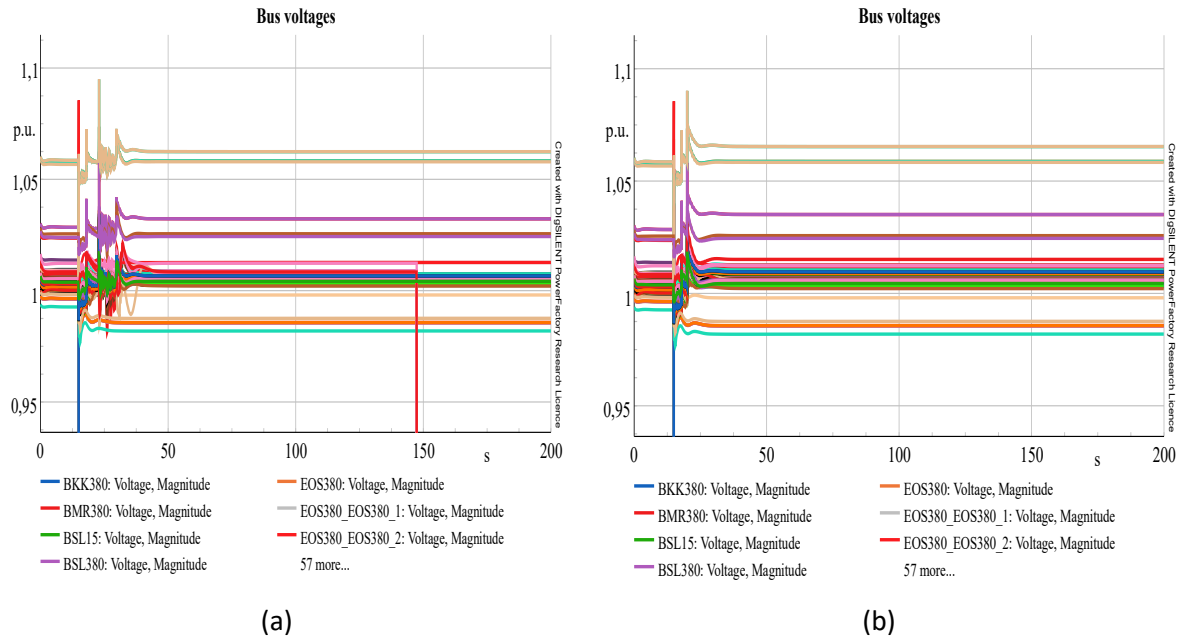


**Figure 3-37: Bus voltages (a) before and (b) after applying the mitigation strategy.**

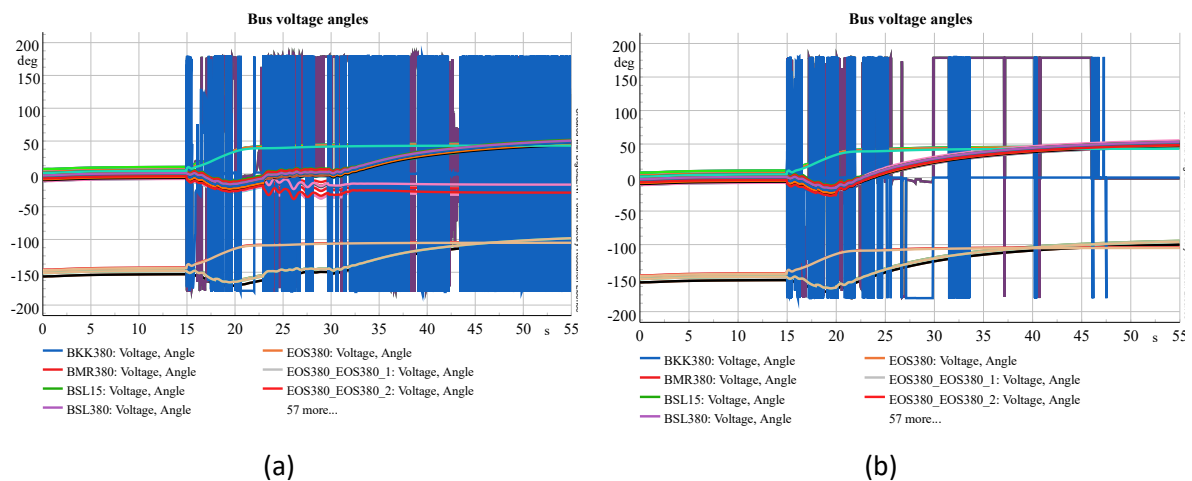


**Figure 3-38: Bus voltage angles (a) before and (b) after applying the mitigation strategy.**

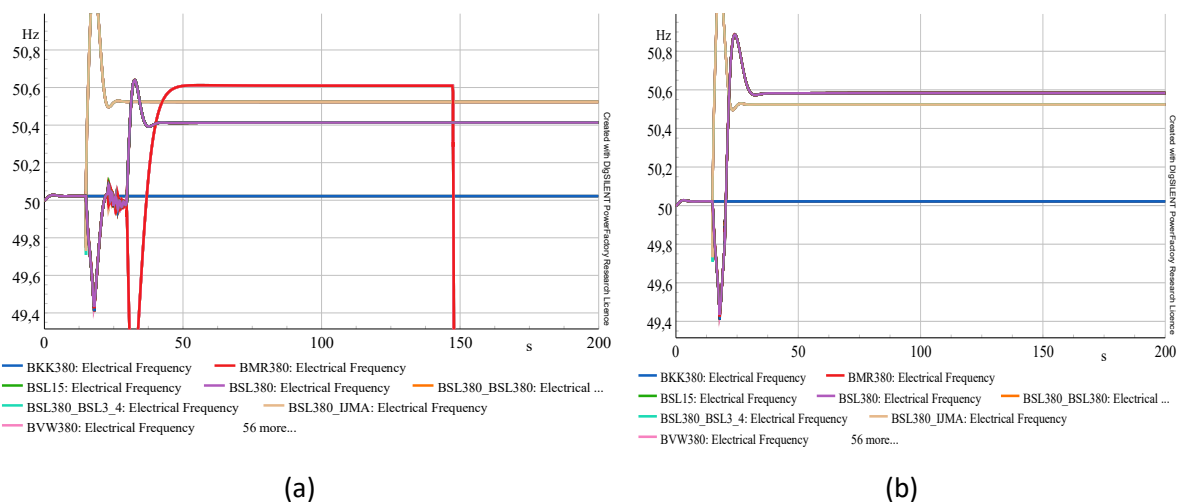


**Figure 3-39: Bus frequency (a) before and (b) after applying the mitigation strategy.**

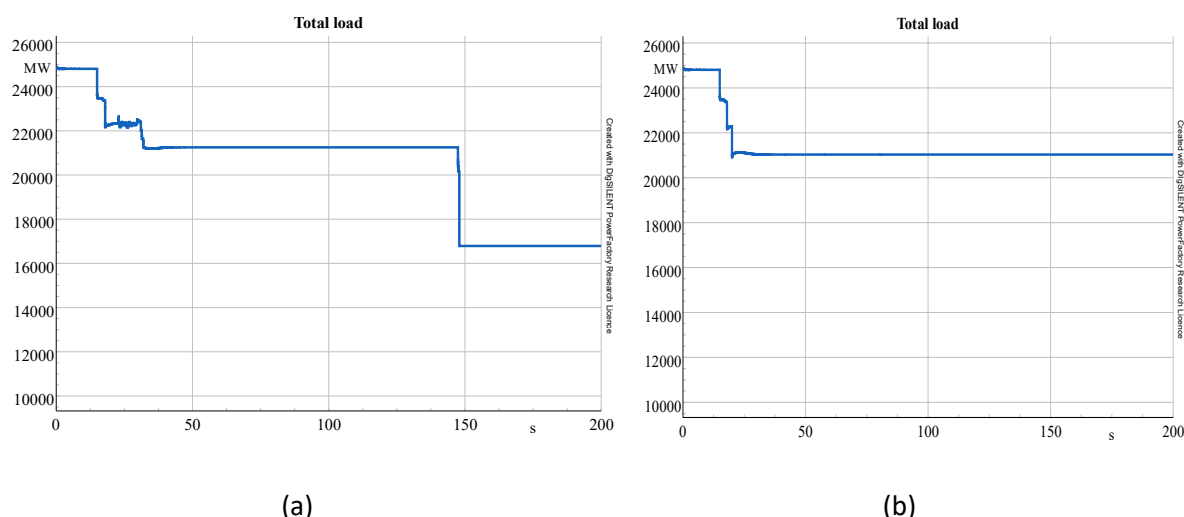


*Figure 3-40: Total load (a) before and (b) after applying the mitigation strategy.*

### 3.5 Alignment with Digital Twin Concepts

The developed DT of the integrated Dutch network demonstrates the practical realization of cyber-physical DT concepts through continuous synchronization between the physical grid and its virtual representation. The physical grid and its DT exchange data continuously, where the physical grid shares measurements, circuit breaker statuses, and control setpoints with the DT. The DT then updates its internal state and performs simulations using real-time operational data from the physical grid. The dynamic behaviour of the proposed DT updated using incoming data streams, ensures a representation of the corresponding physical system. The proposed framework integrates DiGSILENT PowerFactory, mininet-based network emulation, and OPC UA communication, enabling interoperable cyber-physical co-simulation of both power system and communication network dynamics. The DT environment supports cyber attack impact analysis, attack detection, cascading failure analysis, and mitigation planning by emulating realistic network behaviour under both normal and anomalous operating conditions.

The DT-integrated attack detection module further extends the DT concept toward distributed and federated cyber security intelligence. Each substation is emulated as a distributed client within the DT environment, enabling local traffic monitoring and attack detection. In this architecture, each substation DT operates as a local Federated Learning (FL) agent that continuously monitors OT traffic and performs local intrusion detection. To address data privacy and regulatory constraints, the DT attack detection module adopts a cross-silo federated learning paradigm, where substations locally train intrusion detection models and share only model parameters with a central aggregation server using the FedAvg algorithm. This enables system-wide cyber intrusion learning without centralizing sensitive OT data. Thus, The proposed DT framework demonstrates the potential for federated DT ecosystems in future Pan-European energy infrastructures. The distributed substation DT clients, interoperable communication interfaces, and federated cyber security analytics establish the basis for collaboration among geographically distributed system operators while considering data sovereignty and regulatory constraints. Furthermore, the DT environment supports cascading failure assessment and mitigation validation under cyber attack scenarios, enabling operators to evaluate preventive and corrective actions before deployment in the physical grid.

## 4 T5.3 Overview

### 4.1 Challenges Addressed by the Task

The transition towards decentralized and renewable-based energy systems introduces a series of operational and structural challenges for Distribution System Operators (DSOs). In Cyprus, the rapid deployment of photovoltaic systems, coupled with the limited flexibility of existing grid infrastructure, creates conditions prone to local congestion and grid instability. Moreover, as grid operations become increasingly digitalized, new vulnerabilities emerge related to cyber security and system coordination. Task 5.3 aims to focus on these challenges and develop a digital twin of a portion of Cypriot distribution grid that will enable the development of a use case entitled “congestion management in distribution grids through ancillary services”. This use case addresses these multifaceted challenges by integrating into a digital twin framework several tools to enhance congestion management capabilities, optimize the use of distributed flexibility, and improve the resilience of grid operations. More specifically, the challenges addressed in this use case under the Task 5.3 framework are described below:

- High Penetration of Photovoltaic (PV) and Localized Congestion.

Cyprus benefits from abundant solar resources, making PV systems a key component of the national energy strategy. However, the rapid and concentrated deployment of PV units in specific feeders introduces significant operational challenges. These include voltage regulation issues and thermal limit violations due to reverse power flows and variable generation. Traditional grid infrastructure lacks the flexibility to accommodate such dynamics, leading to localized congestion. The proposed use case addresses these challenges through the coordinated activation of DER flexibility, managed by the DSO.

- Limited Monitoring and Control Capabilities at Distribution Level

Distribution networks have historically operated with limited real-time observability and control compared to transmission systems. The increased variability and bidirectional flows introduced by DERs complicate grid management at the distribution level. This use case leverages a digital twin framework to enhance situational awareness, enabling the DSO to simulate and evaluate multiple operating scenarios, identify potential congestion in advance, and implement proactive mitigation strategies.

- High Cost and Delays in Grid Reinforcement

Addressing congestion through conventional grid reinforcement is both capital-intensive and time-consuming. In the context of accelerating renewable energy integration, relying solely on physical infrastructure upgrades is unsustainable. The use case aims to reduce or defer these investments by utilizing DER flexibility to manage congestion dynamically, thereby maximizing the use of existing infrastructure and improving overall grid efficiency.

- Emerging Cyber security Risks in Digitalized Grid Operations

As DSOs increasingly rely on digital technologies for real-time control and market interactions, the risk of cyber attacks becomes more pronounced. Ensuring the cyber-physical resilience of grid operations is a critical challenge. This use case incorporates the evaluation of cyber attack scenarios within the digital twin environment, providing a platform to analyse vulnerabilities and test

countermeasures without compromising the actual grid. This proactive approach supports the development of robust and secure digital grid management systems.

## 4.2 Architecture of Digital Twin and Description

The architecture of the digital twin consists of multiple layers, each serving a critical function in ensuring accurate simulation, control, and monitoring of the distribution grid. The key components include:

- **Data Layer:** Responsible for collecting, storing, and processing grid data from SCADA systems and system operators.
- **Simulation Layer:** Runs real-time simulations to accurately model grid behaviour under various operational conditions.
- **Control and Decision-Making Layer:** Implements advanced algorithms to optimize grid congestion and voltage management in hardware in the loop environment.
- **Communication Layer:** Responsible for data exchange between the simulation layer and control layer.
- **Visualization Layer:** Provides monitoring dashboards (e.g., Grafana) for real-time data representation.
- **Resilience and Security Layer:** Analysis and evaluation of risk, system performance, cyber security, and mitigation measures.

A high-level diagram of the Cypriot digital twin architecture is shown in Figure 4-1. The Cypriot digital twin incorporates a representative section of the Medium-Voltage (MV) distribution network, which includes electrical loads, PV systems, and BESS models, built upon real-world field measurements. The digital twin is designed for execution on a Real-Time Simulator (RTS), enabling dynamic and interactive testing under realistic operating conditions.

To accurately represent the MV grid, all essential data components were collected. These include detailed grid topology, electrical parameters of system components, and operational data from actual field measurements. Power measurements from MV substations were obtained at 15-minute intervals through collaboration with the Cyprus Transmission System Operator (TSO) and the electricity authority of Cyprus (EAC). In addition, high-resolution data from PV power plants were acquired at resolutions of up to 30 seconds, enabling the representation of short-term PV variability within the digital twin environment.

As part of the digital twin's development, various operating scenarios are considered:

- **Cyber security Scenarios:** These simulate potential attacks such as false data injection, assessing their impact on grid stability and control systems.
- **Future Grid Scenarios:** These explore high renewable energy penetration and integration of flexibility services, aimed at evaluating system resilience and congestion management under future operating conditions.

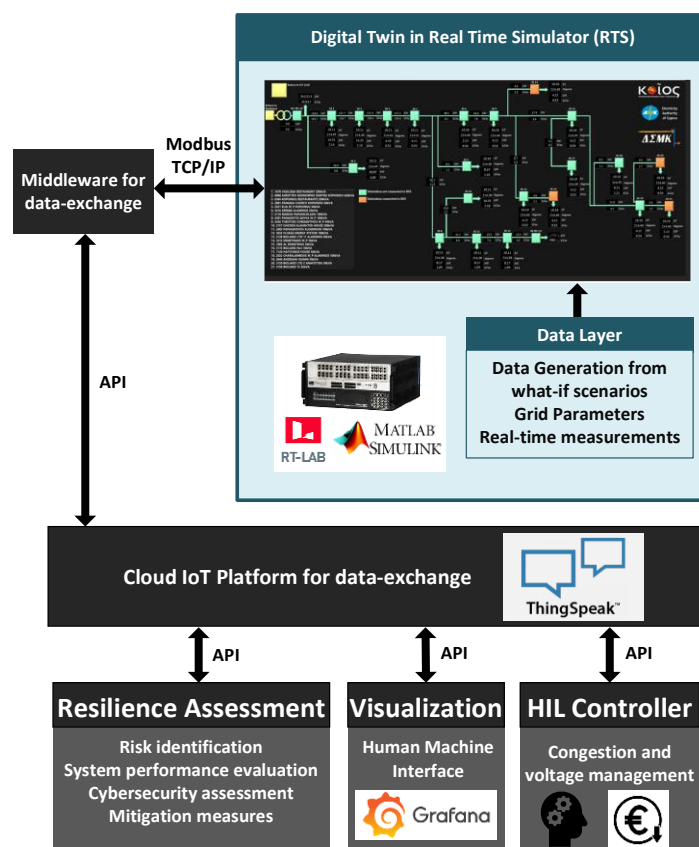


Figure 4-1: High level architecture of the Cypriot digital twin.

## 4.3 Development Roadmap

### 4.3.1 Implemented Functions

To realize an effective digital twin framework for congestion management and ancillary service provision, several functionalities were implemented across the layers of the digital twin architecture. These functions, which fall under the scope of Task 5.3, are outlined below:

**Development of the Digital Twin:** A digital twin of the Cypriot Medium-Voltage (MV) distribution grid was developed and deployed within a real-time simulation environment. To enable this, static data representing the actual MV network topology and parameters were collected and provided by the Cyprus Distribution System Operator (DSO), the electricity authority of Cyprus (EAC). This digital twin replicated the real grid's behaviour and served as a foundation for testing operational strategies and controller interactions in a risk-free, virtual environment.

**Development of Controllers for Ancillary Service Provision:** A key feature of this use case is the integration of controllers into the digital twin environment via a hardware-in-the-loop (HIL) configuration. These controllers were developed to manage congestion and mitigate voltage instability by controlling Distributed Energy Resources (DERs), specifically Battery Energy Storage Systems (BESS). The HIL controllers received real-time measurements from the digital twin and issued setpoints to the BESS to provide active and reactive power support, ensuring the stable and reliable operation of the distribution grid.

**Development of the Communication Layer:** A robust communication framework was established to enable seamless data exchange between the digital twin and its connected components, such as

controllers and visualization interfaces. In Task 5.3, a cloud-based platform was developed using ThingSpeak, which facilitated real-time data sharing. Middleware components (e.g., OneNet Connector) were employed to ensure interoperability between the digital twin simulation environment and the cloud infrastructure. This communication layer also served as a sandbox for implementing and testing cyberattack scenarios as part of the use case's cybersecurity assessment.

**Resilience and Reliability Assessment:** The resilience and operational reliability of the Cyprus distribution grid were assessed under a variety of operating conditions and cyberattack scenarios using defined Key Performance Indicators (KPIs). In particular, the impact of false data injection attacks simulating adversarial access to the communication layer was evaluated. Furthermore, the ability of the implemented controllers to manage grid congestion and ensure voltage stability under varying levels of Renewable Energy Source (RES) penetration was analysed, providing insights into their effectiveness in enhancing grid reliability and flexibility.

### 4.3.2 Software Platforms and Datasets Used for DT Development

To support the implementation of the demonstration plan, a variety of tools and datasets were utilized. Below is a brief description of the main resources that were used:

**Datasets:** The development of the digital twin requires both static and dynamic data.

- **Static data:** includes the topology and connectivity of the distribution network, parameters of three-phase distribution lines (resistance and reactance), HV/MV transformer specifications, and the loading limits of both lines and transformers. Additionally, the locations and rated capacities of Renewable Energy Sources (RES) and Battery Energy Storage Systems (BESS) within the grid are essential.
- **Dynamic data:** includes time-series profiles of active and reactive power for the three-phase dynamic models of the distribution grid, as well as generation profiles of RES units. Real-time measurements from the distribution grid were also obtained through simulation runs during the demonstration.
- **Real-Time Simulator (RTS):** The RTS is a high-performance software and hardware platform with substantial computational capabilities, designed for the real-time simulation of large-scale power systems. It was used to model the distribution grid as a digital twin, allowing for live data integration and dynamic system analysis.
- **ThingSpeak:** ThingSpeak is a cloud-based IoT platform that was used to collect, store, and process real-time data from connected components within the digital twin framework. It supports online data analysis and enables streamlined data exchange between simulation components and visualization interfaces.
- **Grafana:** Grafana is an open-source visualization tool used to create interactive dashboards for monitoring time-series data. In this use case, grafana was employed to display real-time operational metrics from the digital twin and the hardware-in-the-loop controllers, including grid status, controller actions, and flexibility activations.
- **Ettercap – Kali Linux Tool:** Ettercap was used to simulate Man-in-the-Middle (MiTM) cyber attacks within the controlled, sandboxed digital twin environment. This network security tool, part of the kali Linux suite, allows for the interception and manipulation of communication flows. It was used to test the system's response to malicious actions such as packet tampering, session hijacking, and false data injection.

### 4.3.3 Timeline and Milestones

A milestone related to Task 5.3 and the implementation of the congestion management use case and the cyber resilience assessment in the Cypriot distribution grid is provided in Figure 4-2.

| Task/Subtask                                                                | Start<br>Month | End<br>Month | Implementation Plan |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |
|-----------------------------------------------------------------------------|----------------|--------------|---------------------|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|
|                                                                             |                |              | Month               |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |
|                                                                             |                |              | 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 |  |
| T5.3: Scenarios for assessing the cyber and physical resilience of the grid | 9              | 33           |                     |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |
| T5.3.1: Definition of scenarios related to the operation of the grid        | 9              | 15           |                     |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |
| T5.3.2: Definition of scenarios related to the grid cybersecurity           | 12             | 18           |                     |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |
| T5.3.3: Development and integration of scenarios in digital twin systems    | 14             | 28           |                     |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |
| T5.3.4: Assessment of the scenarios impact to the power system operation    | 21             | 33           |                     |   |   |   |   |   |   |   |   |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |  |

*Figure 4-2: Timeline for implementation of congestion management use case.*

### 4.3.4 Demonstration Plan

The demonstration plan for this use case includes several phase as outlined below:

## 4.4 Developed Framework and Results Demonstration

The implementation of the congestion management use case under Task 5.3 was successfully completed across all four planned phases, resulting in a fully operational digital twin of a representative section of the Cypriot Medium-Voltage (MV) distribution network. This chapter showcases the development results for each phase outlined above.

### 4.4.1 Phase 1-Setup the Digital Twin

Phase 1 focused on the establishment of the core infrastructure required for the implementation of the congestion management use case, namely the development of a high-fidelity digital twin of a representative section of the Cypriot Medium-Voltage (MV) distribution network. This phase constitutes a critical foundation for all subsequent activities, as it enables the safe, repeatable, and realistic simulation of grid behaviour under a wide range of operational and contingency scenarios.

The primary objective of this phase was to construct a digital environment capable of accurately replicating the physical and operational characteristics of the distribution grid. To achieve this, significant effort was dedicated to the acquisition, validation, and preprocessing of both static and dynamic datasets, in close collaboration with the Cyprus distribution system operator (EAC) and the TSO. Static datasets included detailed information on network topology, such as feeder configurations and node connectivity, as well as electrical parameters of grid components. These parameters encompassed line resistance and reactance values for three-phase distribution lines, transformer ratings and impedance characteristics, and operational limits, including thermal ratings of lines and transformers.

In addition to the core network description, particular emphasis was placed on the accurate representation of DERs integrated within the grid. This included the identification of PV installation locations, their rated capacities, and their connection points within the MV network. Similarly, the placement and sizing of BESS, which play a central role in the congestion management use case, were incorporated into the network model. This comprehensive representation of DERs ensures that the

digital twin captures the increasing complexity and bidirectional power flows that characterize modern distribution systems.

Complementing the static data, dynamic datasets were collected to reflect real operational conditions. These included time-series measurements of active and reactive power at MV substations, obtained at 15-minute intervals, which provided insights into load demand patterns and overall grid behaviour. In addition, high-resolution PV generation measurements with a temporal resolution of up to 30 seconds were collected to capture the short-term variability and intermittency of solar energy production. Depending on the application, the available datasets were synchronized and resampled to ensure consistency between the different components of the digital twin environment.

Following data acquisition, a comprehensive data validation and preprocessing process was undertaken. This involved consistency checks, gap filling, synchronization of datasets with different temporal resolutions, and normalization where required. Such preprocessing ensured the reliability of the input data and minimized the propagation of errors into the simulation environment.

The validated datasets were subsequently used to develop a detailed three-phase electrical model of the MV distribution network within a Real-Time Simulator (RTS) platform as shown in Figure 4-1. The choice of a real-time simulation environment was instrumental in enabling dynamic and interactive execution of the digital twin, allowing it to respond to inputs and disturbances in a manner consistent with real-world grid operation. The model includes all essential grid components, feeders, loads, transformers, PV units, and BES, while explicitly incorporating operational constraints such as voltage limits, transformer tap settings, and line thermal capacities.

A key aspect of the modelling process was the accurate representation of high PV penetration scenarios, which are characteristic of the Cypriot context. The digital twin was configured to reproduce phenomena such as reverse power flows, voltage rise issues, and congestion in specific feeders due to clustered DER installations. This capability enables the simulation of stressed operating conditions and provides a realistic testbed for evaluating congestion management strategies in later phases.

In addition to the physical modelling of the grid, the digital twin was structured in alignment with the overall architecture described in Chapter 4.2, ensuring compatibility with the subsequent integration of control, communication, and visualization layers. Interfaces were prepared to allow seamless interaction between the simulation layer and external modules, including HIL controllers and cloud-based data platforms. This modularity ensures that the digital twin can evolve progressively throughout the demonstration phases without requiring structural redesign.

To verify the correctness and robustness of the developed model, a series of validation and benchmarking tests was conducted. These tests compared simulation outputs with expected operational behaviour under typical and extreme conditions. Scenarios included variations in load demand, peak PV generation periods, and stress conditions leading to voltage deviations and potential congestion. The results confirmed that the digital twin provides a reliable representation of the real system, accurately reproducing key indicators such as voltage profiles, power flows, and loading levels across the network.

Furthermore, initial exploratory simulations were performed to identify baseline congestion patterns and voltage challenges within the modelled network. These preliminary analyses provided valuable insights into critical nodes and feeders that are more susceptible to operational constraints, thereby guiding the design and testing of control strategies in Phase 2.

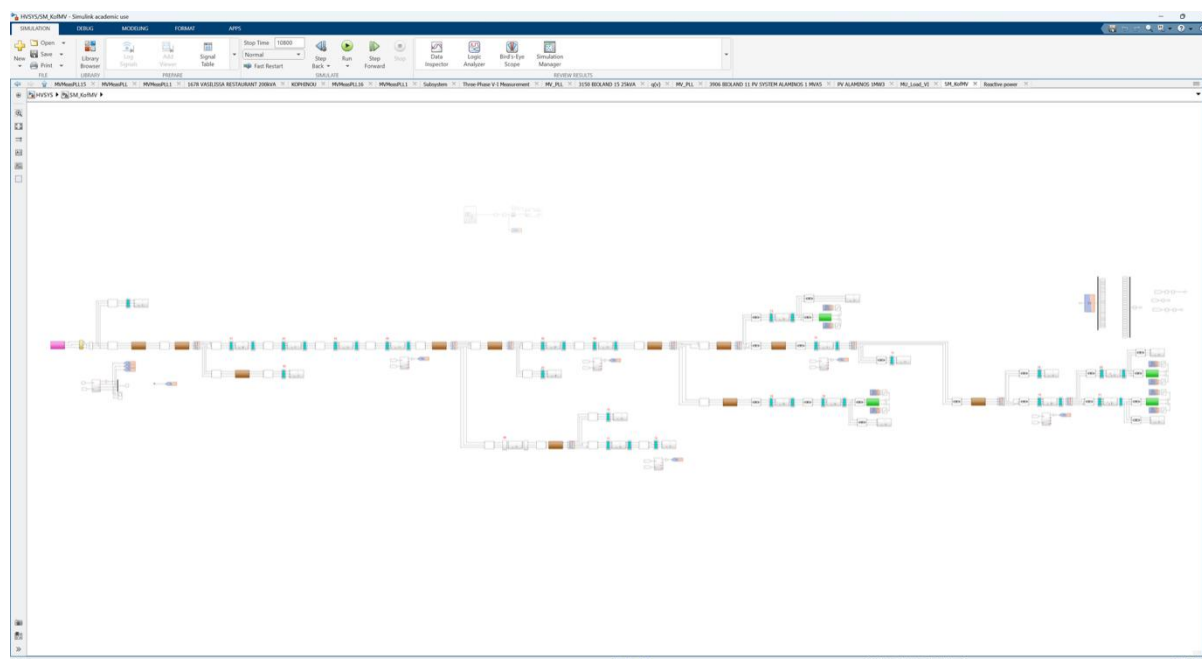


**Figure 4-3: A feeder developed in Simulink for the Cypriot distribution grid digital twin.**

In summary, Phase 1 successfully delivered a robust, validated, and high-resolution digital twin of the Cypriot MV distribution grid, capable of real-time execution and detailed system analysis. The digital twin serves as the cornerstone of the use case, providing a safe and flexible environment for testing advanced control strategies, evaluating DER flexibility, and assessing system resilience under both normal and adverse conditions. The outcomes of this phase ensure that subsequent development steps can be conducted with a high degree of confidence in the accuracy and reliability of the simulation framework.

#### **4.4.2 Phase 2-Development and Integration of Controllers and Coordination of Flexibility**

Phase 2 focused on the development, implementation, and validation of advanced control strategies for the coordinated utilization of distributed flexibility, with the primary objective of mitigating congestion and maintaining voltage stability in the MV distribution grid. This phase builds directly upon the digital twin established in Phase 1 and introduces a real-time control layer capable of actively managing BESS through a HIL configuration.

The core outcome of this phase is the design and deployment of a centralized coordination controller that determines optimal active and reactive power set-points for multiple BESS units connected across the distribution network. The controller is formulated as a Mixed-Integer Linear Programming (MILP) optimization problem for the coordinated dispatch of active and reactive power from multiple BESS units. The objective is to minimize flexibility activation costs while maintaining substation loading and bus voltages within their operational limits. The controller operates within a Hardware-in-the-Loop (HIL) framework and receives real-time measurements from the digital twin. Detailed mathematical formulation, BESS ratings, operational constraints, solver configuration, and quantitative performance assessment are presented in Deliverable D5.2 [18], where the congestion-management use case is evaluated under representative operating conditions.

The controller operates by receiving real-time measurements from the digital twin, including voltage magnitudes at selected buses, active and reactive power flows at the substation, and the operational status of individual BESS units. Based on these inputs, it computes optimal control actions

at regular time intervals, aiming to maintain the apparent power at the HV/MV substation within predefined thermal limits while ensuring that nodal voltages remain within acceptable ranges defined by grid codes. Unlike conventional local or droop-based control approaches, which operate reactively and independently, the proposed controller adopts a system-wide perspective, enabling coordinated decision-making across multiple assets.

A key innovation of the developed control framework lies in its ability to simultaneously address congestion management and voltage regulation problems within a single optimization process. This is achieved by incorporating both substation loading constraints and nodal voltage limits into the decision-making logic, ensuring that control actions contribute to overall system security. The formulation also allows for prioritization between conflicting objectives, for instance, giving precedence to congestion mitigation when simultaneous satisfaction of all constraints is not feasible, thus reflecting realistic operational practices adopted by DSOs.

To ensure computational tractability and real-time applicability, the controller relies on linearized representations of network behaviour. In particular, the relationship between BESS power injections and voltage variations across the network is captured using sensitivity coefficients derived offline from the digital twin model. This approach enables the controller to estimate the system response to control actions without the need for computationally intensive power flow calculations during each control cycle. Additionally, nonlinear constraints related to substation loading are approximated using linear representations, striking a balance between modelling accuracy and computational efficiency, which is essential for real-time deployment.

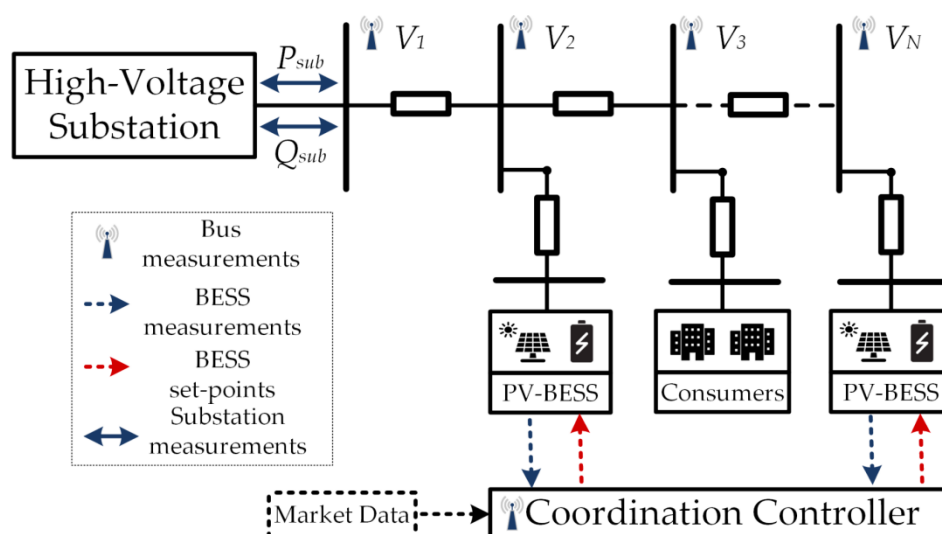


**Figure 4-4: High level controller integration architecture.**

The operational workflow of the controller is executed in discrete time intervals, reflecting realistic communication and processing constraints. At each control step, the controller collects updated system measurements, reconstructs the current operating state, and solves the optimization problem to determine the optimal set-points for each BESS. These set-points include both active and reactive power commands, allowing the BESS units to provide multiple ancillary services simultaneously. The computed control actions are then transmitted back to the digital twin environment, where their impact on the system is evaluated dynamically. The integration of the controller within a hardware-in-the-loop (HIL) framework represents a critical achievement of this phase. The digital twin, running on a real-time simulator, interacts with the external controller through a communication interface that emulates real-world conditions, including data exchange delays and communication protocols.

This setup enables realistic validation of the control strategy, ensuring that its performance is not only theoretically sound but also practically implementable within existing grid infrastructure. The overall architecture of the controller integration is illustrated in Figure 4-4.

Furthermore, the experimental setup includes a cloud-based data exchange platform and middleware services, facilitating the seamless transfer of measurements and control signals between the simulation environment and the optimization engine. This architecture reflects modern digitalized grid operation frameworks, where distributed components interact through interoperable communication layers.

In summary, Phase 2 successfully delivered an advanced, optimization-based control framework for coordinated flexibility management in distribution grids. The integration of this controller within the digital twin environment enables proactive and system-wide congestion management, significantly enhancing the operational capabilities of the DSO.

#### **4.4.3 Phase 3-Development of the Communication Layer**

Phase 3 focused on the design, implementation, and validation of the communication infrastructure that enables seamless data exchange between the different components of the digital twin ecosystem. This phase is a critical enabler for real-time operation, as it ensures interoperability between the simulation environment, the optimization-based controllers developed in Phase 2, and the visualization and monitoring tools used for system supervision.

The primary objective of this phase was to establish a robust, scalable, and flexible communication layer capable of supporting bidirectional data flows under realistic operational conditions. In contrast to traditional power system simulations, where all components operate within a single environment, the digital twin developed in this project relies on a distributed architecture. This architecture requires the integration of heterogeneous components, including real-time simulators, external controllers, cloud platforms, and visualization dashboards, each operating on different platforms and communication protocols. Therefore, ensuring reliable and synchronized communication between these components was essential for the overall functionality of the use case.

At the core of the communication layer is a cloud-based data exchange platform built using ThinkSpeak, shown in Figure 4-5 . This platform serves as an intermediary hub for data aggregation, storage, and processing, enabling the decoupling of system components and facilitating modular system design. The digital twin transmits real-time measurements, such as voltage levels, power flows, and BESS operating states, to the cloud platform, where they are made available to the coordination controller. In turn, the controller processes this data and sends back optimized control set-points, which are then forwarded to the digital twin for execution. This bidirectional data flow enables closed-loop control of the system in real time.

A key achievement of this phase was the successful validation of real-time data exchange between all system components. Extensive tests were conducted to verify the correct transmission, reception, and synchronization of data across the communication chain. These tests confirmed that measurements generated by the digital twin could be reliably transmitted to the cloud platform, processed by the controller, and returned as control signals within the required time constraints. The communication cycle was aligned with the controller execution interval, ensuring that fresh data is available for each optimization step.

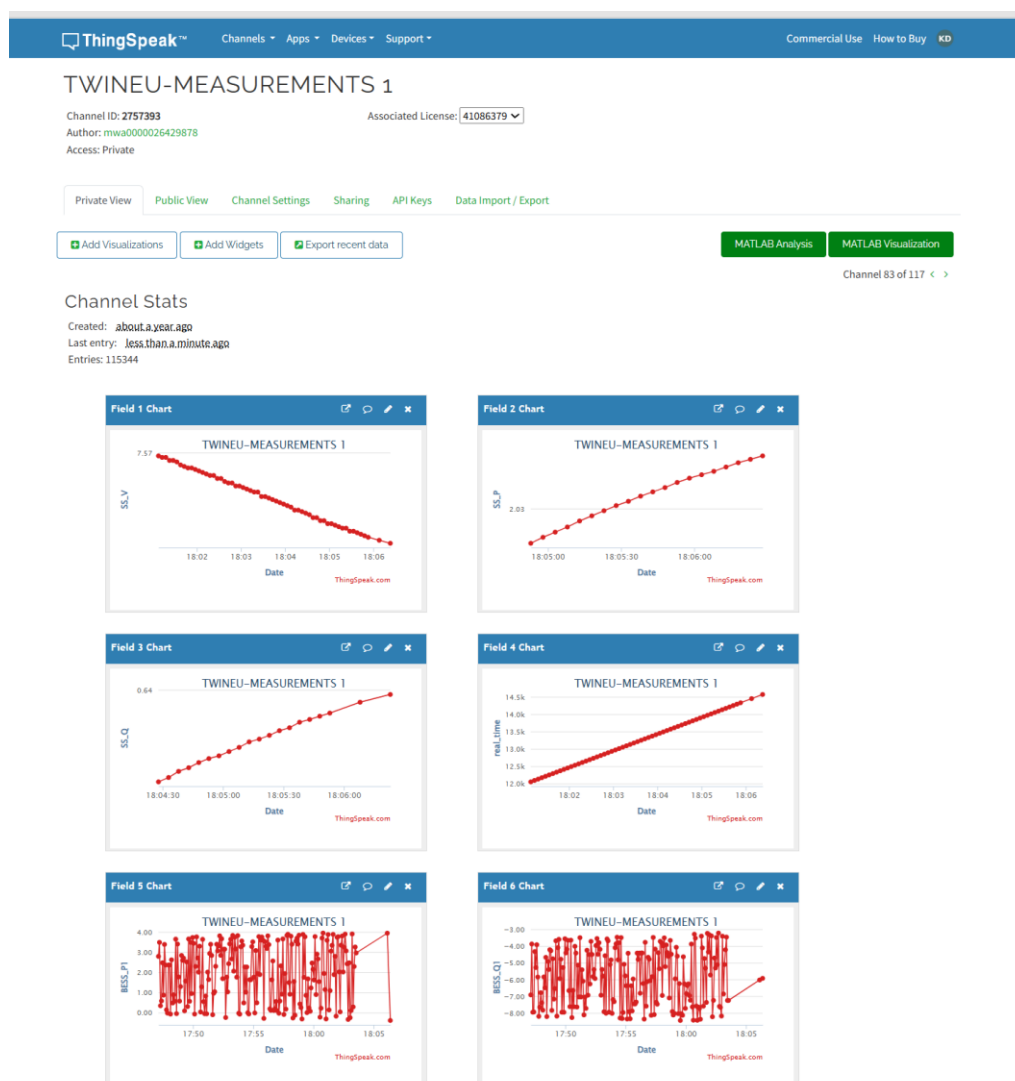


**Figure 4-5: ThinkSpeak interface.**

In addition to enabling controller integration, the communication layer also supports advanced monitoring and visualization functionalities. A dedicated dashboard was developed using Grafana as shown in Figure 4-6, providing real-time insights into system operation. The dashboard displays key performance indicators such as substation loading, bus voltage profiles, and BESS dispatch levels, allowing operators and researchers to track system behaviour and controller actions dynamically. This visualization capability enhances situational awareness and facilitates the interpretation of simulation results during the demonstration.

Another important aspect of the communication layer is its role in supporting cyber security analysis, which is further explored in Phase 4. By establishing a realistic and accessible communication infrastructure, this phase provides the necessary foundation for introducing and evaluating cyber attack scenarios, such as false data injection and man-in-the-middle attacks. The use of a cloud-based platform and middleware components enables controlled manipulation of data flows, making it possible to assess system vulnerabilities and resilience without affecting real grid operations.

In summary, Phase 3 successfully delivered a fully functional and validated communication infrastructure that connects all layers of the digital twin ecosystem. The developed communication layer enables real-time interaction between simulation, control, and visualization components,

supporting the implementation of advanced congestion management strategies. Furthermore, it establishes a realistic operational environment that is essential for testing system resilience and cyber security in subsequent phases.

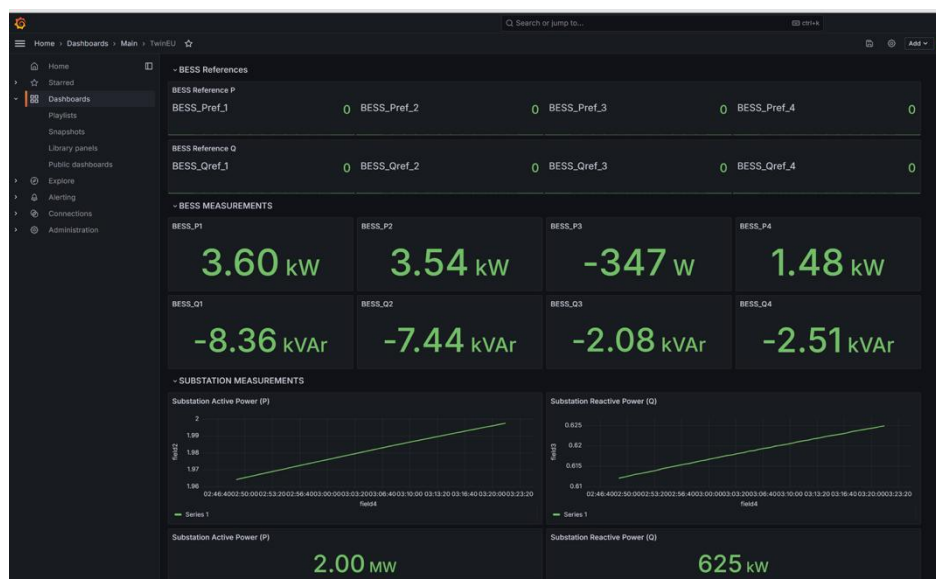


Figure 4-6: Grafana interface for monitoring and visualization.

#### 4.4.4 Phase 4-Digital Twin Validation

Phase 4 focuses on the validation of the developed digital twin framework through the execution of representative operational and cyber security scenarios. Building upon the infrastructure and functionalities developed in Phases 1–3, this phase evaluates the performance of the system under both normal and adverse conditions. The objective is twofold: (i) to assess the effectiveness of the proposed control strategy in mitigating congestion and maintaining voltage stability, and (ii) to analyse the impact of cyber attacks on system operation and resilience.

##### 4.4.4.1 Congestion Management Scenario

The first validation scenario examines the performance of the system under normal operating conditions, with high photovoltaic (PV) penetration and no cyber disruptions. The analysis considers a 24-hour simulation horizon, capturing variations in load demand and renewable generation, including periods of peak PV output that typically induce reverse power flows and network congestion.

Figure 4-7 clearly demonstrate the effectiveness of the proposed MILP-based coordination controller in managing congestion and maintaining voltage levels within acceptable limits. The upper subplot shows the apparent power at the HV/MV substation before and after the activation of the controller. In the baseline case, the substation loading exceeds the predefined thermal limit (2 MVA) during multiple time intervals, particularly during midday hours when PV generation is at its peak. These violations indicate significant congestion that would typically require costly grid reinforcement or curtailment measures. Following the activation of the controller, the substation loading is successfully maintained at or below the operational limit throughout the entire simulation period. This demonstrates the capability of the coordinated BESS dispatch to dynamically absorb or inject power as needed, effectively mitigating congestion in real time.

The voltage profiles, illustrated in the second subplot, further confirm the effectiveness of the control strategy. Without coordinated control, voltage levels at critical buses approach or exceed the

upper permissible limit (1.05 p.u.) during peak PV generation. With the controller in operation, all monitored voltages remain within the acceptable range, indicating successful voltage regulation across the network.

The lower subplots provide insight into the operational behaviour of the BESS units. During congestion periods, particularly around midday, multiple BESS units are activated simultaneously. Active power absorption is the dominant mechanism for reducing reverse power flow and relieving substation loading, while reactive power support is used to regulate voltage levels at sensitive buses. The coordinated use of both active and reactive power highlights the flexibility and effectiveness of the centralized optimization framework.

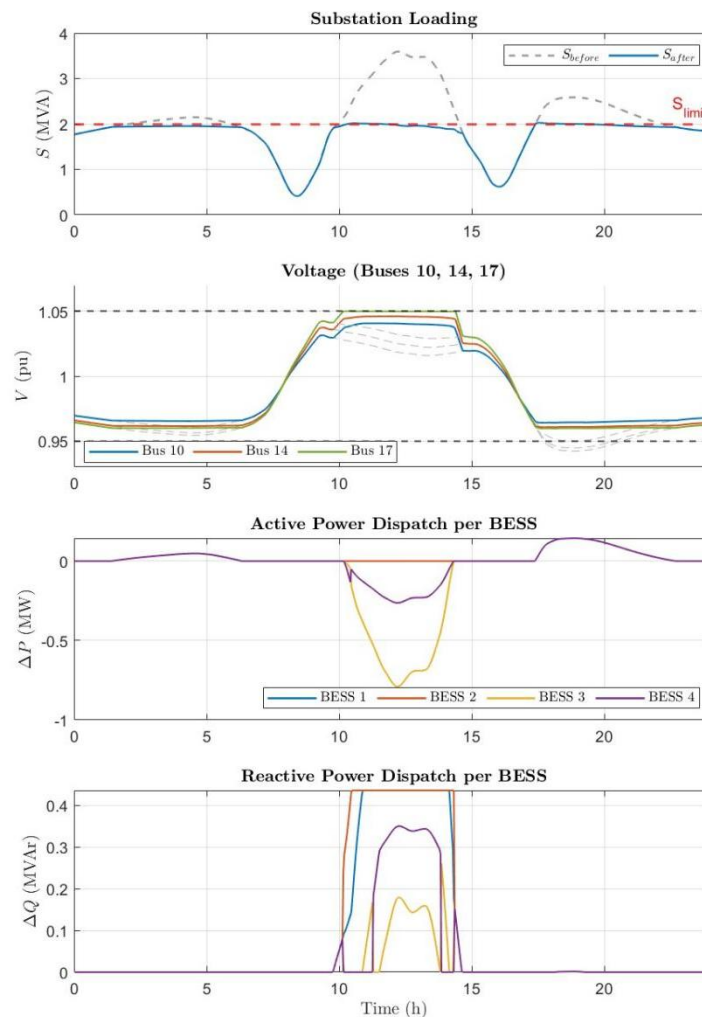


**Figure 4-7: Validation results under normal operating conditions.**

The objective of the validation phase presented in this deliverable is to demonstrate the successful integration and operation of the digital twin architecture, communication infrastructure and controller framework. Detailed quantitative assessment of congestion magnitude, voltage violations, BESS utilization, communication performance and cyber-attack impacts is provided in Deliverable D5.2 [18], which focuses on the evaluation of operational and cyber-resilience performance under representative scenarios.

#### 4.4.4.2 Cyber Attack Scenario

The second scenario evaluates the impact of cyber attacks on the performance of the system, focusing on the integrity of the communication layer and its influence on control decisions. In this case, a False Data Injection (FDI) attack is introduced by manipulating measurements from the substation that are transmitted to the controller (as shown in the upper subplot of Figure 4-8).

The results in Figure 4-8 reveal a clear degradation in system performance under attack conditions. The upper subplot compares the baseline, real, and attacked substation loading profiles. While the controller under normal conditions successfully maintains the loading within limits, the presence of corrupted measurements leads to inaccurate control actions. As a result, the substation loading may temporarily exceed the operational threshold or fail to optimally utilize available flexibility.

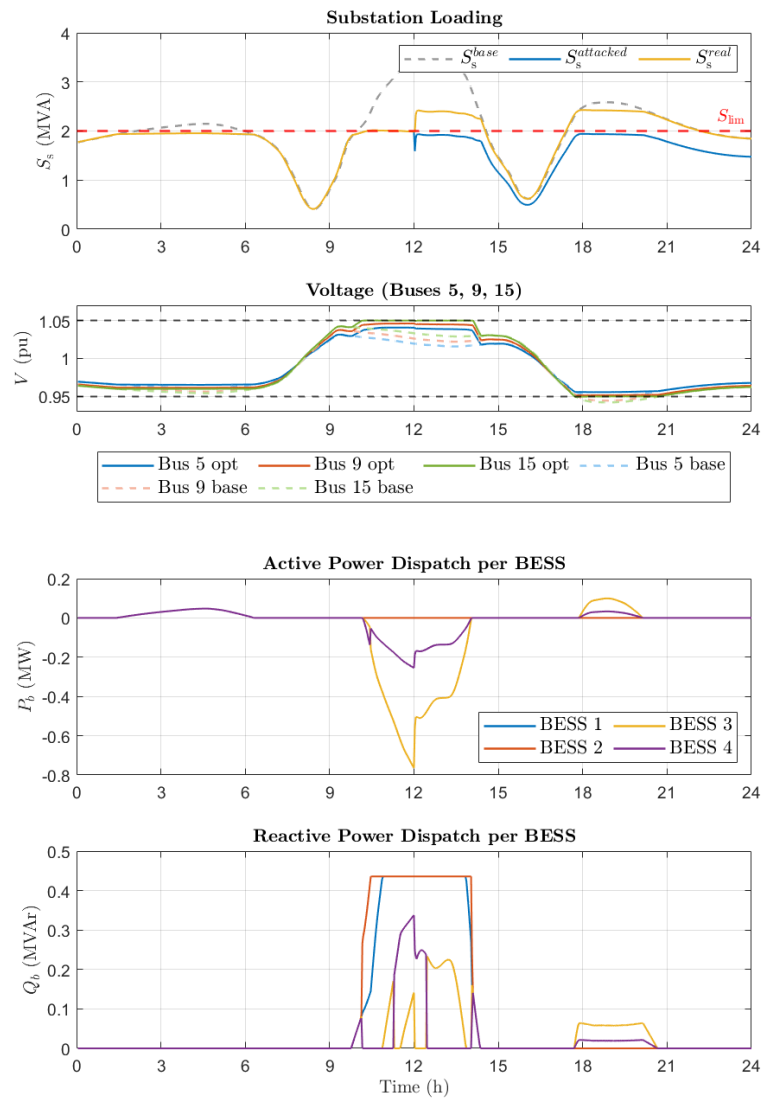


**Figure 4-8: Cyber attack impact on the distribution grid operation.**

The voltage profiles similarly show the impact of the attack, with slight deviations observed compared to the controlled case. Although the system does not exhibit catastrophic failure, the degradation in voltage regulation performance highlights the sensitivity of the control framework to measurement integrity.

The BESS dispatch patterns further illustrate the consequences of the attack. Under manipulated inputs, the controller activates BESS units in a suboptimal manner, either underutilizing available resources or dispatching power in directions that do not fully address the underlying grid constraints. This behaviour underscores the importance of accurate and reliable data for optimization-based control strategies.

The cyber-security validation focuses on representative false-data injection attacks targeting measurements and control signals exchanged through the communication layer. These attacks include manipulation of substation loading measurements, voltage measurements at critical buses, and BESS control signals. The objective is to assess the sensitivity of the optimization-based controller to corrupted information and to identify potential vulnerabilities within the digital twin ecosystem. A detailed quantitative evaluation of individual attack cases is provided in Deliverable D5.2 [18].

Overall, Phase 4 successfully demonstrates the capability of the developed digital twin framework to support realistic, end-to-end validation of advanced grid management strategies. The results confirm that optimization-based coordination of BESS can significantly improve distribution network performance while also revealing potential vulnerabilities introduced by increased digitalization. The insights gained from this phase provide a strong basis for future work on integrating resilience and cyber security measures into smart grid control architectures.

## 4.5 Alignment with Digital Twin Concepts

The digital twin developed under Task 5.3 is fully aligned with the core principles and architectural concepts that define a digital twin in the context of modern energy systems. Broadly, a digital twin is understood as a virtual representation of a physical system that is continuously updated with real-world data, capable of simulating system behaviour, supporting decision-making, and enabling the testing of operational strategies in a risk-free environment. The Cypriot digital twin embodies all of these characteristics within a distribution grid context.

A fundamental requirement of any digital twin is real-time fidelity, namely the ability to accurately mirror the behaviour of its physical counterpart. In the Cypriot pilot, the physical counterpart is a representative section of the Cyprus Medium-Voltage (MV) distribution network operated by EAC, while the digital twin itself is implemented as a real-time simulation model running on a Real-Time Simulator (RTS). The digital twin is parameterized using actual network topology, equipment characteristics, and operational measurements obtained from EAC and the Cyprus TSO. These measurements include substation power measurements at 15-minute intervals and photovoltaic generation measurements at up to 30-second intervals, ensuring that the simulated environment reflects realistic network operating conditions.

To clarify the experimental configuration, the operational distribution network is not directly controlled by the digital twin. Instead, the physical grid provides the network model, parameters, and measurement datasets used to develop and validate the digital representation. The MV feeders, loads, photovoltaic units, and Battery Energy Storage Systems (BESS) are simulated within the RTS environment, which acts as the real-time executable representation of the physical counterpart. This approach enables the execution of operational and cyber-security experiments without introducing risks to active grid infrastructure.

Beyond passive monitoring, a true digital twin supports bidirectional interaction between the virtual and physical domains. In this use case, this principle is realised through the hardware-in-the-loop configuration, in which HIL controllers receive live measurements from the digital twin and issue

control setpoints back to the simulated BESS units. This closed-loop interaction demonstrates that the digital twin is not merely an observational tool but an active component in the operational and control chain.

The Hardware-in-the-Loop (HIL) controllers constitute the physical hardware components of the demonstration platform. During operation, the controllers receive real-time measurements generated by the RTS through the communication layer and calculate active and reactive power setpoints for congestion management and voltage regulation. The resulting control commands are applied to the simulated BESS assets within the RTS environment rather than to field-deployed devices. This allows realistic validation of control functions while maintaining complete separation from the operational grid.

The layered architecture of the Cypriot digital twin, spanning the Data, Simulation, Control, Communication, Visualization, and Resilience layers, is consistent with the modular and hierarchical design principles advocated in digital twin frameworks for cyber-physical systems. Each layer fulfils a distinct and well-defined function, while the layers collectively enable an integrated and coherent system capable of supporting multiple use cases simultaneously, from congestion management to cyber security assessment.

Synchronization across the digital twin ecosystem is achieved through the communication layer, which integrates the RTS, HIL controllers, ThingSpeak cloud services, and Grafana monitoring dashboards. Real-time measurements and control signals are exchanged continuously throughout the simulation process, ensuring consistent operation of all components on a common simulation timeline. This synchronization mechanism enables realistic testing of operational strategies, controller performance, and cyber-security scenarios under conditions representative of actual distribution-grid operation.

Finally, the incorporation of cyber attack simulation within the digital twin environment reflects an increasingly recognized dimension of digital twin applications: cyber-physical resilience. By enabling the evaluation of adversarial scenarios, such as false data injection and man-in-the-middle attacks without any risk to the actual infrastructure, the digital twin provides a critical platform for security testing and the development of robust countermeasures. This capability positions the Cypriot digital twin as a comprehensive tool not only for operational optimization, but also for the long-term security and reliability of digitalized distribution grid management.

## **5 T5.4 Overview on Abnormal Market Participation Detection and Protocol Activation**

### **5.1 Challenges Addressed by the Task**

The DTs already deployed by the Market Operator (MO) (OMIE) and the System Operators (SOs) in the Iberian peninsula will collaborate to identify abnormal market participation, propagating the threat detection to all stakeholders and implementing the necessary countermeasures to secure the normal operation of the market.

This workstream will be implemented through the demonstration of the BUC Ib04 for the specific case of local flexibility markets in the distribution level. The inclusion of a high number of small independent DER operators as flexibility service providers directly participating in energy markets poses additional cyber risks with an exponentially increased number of potential vulnerabilities in the electricity system.

Additionally, based on a secure integration framework for wholesale and local markets (energy/balancing/flexibility), the Iberian pilot will make use of the federated DT to simulate the multi-systems integration framework (TSO-DSO-MO-Prosumer). The final aim is to improve the integration framework (and/or draw recommendations for deployment) according to the results, exploiting coordinated grid qualification in operational planning or near real-time contingency analysis.

### **5.2 Architecture of Digital Twins and Description**

#### **5.2.1 ANELL's Distribution Grid DT and OMIE's LFM DT (Implementation of BUC Ib04)**

The use case implementation depends on the established collaboration between the DSO DT and the LFM DT. The implementation was carried out according to the reference collaboration framework designed in WPs 3 and 4.

ANELL's distribution grid DT is based on ETRA's Advanced Distribution Management System (ADMS) – ÉTER –. ÉTER targets Distribution System Operators (DSOs), aiming at facilitating the monitoring, control and planning activities of modern distribution grids efficiently. The platform is equipped with a Digital Twin module provided with the advanced simulation profiling capabilities. Apart from the DT service, ÉTER offers, for both systems general operation and support to the Use Cases implementation, a series of services dedicated to enhance the value that this ADMS offers., Namely, (1) Geographic Information System (GIS), (2) a topology processor, (3) intelligent alarm processing, (4) on-line power flow calculation, (5) short-circuit analysis, (6) state estimation, (7) fault location, isolation, and service restoration, (8) Volt/VAR optimization, (9) optimal network reconfiguration, (10) switch order management, (11) emergency load shedding, and (12) short-term load forecasting. Figure 5-1 depicts the main components and services of ÉTER.

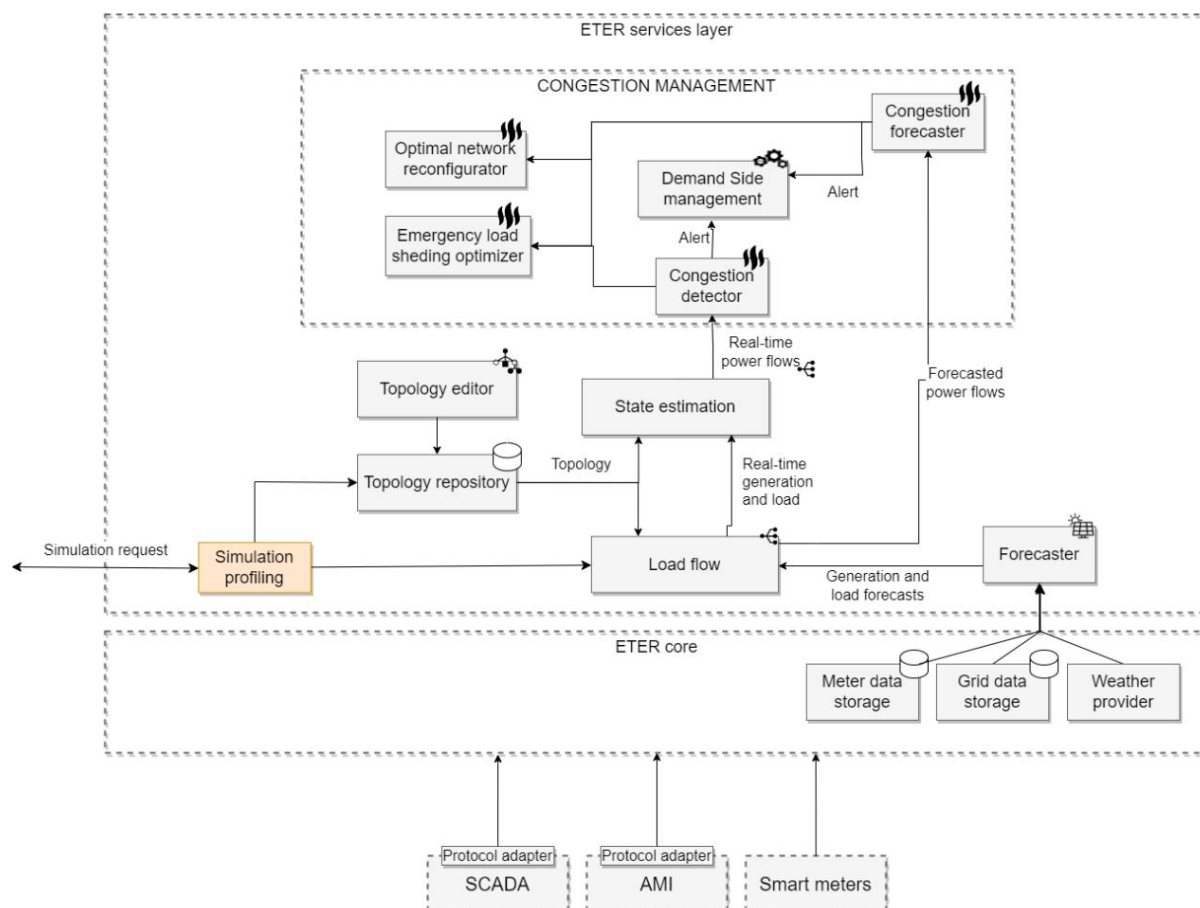


**Figure 5-1: ÉTER architecture.**

OMIE's LFM DT involves the modelling of two market platforms for procuring local flexibility markets. One for local short-term negotiations (with the same technology as the LTS system to provide grouping functionalities in the same market tool) and a second one for long-term flexibility negotiations. For this second one, a new market platform has been developed seeking the objective of achieving a more attractive and user-friendly tool focused on new roles such as aggregators, DSOs or active consumers with renewable energy resources that have manageable capacity. This long-term flexibility platform has been designed to cover all the processes related to local flexibility procurement to demonstrate this type of negotiation.

This market platform and its DT is based on a web application where users, both flexibility-providing market participants and DSOs, can register themselves using a username and password. Once registered, users will be able to participate in long-term flexibility auctions through the GUI to integrate their energy flexibility into the markets. Figure 5-2 represents OMIE's DTs, including the aforementioned DTs – applicable to LFM – as well as the DT of the wholesale electricity markets in the Iberian system.

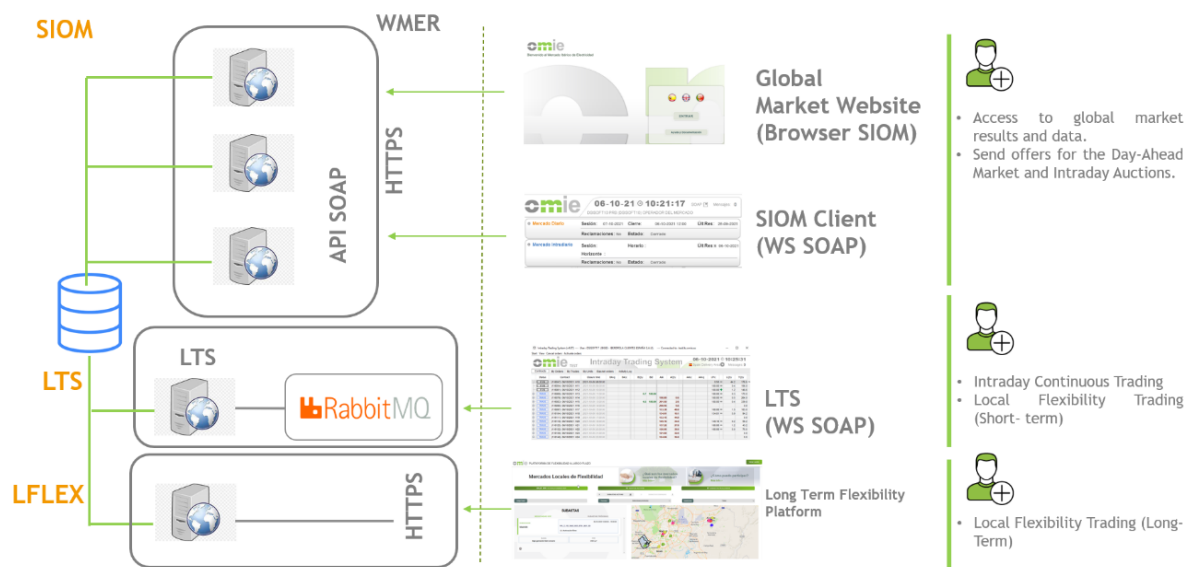


**Figure 5-2: OMIE's market operator information system (SIOM) architecture.**

The architecture for the integration of both DTs in accordance with the reference architecture of the TwinEU framework has been defined using the SGAM methodology. The result is a three-layer representation of the component (see Figure 5-3), the communication models (see Figure 5-4) and the information exchanged (see Figure 5-5). These are:

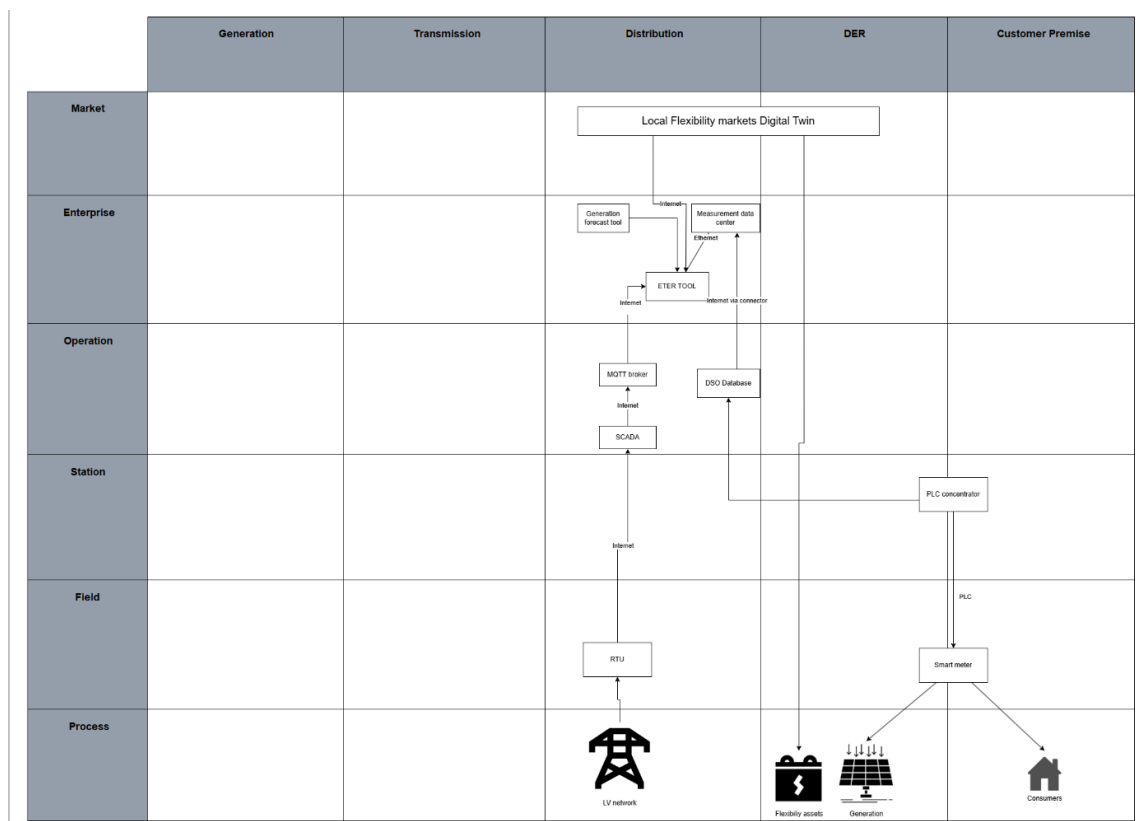


**Figure 5-3: SGAM component layer.**

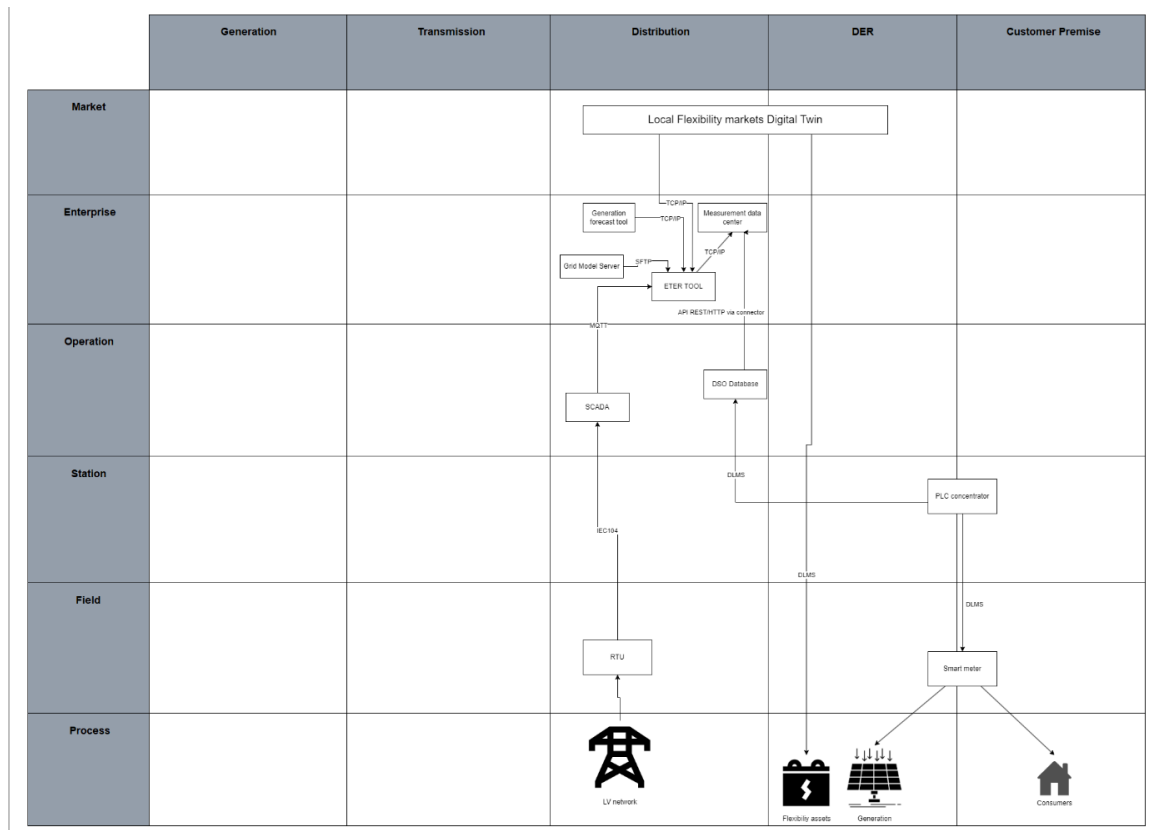


**Figure 5-4: SGAM Communication layer.**

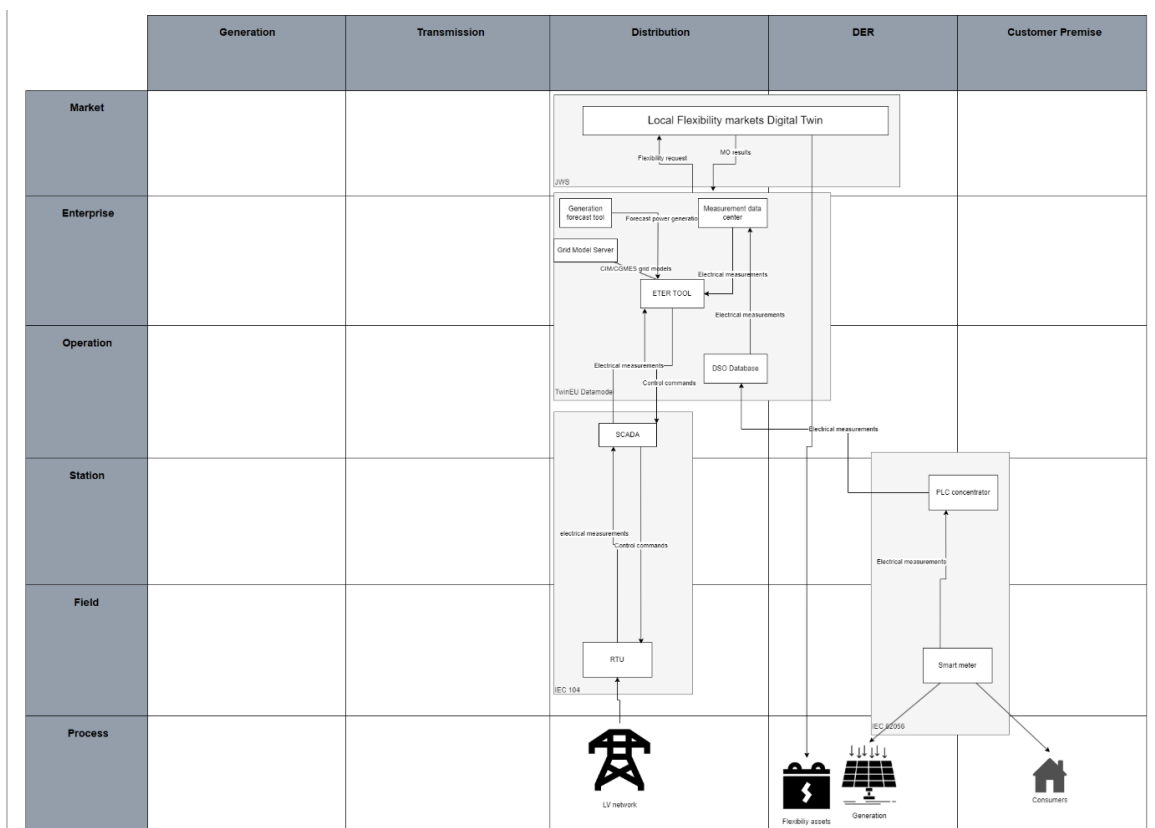


**Figure 5-5: SGAM information layer.**

## 5.2.2 REN's Transmission Grid DT and Portuguese Distribution Grid DT model (UC Ib12)

The execution of UC Ib12 relies on the implementation of REN's Transmission Grid DT. The DT of REN's Transmission Grid encompasses several key features and capabilities to effectively model, simulate, and optimize the operation of the Portuguese transmission grid and interface with the internal DSO digital model. The DT can be divided into 2 different frameworks: one stationary and another dynamic.

The stationary DT transmission grid model details comprehensively a representation of the entire Portuguese transmission network, including substations, transformers, transmission lines, and other grid components. It accurately captures the physical and operational characteristics of each asset regarding steady-state. The DT involved in the Pilot Site Ecosystem supports scenario analysis capabilities, allowing grid operators to simulate and evaluate different operating scenarios, such as changes in demand, renewable energy integration, or network contingencies. This helps in assessing the impact of various factors on grid stability and reliability. Regarding the dynamic DT, the main objective is to connect a model that represents in a reliable way the distribution grid behaviour to disturbances seen from the TSO perspective. The role that distributed generation units connected to these parts of the network have in the overall system performance must be taken into account with respect to different phenomena and planning/operation strategies, once it may represent an important percentage of the total generated power in a given region.

The DTs coordination will include the implementation of protocols and data exchange mechanisms, enabling the simulation of the integrated market coordination for the resolution of technical constraints using the federation of Digital Twins. This will conclude with a risk assessment and the security monitoring systems will be implemented to ensure a security-wise coordination between TSOs, DSOs, MOs, and prosumers.

The architecture for the integration of the UC ecosystem through the reference architecture of the TwinEU framework has been defined using the SGAM methodology. The result is a three-layer representation of the component (see Figure 5-6), the communication models (see Figure 5-7) and the information exchanged (see Figure 5-8). These are:

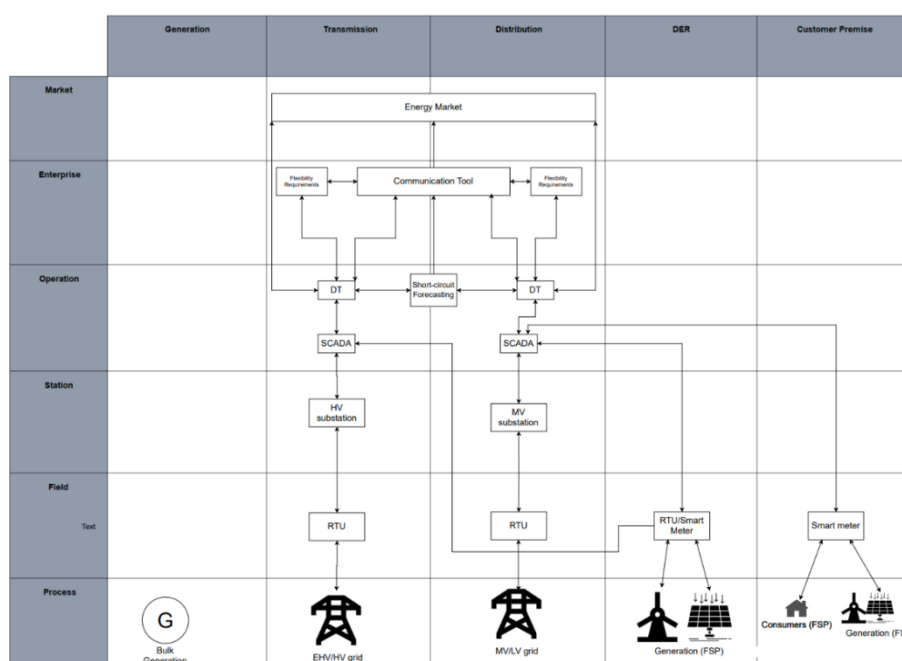


**Figure 5-6: UC Ib12 component layer.**

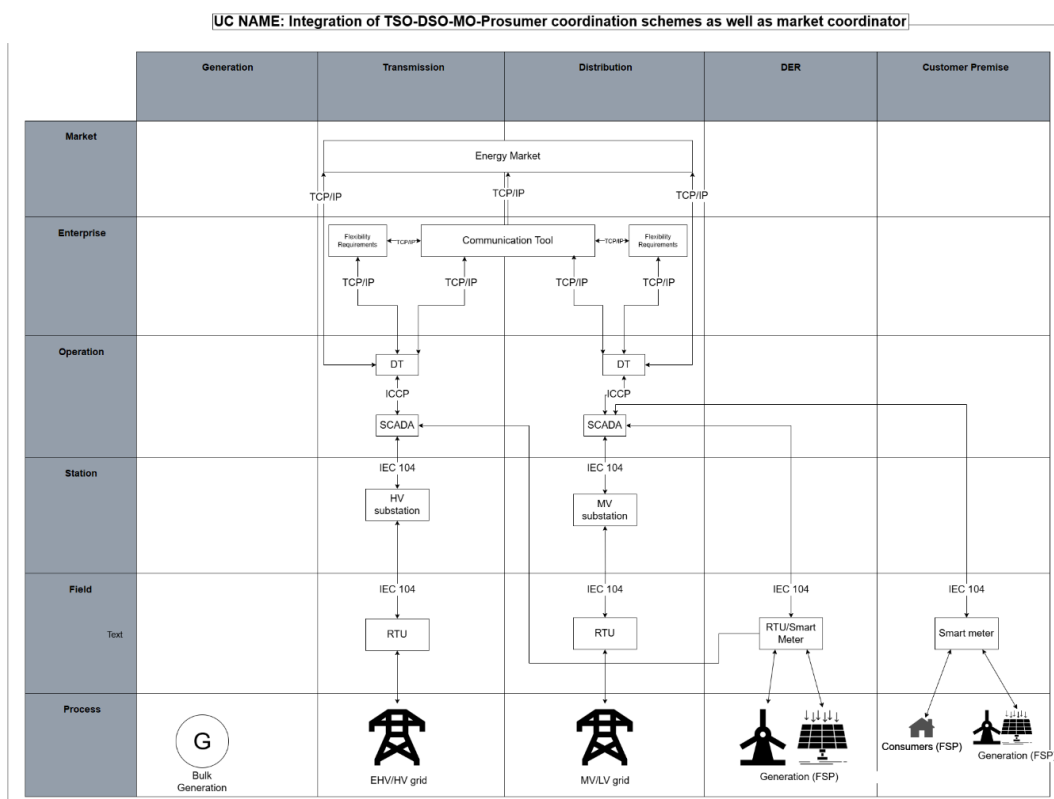


**Figure 5-7: UC Ib12 communication layer.**

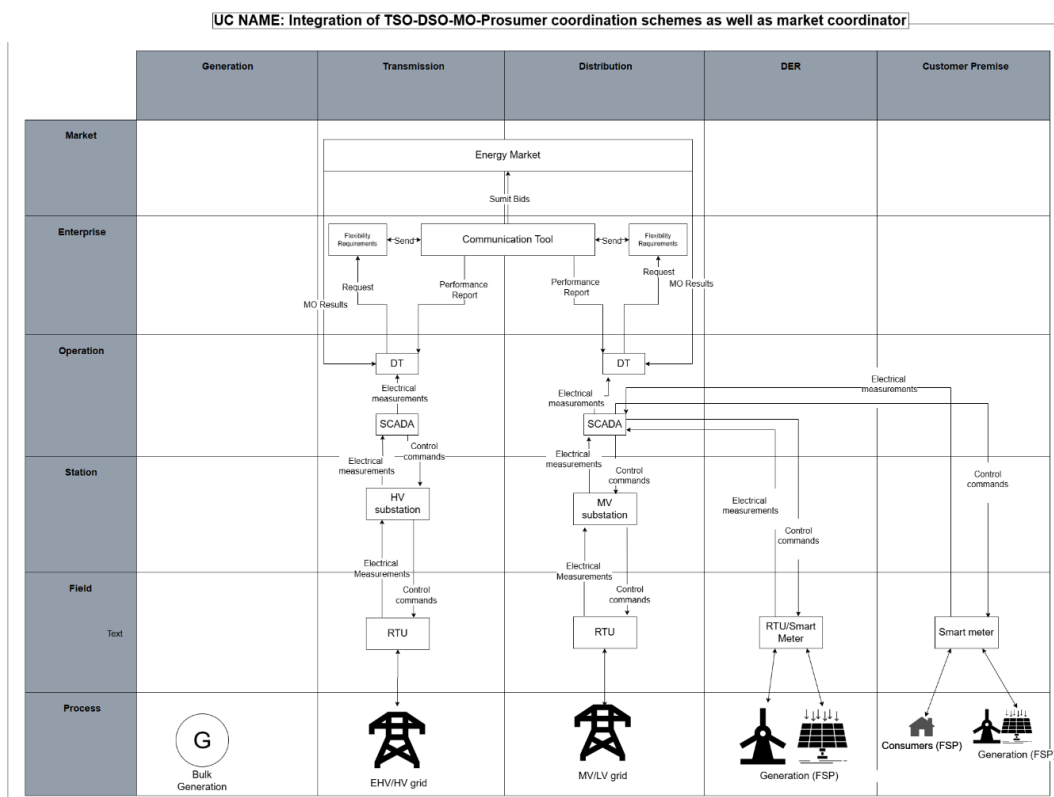


**Figure 5-8: UC Ib12 information layer.**

## 5.3 Development Roadmap

### 5.3.1 ANELL's Distribution Grid DT and OMIE's LFM DT (Implementation of UC Ib04)

A specific development plan has been drafted to follow up on the plan for the enhancement of the DSO DT and the definition of procedural actions towards simulating eventual cyber attacks on the LFM operation that led to abnormal market participation behaviours. This will trigger the protocol activation to mitigate the risk and consequences of such abnormal behaviour.

The following Gantt chart (see Figure 5-9) maps all main pieces of development and fine-tuning of general definition required for the demonstrations' execution.

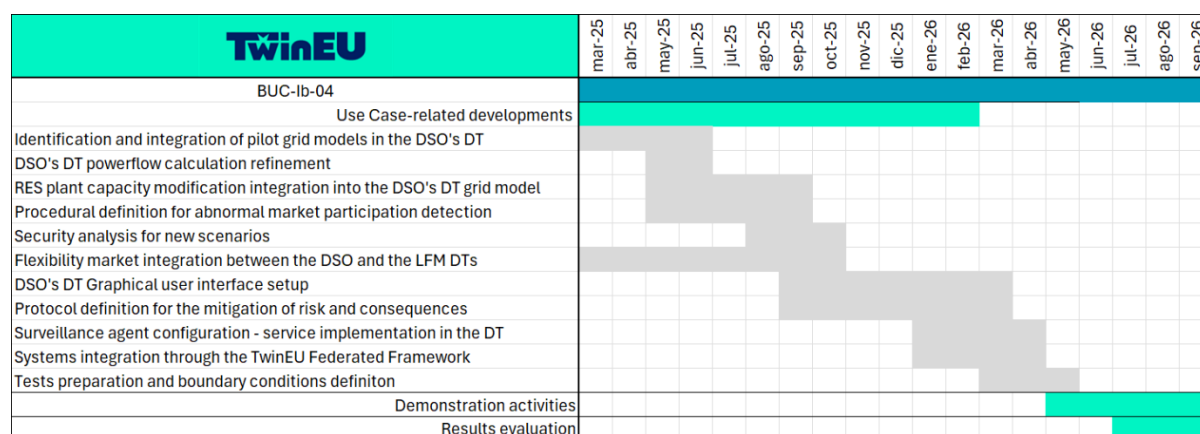


Figure 5-9: BUC implementation - development plan (Gantt chart).

### 5.3.2 REN's Transmission Grid DT and Portuguese Distribution Grid DT model (UC Ib12)

The development plan for REN's Transmission Grid DT and Portuguese Distribution Grid DT model can be seen in the following Gantt chart as shown in Figure 5-10, marking the next steps that are going to be taken.

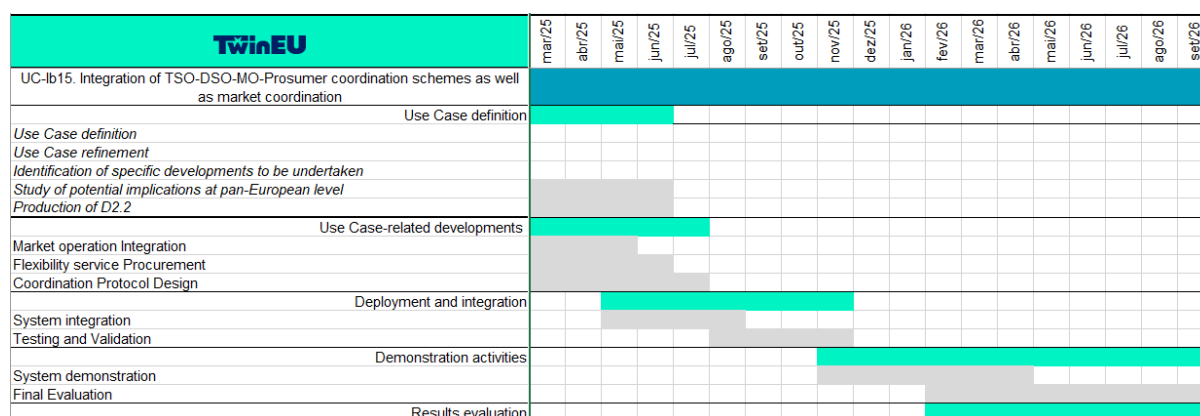


Figure 5-10: UC Ib12 - development plan (Gantt chart).

## 5.4 Developed Framework and Results Demonstration Results

### 5.4.1 ANELL's Distribution Grid DT and OMIE's LFM DT (Implementation of UC Ib04)

A full assessment on cyber security breached that could lead to abnormal market participation behaviours in local flexibility markets was performed, identifying three main scenarios:

- Fake offers sent to the market;
- Unforeseen delivery validation executions from FSPs;
- Compromised databases integrity

For each one of these scenarios a dedicated protocol was depicted on how to tackle the incident and prevent the systems to spread the eventual cascading effects.

Scenario S1 – Fake offers, describes a protocol aimed at mitigating the risks associated with malicious or compromised bids submitted by Flexibility Service Providers (FSPs) in local flexibility markets. The process begins with the Distribution System Operator (DSO) issuing a flexibility request and the Local Flexibility Market Operator (LFMO) opening a market session. FSPs then submit bids specifying the amount and timing of flexibility they are willing to provide. The core vulnerability arises at this stage: if an FSP's internal systems are compromised, a fake offer can be submitted that appears legitimate. LFMs are especially vulnerable as they are currently emerging and introducing a large number of new market participants that so far had never been an active part of the electricity system and whose core business is not within the sector.

The LFMO performs standard validation checks to ensure that bids meet formal requirements—such as correct structure and required fields—but these checks are purely syntactic. As a result, if the systems of one of these new market participants had been attacked, a malicious offer can pass validation if it is correctly formatted, even if it is not genuine.

Once validated, bids proceed to market clearing, where accepted offers may be matched with system needs. At this point, fake offers can directly influence the market outcome, potentially leading to incorrect dispatch decisions. To mitigate this, the protocol introduces a post-clearing validation step in which the LFMO re-confirms matched offers with the corresponding FSPs. This step is critical but also highlights a major challenge: if the FSP's systems are compromised, even this confirmation process may not be trustworthy. Consequently, the protocol proposes the use of an alternative communication channel and suggests secure, certificate-based exchanges through the federated infrastructure in TwinEU, i.e., its data space, as well as the development of cross-validation mechanisms. If a fake offer is detected, the DSO can trigger a re-clearing of the market excluding that offer and may impose restrictions on the offending FSP's future participation. A key insight from this scenario is that traditional market validation mechanisms are insufficient in the context of cyber threats, as they fail to account for behavioural anomalies or compromised actors.

Building on this, Scenario 2 on Delivery Validation continues the logic of S1 by addressing what happens when market a threat couldn't be detected goes forward in the negotiation phase and results into mismatching schedules between the DSO and the LFMO. It assumes that even if bids were accepted as valid, issues may arise during delivery, either due to fake offers or operational failures. After the DSO validates the feasibility of the market outcome using its digital twin (ÉTER), including the possible imposition of technical constraints, the system moves into the operational phase. On the day of delivery, the DSO relies on real-time monitoring capabilities to verify whether FSPs are

providing the agreed flexibility. This is typically done using submetering data, which introduces its own challenges, particularly in establishing reliable baselines for expected performance. The protocol emphasizes the importance of neutral and accredited submetering systems accessible to all parties, as a way to ensure trust in measurement data.

If an FSP fails to deliver as expected, the DSO must respond in real time. In less severe cases, the system may be recalculated dynamically, resulting in a suboptimal but still functional outcome. However, in more critical situations—such as when grid congestion arises or system stability is threatened—the protocol proposes more robust mitigation measures. These include the introduction of reserve flexibility capacity, whereby additional FSPs remain on standby and can be activated immediately if needed. If the situation cannot be resolved within the market framework, the session may be interrupted and penalties applied. Finally, an ex-post analysis is conducted to determine the root cause of the failure, whether it be a cyber attack, technical issue, or metering problem, and appropriate penalties or corrective measures are enforced.

S2 relies on real-time monitoring on the DSO side for detecting anomalies, effectively serving as the operational continuation of the security concerns identified in S1. It highlights a transition from trusting declared bids to verifying actual physical performance, leveraging digital twins and measurement systems as central tools.

Finally, S3 – Databases Integrity takes a broader and more systemic perspective by addressing the integrity of data throughout the entire market lifecycle. Unlike S1 and S2, which focus on specific operational events, S3 identifies vulnerabilities and mitigation measures across all stages of the market, from participant registration to final settlement. During registration, risks include credential theft and impersonation, which are mitigated through strong authentication, encrypted communications, and validation of participant identity and asset data. In the bid submission phase, the main threats involve interception or manipulation of bids, addressed through encryption, strict data formats, and integrity checks.

The scenario then considers the market clearing process itself, where threats include algorithm manipulation, database injection, and insider attacks. Mitigation measures focus on secure execution environments, integrity controls, and strict access management. The publication of market results introduces additional risks, such as data tampering or defacement of public information, which are countered by anonymization, digital signatures, and hardened web infrastructure. In the settlement phase, the integrity of financial data is paramount, requiring strict access controls, validation of inputs, and comprehensive auditing. The scenario also highlights broader risks such as data exfiltration and vulnerabilities in API-based integrations with stakeholders, which could enable lateral movement across interconnected systems.

The main insight from S3 is that cyber security in local flexibility markets must be addressed as an end-to-end problem, where integrity is ensured not only at the point of market participation but throughout all systems and processes. It emphasizes that the most critical risk is not necessarily system unavailability, but rather the undetected manipulation of data, which could compromise market outcomes and financial settlements. It also underscores the importance of considering insider threats alongside external attacks.

Taken together, the three scenarios form a coherent framework for cyber-resilient market design. S1 focuses on detecting and mitigating fake offers at the market participation stage, S2 ensures that real-time delivery is validated and system stability is maintained despite potential failures, and S3 provides the foundational data integrity mechanisms required to secure the entire ecosystem. A

central conclusion is that future flexibility markets must adopt a zero-trust approach, combining secure communication, independent validation channels, real-time monitoring, and redundancy mechanisms to ensure both market and grid resilience in the face of increasingly sophisticated cyber threats.

Within the DT-based demonstration activities of UC04, specific experiments were performed to execute how Scenario 1 on fake offers would look like in an operational environment. As LFMs in Spain are still under development (not an operative figure yet), demonstrations for the delivery validation or the databases integrity could not be executed. However, TwinEU has made use of the proposed work to identify resilience mechanisms to be implemented in the final operation figure by-design.

#### **5.4.2 REN's Transmission Grid DT and Portuguese Distribution Grid DT model (UC Ib12)**

In the case of UC Ib12, the simulation assessed the integration of FIRME flexibility bids into the Portuguese mFRR-R market through a coordinated TSO-DSO framework. The model represented the main operational stages of the use case, including the submission of local flexibility bids, aggregation of smaller offers, DSO validation, forwarding of eligible bids to the TSO market, merit-order clearing, activation management and calculation of economic and operational performance indicators.

The results indicate that flexibility resources participating in the local market can contribute to system-level balancing and the resolution of operational needs when they comply with the applicable mFRR-R requirements. FIRME bids were able to compete with native mFRR-R bids after being converted into a compatible format and checked against criteria such as prequalification status, activation direction, delivery period, location, response time and availability.

The forwarding process highlighted the role of the DSO as a gatekeeper between the local flexibility market and the TSO balancing market. Only bids that had already been validated, remained available and complied with the forwarding requirements were transferred to the mFRR-R pool. Bids were excluded when they failed eligibility criteria, were still subject to recovery restrictions, had already been used incompatibly or did not satisfy the required product characteristics.

During clearing, forwarded FIRME bids and native mFRR-R bids were assessed within the same market pool. Eligible bids were ordered according to economic merit, with response time and submission time used as additional selection criteria. Bids were activated until the required flexibility need was covered. Marginal pricing was used as the default settlement mechanism, meaning that accepted bids within each clearing period were remunerated according to the price of the marginal accepted offer.

Effective lifecycle management is essential for flexibility bids. Capacity cleared in the local flexibility market should not be considered a single-use annual product. Instead, it may be activated multiple times during the relevant service period, provided that the resource remains available, satisfies the applicable recovery-time requirements, and stays within its contractual and operational limits. This lifecycle approach helps prevent overlapping or conflicting activations while allowing flexibility resources to be reused whenever the market and technical conditions permit.

### **5.5 Alignment with Digital Twin Concepts**

In the case of UC Ib04, Scenario 2 on Delivery Validation conceptually represents the stage of the process in which role of the Digital Twin (in this case embedded into ETRA's ÉTER as an ADMS) within

the distribution grid becomes most operationally critical. In this context, the digital twin would act as the core mechanism through which the DSO ensures that the flexibility contracted in the market is actually delivered as expected and that any deviations—whether caused by technical issues or cyber attacks—are detected, interpreted, and mitigated without compromising system stability.

The DSO's grid DT in Scenario 2 is proposed to monitor delivery in real time, detect anomalies through a surveillance agent linked to cyber or technical issues, evaluate their impact on the network, and support the activation of corrective measures. By doing so, it would provide flexibility markets with enhanced resilience mechanisms.

The UC Ib12 simulation aligns with digital twin concepts reproducing key processes such as bid submission, validation, clearing, and activation. The DSO validation step embeds technical and network constraints, ensuring only feasible bids are forwarded, while continuous eligibility checks maintain consistency between digital models and real conditions. The inclusion of clearing, activation, and lifecycle management reflects the dynamic and time-dependent nature of system operation, where resources are repeatedly assessed and reused. Overall, the simulation integrates market and operational dimensions into a single environment, supporting validation, coordination, and performance analysis, which are core functions of a digital twin.

## 6 T5.5 Overview

### 6.1 Challenges Addressed by the Task

The scope of this task concerns cooperative training sessions for system operators and testbed for software or hardware modules. The objective of this task is to improve the training of system operators on realistic network scenarios, involving power networks as well as communication network events. The DT should be able to play scenarios and to record the results for a debrief with trainees. The DT is meant for training system operators on stability-critical scenarios and for testing new components (automata, software decision modules). It will include several modules within a co-simulator interfaced through an orchestrator module:

- Cyber-physical simulators to represent physical and cyber networks.
- SCADA that will display network state to operators and send orders from the operators to the cyber-physical simulators.
- A game master will supervise all the modules and will have the ability to run training scenarios.

The twin provides input/output interfaces for interfacing software or hardware modules. The aim is to develop a kind of twin of the control room that can be used both to train our operators and to test under real conditions the new decision-support assistants that we are developing in Research and Development (R&D) division. For this we want to model cyber-physical aspects, including the new range of automatic controllers that we are designing; we want to model telecoms networks, and of course all this will be scenarized to be able to simulate events on both physical and telecom networks.

It will be an innovative educational tool specifically calibrated to analyse stability-critical scenarios, providing a comprehensive platform for operator readiness and response optimization. The integration of SCADA interfaces and a communication system simulator into the DT will enhance the training experience, offering a realistic and immersive environment for operators to hone their skills and adapt to dynamic grid conditions effectively.

This framework is made of:

- **Cyber-physical simulators** that can be like training simulators. They use real-time data and scenario inputs and simulate the real-world physics and cyber layers (LAN and MAN layers). This simulator must give accurate results over time, as the training session may last a while (hours) but should also run fast, as the operator shouldn't experience any lagging or freezing effects. In other words, it must deal with all the time-domain simulation complexities (digital controllers, various automata, etc.) while respecting short timing (less than 1 sec computation time for 1 sec simulated scenario). Co-simulation can be considered between the asset simulator (including telecommunication components) and the cyber-physical simulator.
- **SCADA** as the interface between the operator, the game master, and the cyber-physical simulators. This SCADA displays the information (GUI) and receives the operators' orders as they would be sent/received as in the real world. Different levels of details are possible: a proxy of the real SCADA and WAN systems, a micro-WAN, and an open-source SCADA simulator or replicas using the same protocols for sensors and actuators.
- **Game Master** that generates scenarios for the game (training session) such as: wind scenarios – PV variations – classical generation outages, events affecting the data acquisition - delays, cyber-attacks, events that impact the automata on the field, electrical grid failures (faults,

overloads). Creates contrasted and "queue distribution" while realistic scenarios to stress the operators during the game. Historizes and capitalizes on the game and on decision making. It enables ex-post comparison of the various decision support modules. It gives the opportunity to debrief the sessions, enabling efficient comparison between the different modules tested. Game master is also responsible for configuring the system modules (grid model, mapping of grid assets with their telecommunication correspondents, etc.).

- **Smart assistant layer** is an independent module from the digital twin. Any proven convenient solution could be plugged into the framework.

Live demos will demonstrate the tool's ability to perform advanced training sessions, including the various features of each module.

## 6.2 Architecture of Digital Twin and Description

This architecture involves two key personas: the Trainer and the Trainee as illustrated in Figure 6-1. The training process is conducted using a training simulator, which enables trainees to handle complex and critical scenarios. The trainer is responsible for configuring the game simulation in alignment with the Game Master system.

Game Master:

The Game Master system consists of three primary components:

- **Game Master** – This component manages the trainer's actions and configurations, interacting with the real-time system through an orchestrator. Actions from the Game Master are pulled by the orchestrator for execution.
- **State View** – The trainer has access to an unfiltered network view, allowing them to observe all simulated values (not available for the trainee). The trainee's observability of substations can be selectively disabled to ensure controlled training conditions.
- **Game Master KPI** – This component is responsible for monitoring and computing Key Performance Indicators (KPIs) during the simulation. It takes relevant data inputs to analyse the system's behaviour and inform the Game Master of any necessary actions in response to the system events.

Once the training is configured, the Game Master pushes the settings to the Orchestrator. The Orchestrator then processes these configurations, utilizing defined external interfaces to push events into the event queue. Acting as a bridge between Game Master and the Cyber-Physical Simulator, the Orchestrator ensures seamless communication between these systems. (Simulation results from simulator through orchestrator to SCADA & Game Master).

Cyber-Physical Simulator:

The Cyber physical simulator is composed of three key modules:

- **Grid Simulator** – A dynamic simulator based on Dynawo, representing the physical state of the system. It pushes relevant measurement and signal data to the orchestrator.
- **Asset Simulator** – This module represents the physical state of the network and maps physical values to telecommunication values. It ensures the correct transmission of cyber data (SCADA-related information) to the information flow model. For instance, if a trainee attempts to open a breaker, the Asset Simulator ensures that the action is mapped accordingly.

- **Information Flow Model** – This telecom simulation module handles network characteristics such as delays and data loss, it is connected to SCADA on one side (trainee interface) and external software systems (e.g., centralized automata for testing purposes) on the other side through Orchestrator.

The system is designed to be event driven. The Grid Simulator sends data to the Asset Simulator through the orchestrator, which maps the changing data to trigger actions in the information flow model. The information flow model in turn, receives and published telecom information, including the tele information TS (state values), TM (Telemetry), TC (remote controls), and TVC (setpoint values). It can also request data updates from the Asset Simulator as needed.

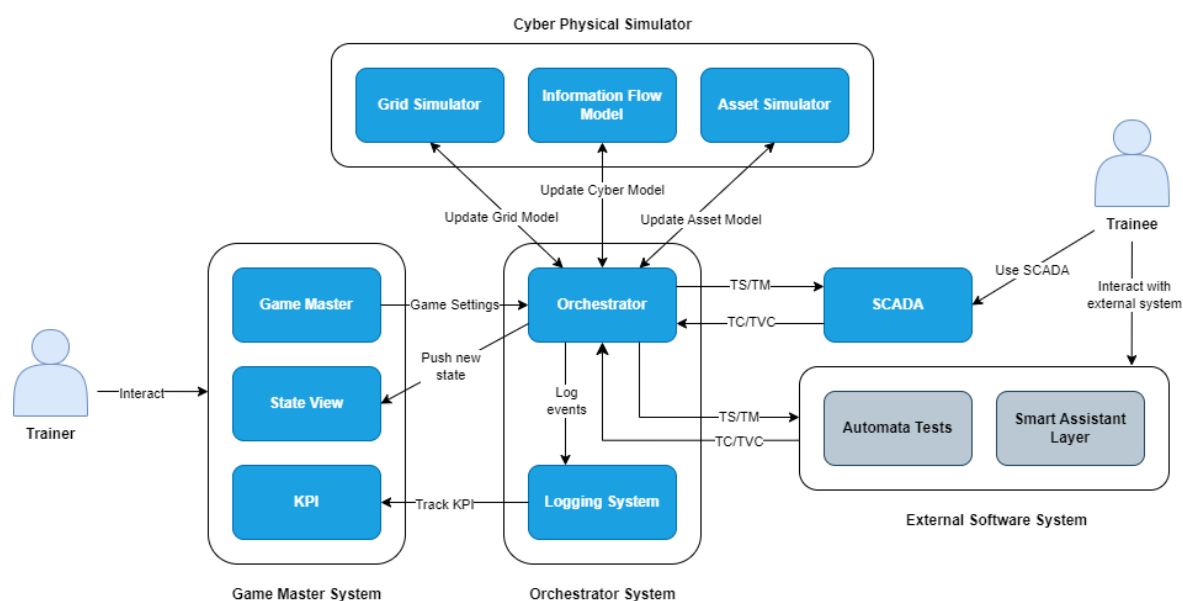


**Figure 6-1: French digital twin architecture.**

#### Orchestrator:

The orchestrator functions as the central scheduling engine for system events and timekeeping, including predefined scenario from the Game Master, system events, telecom events, grid event and external module interactions. The Orchestrator also facilitates communication with SCADA or external software systems, enabling automation testing or integration with a smart assistant layer. It operates in real-time, centralizing actions from the Game Master, trainees, and external modules through the telecommunication system. At each refresh time step, it updates the Grid Model and Asset Model to account for any modifications. The Orchestrator operates on a time-based system, triggering new steps at each second while managing real-time event-based interaction between modules. If a trainee interacts with SCADA, the action is processed by the Orchestrator, which then pushes an event onto the overall queue. Events do not directly interact with the Information Flow Model but must pass through the Orchestrator. (Orchestrator queries information flow model to alter the data)

#### Logging System:

A comprehensive logging function records all events, allowing for scenario replay and performance analysis. This system tracks what actions were performed correctly or incorrectly by the trainee. The most effective method for logging is capturing the event queue from the Orchestrator's perspective, enabling monitoring, tracking, and offline computations of KPIs. Additionally, the Trainer can intervene during the session based on the trainee's input, providing guidance and corrections as needed. This structured approach ensures an effective and seamless training experience, enhancing

both real-time decision-making and post-session analysis. Storage and recording availability will be provided within the logging system.

SCADA Emulator:

The SCADA Emulator is designed to replicate the control room experience for the trainee. It serves as the primary interface for the trainee, enabling interaction with the simulated grid environment.

- **Trainee View:** The SCADA emulator provides a restricted interface tailored for the trainee, simulating what an actual system operator would see in a real control room environment. It reflects only the measurements and controls that are typically available to operators, ensuring realism in the training process.
- **Dispatcher environment:** The interface is designed to mimic a dispatcher's workstation, allowing the trainee to monitor events, analyse system status, and execute control actions.
- **Decision-making and control:** By observing system responses through SCADA measurements, the trainee is encouraged to interpret events and take operational decisions.

## 6.3 Development Roadmap

### 6.3.1 Implemented Functions

The development roadmap focused first on implementing the core functions required to configure, execute and observe a basic cyber-physical training scenario. These functions cover system configuration, interaction between the Game Master and SCADA emulator, dynamic simulation, cyber event handling and the integrated logging and performance assessment.

The system configuration function provides the basis for preparing a training session. This includes the use of IIDM, cyber configuration, Information Flow Model configuration, and scenario definition. These configuration elements allow the platform to initialize the grid, cyber and scenario parameters before a training session is launched.

A basic training scenario was implemented through the interaction of the Game Master and SCADA emulator. On the Game Master side, the trainer can perform actions such as modifying load and generation values and applying topological modifications. These actions allow the trainer to create or modify operational situations during the session. On the SCADA side, the trainee can observe the network state through a substation level view and perform topological actions that are processed by the simulation environment.

The dynamic simulation and cyber-event handling functions were also implemented. The dynamic simulator server operates with a one-second timeframe and update rate, enabling the platform to support real-time interaction during training. The Information Flow Model supports cyber-event handling by representing communication effects such as delays and data loss. This allows the training environment to reproduce situations where the operator's view may be affected by degraded communication or missing information.

The next development activities focus on extending event-handling capabilities and improving the integration of the platform components. This includes the implementation of additional SCADA events, Dynawo events, models and extension to the Game Master language. Together, these implemented functions and planned extensions provide the technical basis for moving from a basic proof-of-concept scenario towards a more complete training platform capable of supporting realistic operator training, cyber-physical event simulation and post-session evaluation.



These actions include opening transformer breakers 1 and 2 to create a contingency, removing observability of a substation to simulate a communication-related contingency, modifying generator setpoints, and decreasing loads.

The trainee can apply different remedial actions to resolve the overload condition. The first option is topological actions, such as opening the busbar coupler. The trainee may also call the trainer to trigger a 5% voltage reduction, referred to as Un-5%. In addition, the trainee can request the trainer to lower active power generation.

Detailed scenario in DSL:

```
// Operate switch
open switch "MQIS P7_MQIS 7COUPL DJ_OC";
close switch "MQIS P7_MQIS 7COUPL DJ_OC";

// Lose communication
change network characteristics link from "RTU_ICCP_MQIS" to "FLOIR", drop fixed true;
change network characteristics link from "FLOIR" to "RTU_ICCP_MQIS", drop fixed true;

// Change setpoints
at [now, now + 15 seconds] with law "linear", decrease generator "BLAYA7GR4" by 15% P;
at [now + 5 seconds, now + 19 seconds] with law "linear", set generator cluster "MPC_GEN" [
"N.SEUIN1", "N.SEUIN2", "N.SEUIN3", "M.PININ1", "M.PININ2", "M.PININ3"] to 40 P
```

The second phase focused on more stressful scenarios to enhance trainee preparedness. The following electrical events were simulated:

- Frequency regulation (ambition)
- Congestion Management (ambition)
- Voltage regulation (ambition)
- Voltage collapse
- NAZA: This automaton was developed to enhance the flexibility of the electrical grid, particularly in managing fluctuations associated with renewable energy sources. NAZA operates by continuously monitoring electricity flows on the transmission network. During instances of surplus production that exceed the network's capacity such as during peak wind or solar conditions. NAZA automatically adjusts the output of renewable energy sites to prevent network saturation.

Additionally, the main cyber components to be simulated include:

- SCADA system
- Substation network gateway
- Remote Terminal Units (RTUs)
- Automaton-based controls

This phased approach ensures that the simulator is first validated with a simple scenario as a proof of concept, allowing for an initial understanding of system complexity. Phase 2 leads to the development of more complex and realistic training scenarios.

The advanced scenario we were able to test implements the action of the NAZA automaton, a cyber-physical congestion management automaton, which is a first in the context of our operators' training. Below are a few screenshots of the session. The panel on the right is the interface of the automaton present at the dispatching centre:

## D5.1 From conceptual use cases to real demonstration – Digital twin for cyber-physical grid resilience

We start from the base case, with the wind power production curves of the area that are flat.

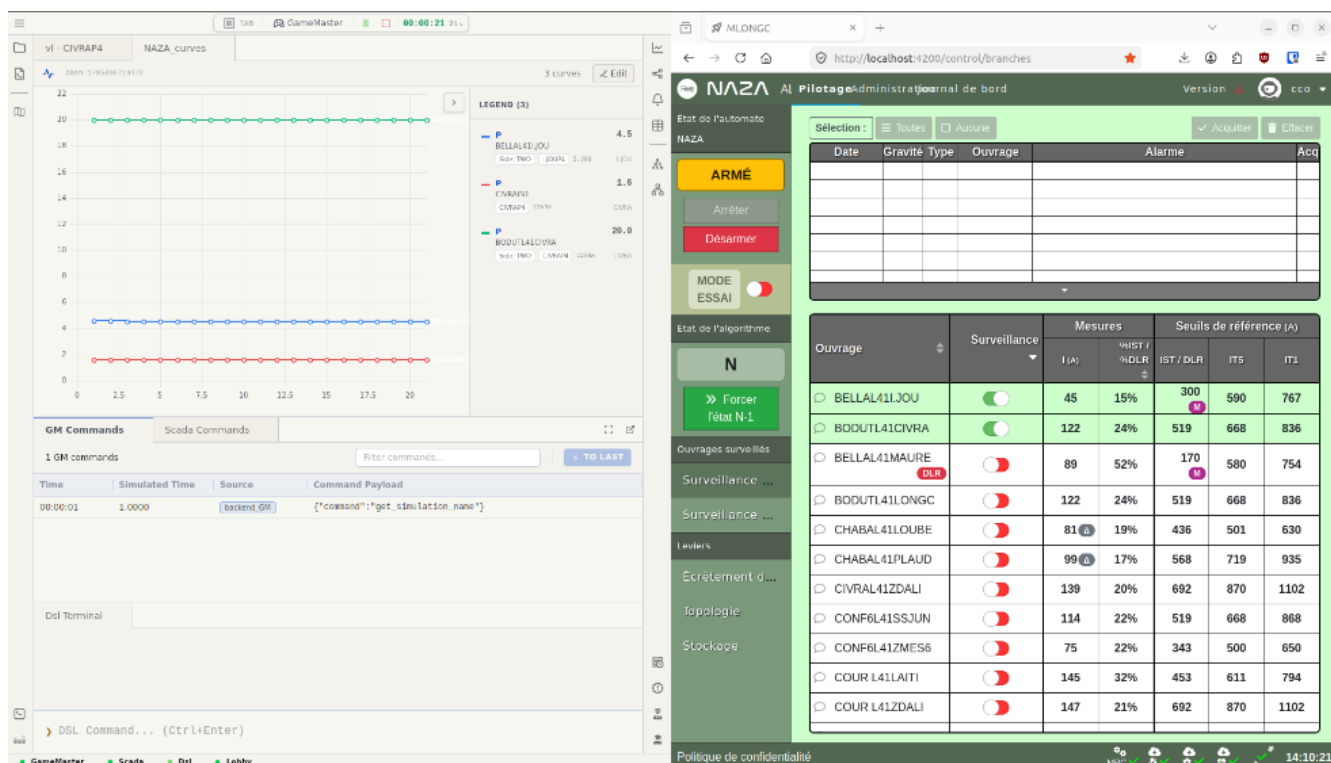


Figure 6-4: Base case situation

The trainer scripts a step-wise ramp-up in wind power output (an increased wind over the zone). See DSL command: at [now+5 seconds, now+...].

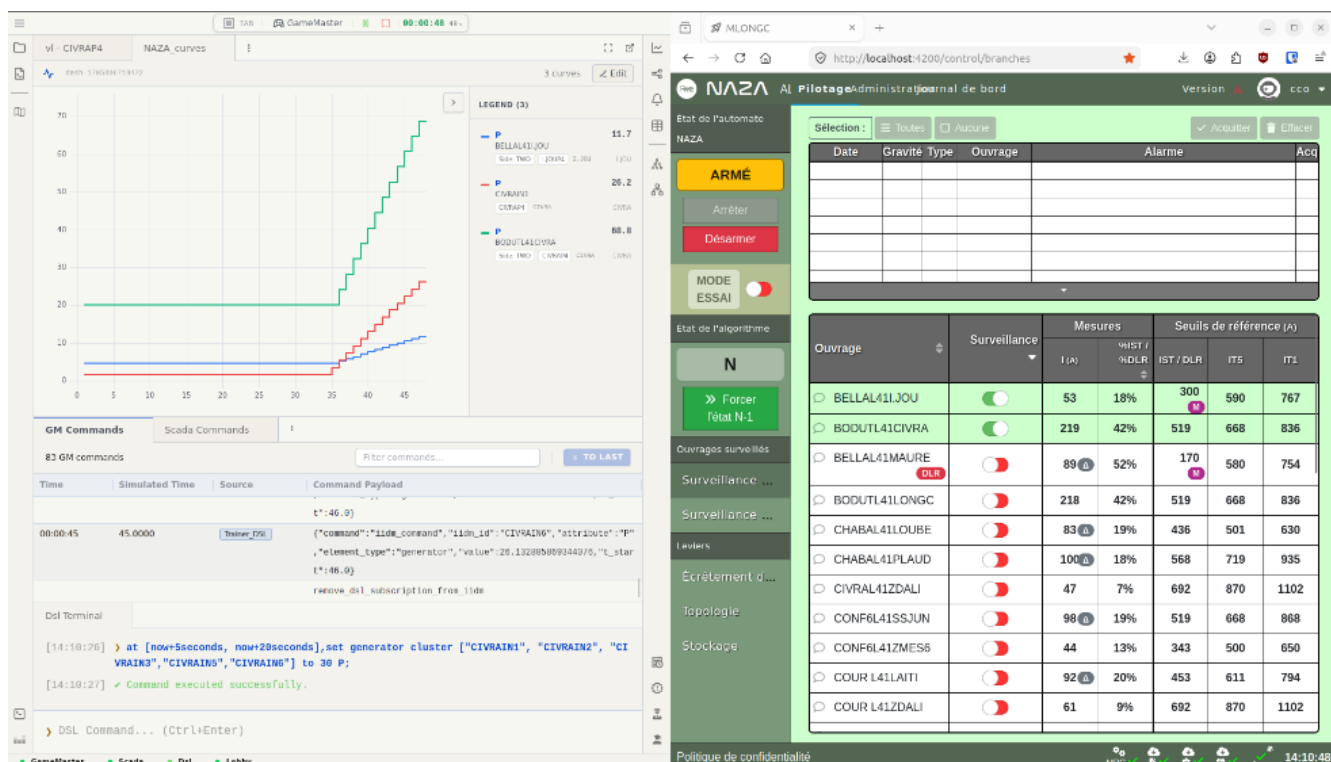


Figure 6-5: Ramp-up in wind power unit

## D5.1 From conceptual use cases to real demonstration – Digital twin for cyber-physical grid resilience

This increase in power fed into the grid causes a congestion on the BODUTL41CIVRA line. This one passes in red on the NAZA screen.

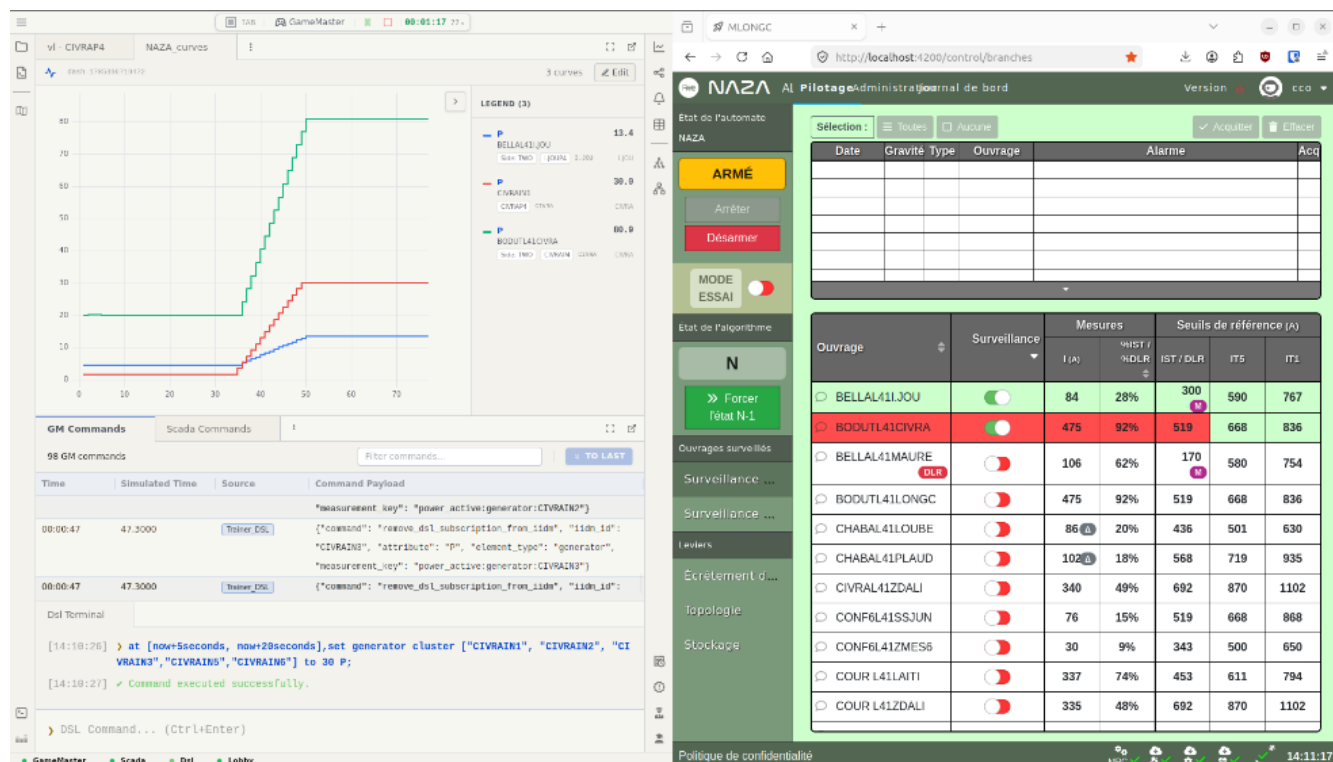


Figure 6-6: Congestion on the grid

The automaton proceeds to curtail the wind production concerned — this is genuinely the field algorithm integrated into TwinEU. The production limitation orders are sent by the automaton via the SCADA network automatically, and the constraint disappears.

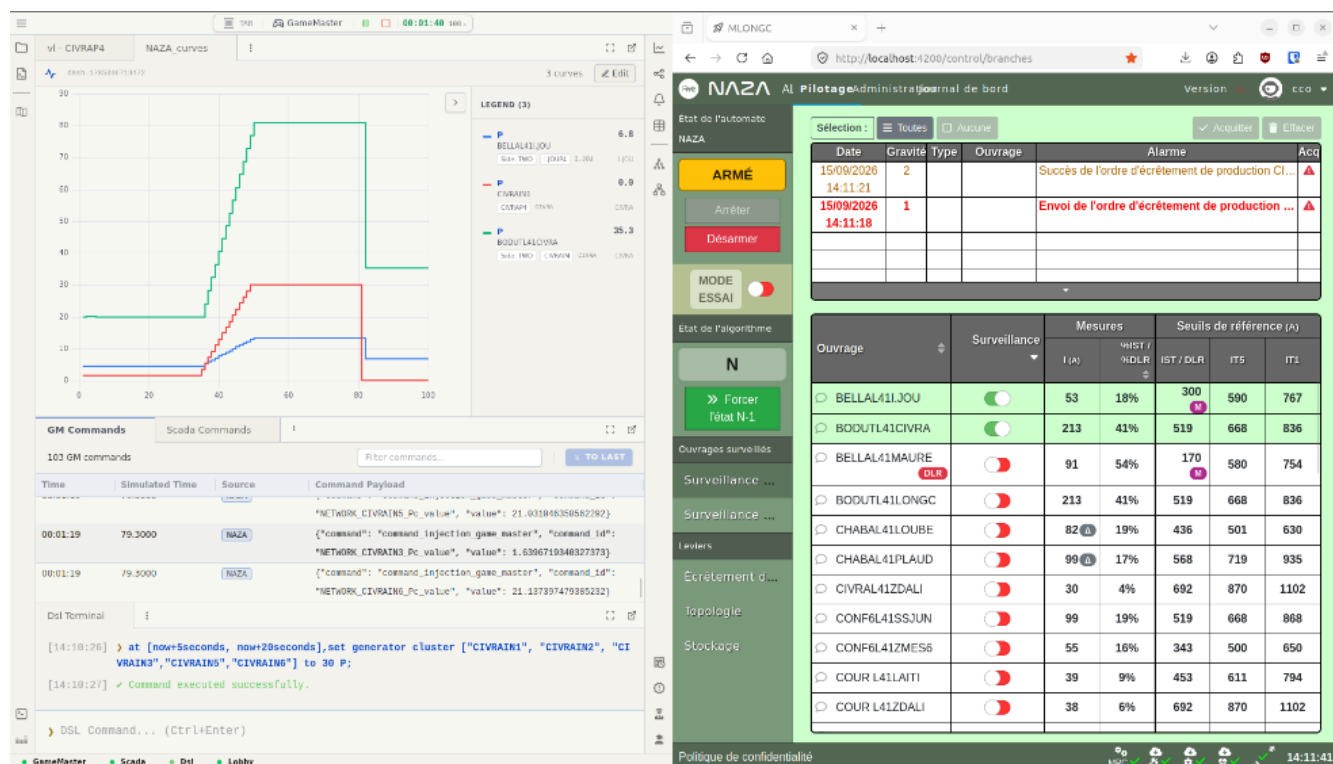


Figure 6-7: Wind Curtailment

More generally, we've reached out to our dispatchers to work on longer, even more representative scenarios

## **6.4 Developed Framework and Results Demonstration**

### **6.4.1 Cyber Physical DT Architecture**

A modular cyber-physical Digital Twin architecture was designed and implemented to support power system operators' training and validation of advanced operational functions. The architecture integrates multiple components, including Cyber-Physical Simulator (grid simulator, information flow model, and asset simulator), Game Master, SCADA emulator, and Orchestrator. Each component communicates through well-defined interfaces coordinated by a central orchestrator, enabling synchronized interaction between physical simulation, cyber-event modelling, operator activities, and training management functions.

The main development outcome is the definition of the overall system architecture and the establishment of communication flows between the different modules.

### **6.4.2 Event-Driven Orchestration Framework**

A real-time event-driven orchestration framework was developed to coordinate the execution of all components. The orchestrator synchronizes physical power simulation, cyber-layer events, operator actions, Game Master, and smart assistant recommendations. The framework establishes a common execution timeline across all modules, ensuring consistent system behaviour.

The implementation resulted in a centralized orchestration layer capable of synchronizing the physical and cyber domains, coordinating interactions between the trainee, operator, trainer and external modules, and supporting reproducible execution of complex scenarios.

### **6.4.3 Real-Time Digital Representation of the Physical Grid**

Incorporated a high-fidelity representation of the transmission system based on detailed network topology and dynamic system behaviour. The simulation continuously updates network conditions in response to operator actions, allowing a realistic representation of evolving operational situations. The simulation environment is based on Dynawo and provides the physical-system representation used during training sessions.

The development work enabled the integration of the Dynawo simulation environment within the training platform and demonstrated real-time simulation capability. It also enables interaction between operator actions and network behaviour. The Dynawo modelling was further enhanced to support training scenarios involving automation and switching behaviour. This included additional automation models, such as lack-of-voltage relays and automatic reclosers, as well as the testing and adaptation of existing models for switch-on configurations.

### **6.4.4 Information Flow Model**

An Information Flow Model (IFM) was implemented to represent the cyber layer of the Digital Twin. Instead of modelling the communication protocols in detail, the IFM reproduces operational effects that impact grid operation, including communication delays, data corruption, unavailable measurements. The model provides a scalable representation of cyber -induced effects without requiring detailed communication network simulation.

The implementation enabled delay modelling, telemetry loss and communication failure scenarios to be introduced into the platform. This allows the platform to reproduce situations where the operator's perceived system state differs from the underlying simulated system state.

### 6.4.5 Implementation of Trainer and Trainee SCADA Interfaces

Dedicated interfaces were developed for operators and trainers to interact with the training simulator. Operators receive the perceived system state through the SCADA interface, whereas the Game Master or Trainer access the complete underlying system state and can influence scenario progression.

Figure 6-8 shows the training session lobby and Figure 6-9 shows the lobby interface used to access a collaborative training session. Through this interface, a session can be created or joined by selecting the required configuration elements. This lobby interface provides the entry points for the training activity and allows different users to access the same active session with their respective roles, such as Game Master or trainee.

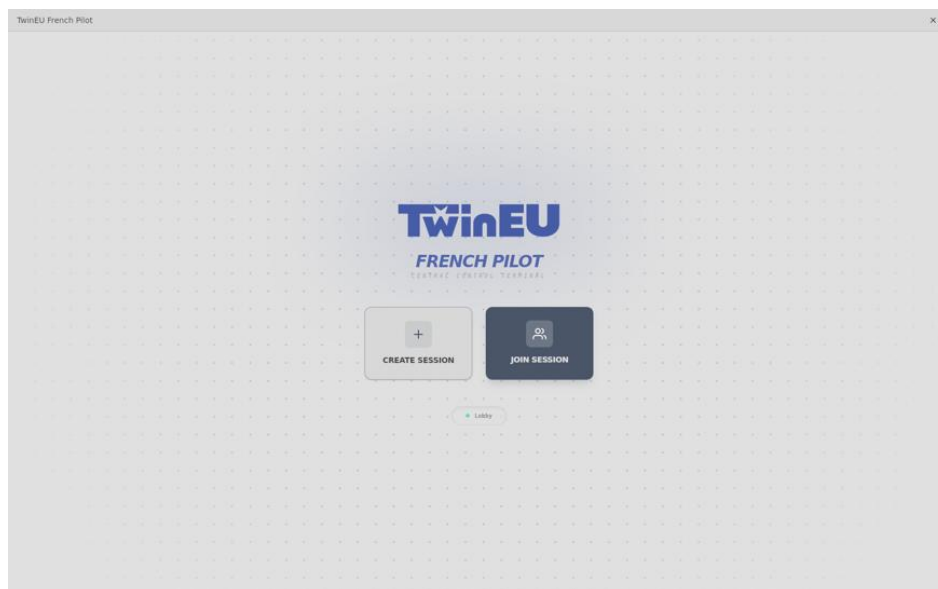


**Figure 6-8: Training Session Lobby**

Figure 6-10 shows the Game Master interface used by the trainer. This interface give the trainer access to the complete simulates system state includes variables and information that are not available to the trainee. The trainer can start the simulation, monitor the substation of interest, observe curves and constraints, and inject events or actions during the scenario. This enables the trainer to supervise the exercise and adapt the scenario progression according to the trainee's response.

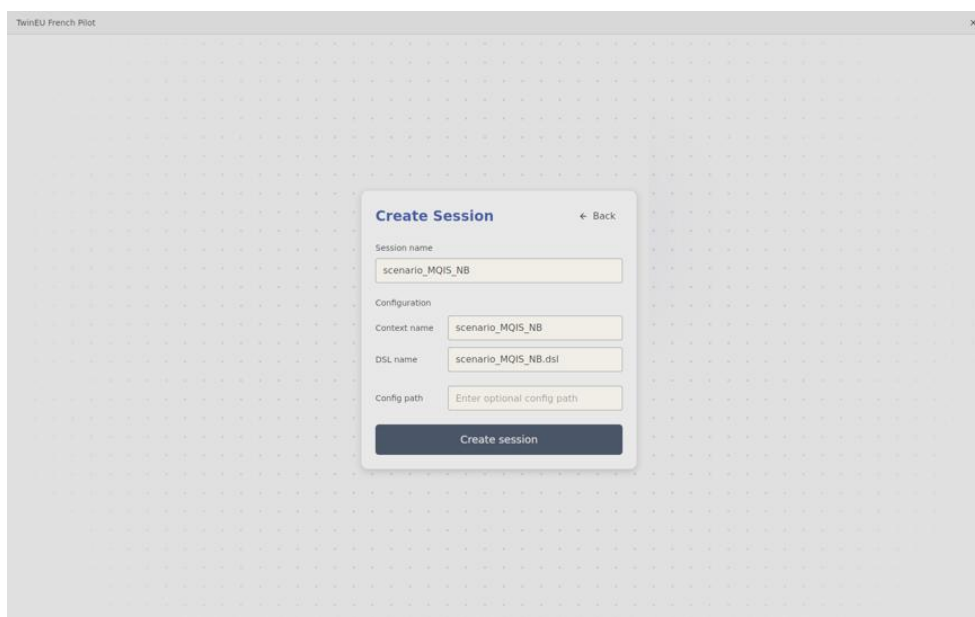


**Figure 6-9: Session Creation Interface**

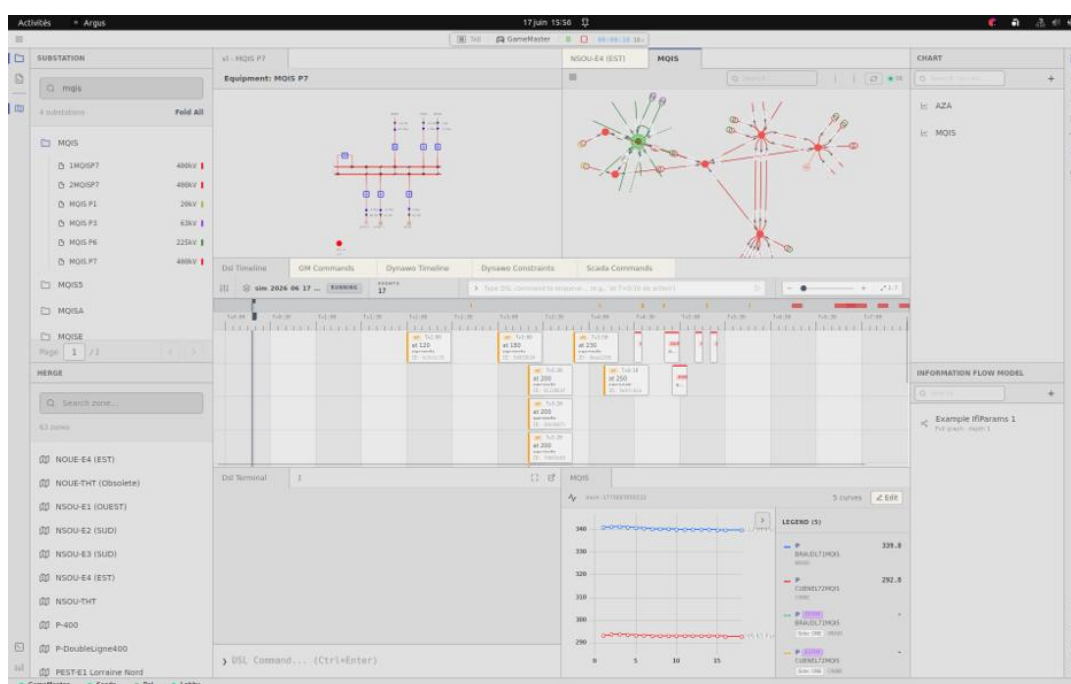


**Figure 6-10: Game Master Interface for trainer supervision**

Figure 6-11 shows the trainee SCADA visualization. The trainee interface is designed to reproduce the control-room experience by displaying the network state, measurements, estimated values and available control actions. The trainee can observe and analyse the operation situation and execute corrective actions.

The parallel views demonstrate the distinction between the complete trainer state view and the restricted trainee SCADA view used for the realistic operator training.

Together, these interfaces enable the core interaction workflow of the training simulator. The lobby supports session access and role selection, the Game Master interface supports trainer

supervision and scenario control, and the trainee SCADA interface supports operator decision-making and command execution. The interfaces also support real-time status updates and monitoring of trainee actions, network evolution and constraints, providing the basis of realistic training and post-session analysis.

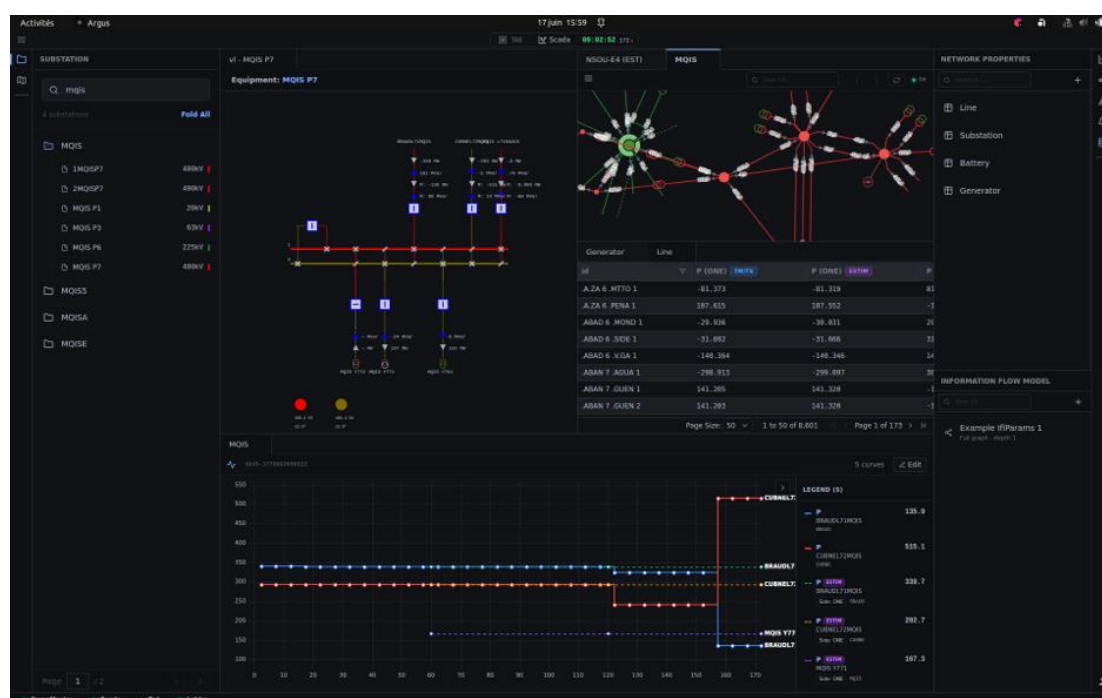


Figure 6-11: Trainee SCADA visualization

## 6.4.6 Scenario Generation and Game Master Control

A scenario management framework was implemented to create, execute, and supervise training exercises. Scenarios define the sequence of operational events, disturbances, failures, and cyber incidents occurring during a training session. The framework supports both predefined and dynamically injected events during training execution.

The Game Master can dynamically modify scenario progress, introduce additional disturbances, adjust difficulty levels, and monitor trainee performance throughout the exercise. The Game Master manages event storage, schedules actions, and issues control commands.

The development resulted in the implementation of PowerEventDSL, a domain-specific language integrated into the Game Master runtime modules and coordinated with the Orchestrator. The DSL was designed based on training requirements and provides a unified grammar for physical grid actions and ICR degradation commands. The scenario framework also supports event scheduling, execution mechanisms and trainer intervention during exercises.

## 6.4.7 Operator Training Scenarios

The developed platform was validated through the representative cyber-physical training scenarios involving equipment outages, network overloads, communication disturbances, and corrective operator actions.

The validation demonstrated the ability of the Digital Twin to reproduce realistic operational conditions while supporting operator training and technology assessment.

The demonstrated scenario focused on a French transmission-network overload case. The platform was used to execute overload management scenarios, validate cyber contingency handling, and demonstrate operator interaction workflows. The scenario showed how a trainee can analyse an overload through the SCADA interface, apply corrective actions and observe the resulting impact on the simulated network state.

#### 6.4.8 Logging and replay basis

A monitoring and logging framework was developed to capture system events, operator actions, automaton responses, and scenario evolution. The collected information provides the basis for session replay, KPI generation, post-event analysis, and future learning analytics capabilities.

The implementation enabled centralized event logging and capture of operator actions, system states, alarms, constraints and simulation events. This supports post-session analysis and provide the foundation for replay functionality.

### 6.5 Alignment with Digital Twin Concepts

The developed platform aligns with the Digital Twin vision of providing a virtual representation of operational environments that can be used for monitoring, analysis, testing, and evaluation of future operation situations. The alignment is demonstrated through the coverage of the use cases identified for this pilot.

- 1) **Anticipating and simulating cyber-attacks and grid outages:** The information flow model and grid simulator are co-simulated rather than only logging real telecom and real events after the fact, the platform can advance scenarios that have not occurred yet—communication delays, data loss, automation failures, transformer overloads- and observe how operators and automata respond under conditions that would be unsafe or impossible to rehearse on the live grid.
- 2) **Simulate grid state for monitoring and operation:** The State View/ Game Master available to the trainer, the restricted Trainee SCADA view, and the periodic state estimation each implement the core synchronization property of a twin (a virtual representation) that is kept consistent with the state of the physical system. In an operational environment, this same view and estimation pipeline would simply be redirected to live measurements instead of Grid/ Asset Simulator, giving operators in the control centre the same kind of unfiltered system view.
- 3) **Coordination between TSO and DSO:** The architecture supports training sessions involving multiple stakeholders. The framework can be extended to represent interactions between Transmission System Operators (TSOs), Distribution System Operators (DSOs) enabling training and evaluation of coordinated operation procedures.

Through the integration of physical-system simulation, cyber-event modelling, operator interaction, and scenario management, the developed platform realizes the key characteristics of a cyber-physical Digital Twin for power-system operation. The resulting environment supports operator training, technology validation, and resilience assessment under realistic operation conditions.

## 7 Conclusion

This deliverable reports the progress and results achieved within Tasks 5.1 to 5.5, addressing the WP5 objective of developing and demonstrating Digital Twin (DT) capabilities for cyber-physical grid resilience. The results cover cyber security of power systems with high penetration of RES, cyber-physical resilience assessment, congestion and stability analysis, abnormal market participation, and power system operator training within the respective TwinEU pilot environments.

Task 5.1 established the conceptual framework for the WP5 demonstrations by transferring and adapting the TwinEU concept to the cyber-physical system resilience pilot and defining the use cases and requirements that guided the developments in Tasks 5.2–5.5. Task 5.2 developed and demonstrated DT for cyber security assessment and cyber-physical resilience of power systems with high penetration of RES in the Dutch transmission and distribution grid environments. Task 5.3 developed and demonstrated DT-based what-if scenarios for assessing the cyber and physical resilience of the grid under different operational and cyber security conditions in the Cypriot pilot environment. Task 5.4 developed and demonstrated market-operator and system-operator DT capabilities for detecting abnormal market participation and assessing mitigation measures within the Iberian and Portuguese pilot. Task 5.5 developed and demonstrated a DT-based power system operator training environment for complex and critical operational situations as part of the French pilot. In brief, the results demonstrate the DT capabilities achieved within the scope of the WP5 pilots regarding cyber-physical grid resilience. The WP5 demonstrations cover cyber attack simulations and detection, cyber attack impact analysis, cyber and physical resilience assessment, congestion and stability-related analysis, abnormal market participation and mitigation, and operator training for complex and critical situations. The results reported in this deliverable represent the demonstrated maturity of these capabilities within their respective pilot environments and test scenarios. Validation beyond the reported scenarios and pilot configurations, as well as broader deployment and operational-scale assessment, falls outside the scope of the work reported in this deliverable.

## References

- [1] Origins of The Digital Twin Concept: August 2016 | PDF | Product Lifecycle | Simulation, <https://www.scribd.com/document/530059103/MWGDigitalTwinExcerpt>.
- [2] Srivastava *et al.*, “Digital Twins Serving Cyber security: More Than a Model: Cyber security as a Future Benefit of Digital Twins 2,” *IEEE Power and Energy Magazine*, vol. 22, pp. 61–71, Jan. 2024, doi: 10.1109/MPE.2023.3325196. Online Available: <https://ieeexplore.ieee.org/document/10398550>.
- [3] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, “Digital Twin in Industry: State-of-the-Art,” *IEEE Trans. Industr. Inform.*, vol. 15, pp. 2405–2415, Apr. 2019, doi: 10.1109/TII.2018.2873186. Online Available: <https://ieeexplore.ieee.org/document/8477101>.
- [4] X. He, Q. Ai, R. C. Qiu, and D. Zhang, “Preliminary Exploration on Digital Twin for Power Systems: Challenges, Framework, and Applications,” Sep. 2019. Online Available: <https://arxiv.org/abs/1909.06977>.
- [5] “Cyber-Attack Against Ukrainian Critical Infrastructure | CISA,” <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>.
- [6] R. Amoah, S. Camtepe, and E. Foo, “Securing DNP3 Broadcast Communications in SCADA Systems,” *IEEE Trans. Industr. Inform.*, vol. 12, pp. 1474–1485, Aug. 2016, doi: 10.1109/TII.2016.2587883. Online Available: <https://ieeexplore.ieee.org/document/7506334>.
- [7] J. G. Wright and S. D. Wolthusen, “Stealthy Injection Attacks Against IEC61850’s GOOSE Messaging Service,” in *Proceedings - 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe 2018*, Institute of Electrical and Electronics Engineers Inc., Dec. 2018. doi: 10.1109/ISGTEurope.2018.8571518. Online Available: <https://ieeexplore.ieee.org/document/8571518>.
- [8] J. Hong, C. C. Liu, and M. Govindarasu, “Integrated anomaly detection for cyber security of the substations,” *IEEE Trans. Smart Grid*, vol. 5, pp. 1643–1653, 2014, doi: 10.1109/TSG.2013.2294473. Online Available: <https://ieeexplore.ieee.org/document/6939779>.
- [9] A. Elgargouri, R. Virrankoski, and M. Elmusrati, “IEC 61850 based smart grid security,” in *Proceedings of the IEEE International Conference on Industrial Technology*, Institute of Electrical and Electronics Engineers Inc., Jun. 2015, pp. 2461–2465. doi: 10.1109/ICIT.2015.7125460. Online Available: <https://ieeexplore.ieee.org/document/7125460>.
- [10] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, “Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation,” *IEEE Trans. Smart Grid*, vol. 10, pp. 3044–3056, May 2019, doi: 10.1109/TSG.2018.2817387. Online Available: <https://ieeexplore.ieee.org/document/8320388>.
- [11] K. Pan, P. Palensky, and P. M. Esfahani, “From Static to Dynamic Anomaly Detection with Application to Power System Cyber Security,” *IEEE Transactions on Power Systems*, vol. 35, pp. 1584–1596, Mar. 2020, doi: 10.1109/TPWRS.2019.2943304. Online Available: <https://ieeexplore.ieee.org/document/8846711>.
- [12] J. J. Q. Yu, Y. Hou, and V. O. K. Li, “Online False Data Injection Attack Detection with Wavelet Transform and Deep Neural Networks,” *IEEE Trans. Industr. Inform.*, vol. 14, pp. 3271–3280, Jul. 2018, doi: 10.1109/TII.2018.2825243. Online Available: <https://ieeexplore.ieee.org/document/8334607>.
- [13] J. D. Markovic-Petrovic and M. D. Stojanovic, “Analysis of SCADA system vulnerabilities to DDoS attacks,” in *2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services, TELSIKS 2013*, 2013, pp. 591–594. doi: 10.1109/TELSKS.2013.6704448. Online Available: <https://ieeexplore.ieee.org/document/6704448>.

- [14] R. Kalluri, L. Mahendra, R. K. S. Kumar, and G. L. G. Prasad, "Simulation and impact analysis of denial-of-service attacks on power SCADA," in *2016 National Power Systems Conference, NPSC 2016*, Institute of Electrical and Electronics Engineers Inc., Feb. 2017. doi: 10.1109/NPSC.2016.7858908. Online Available: <https://ieeexplore.ieee.org/document/7858908>.
- [15] "A. Carcano, A. Di Pinto, Y. Dragoni, and A. Carcano, 'The Future of Securing Intelligent Electronic Devices Using the IEC 62351-7 Standard for Monitoring,' in *Proc Black Hat USA, USA, 2019*, pp. 1-21." Online Available: <https://infocondb.org/con/black-hat/black-hat-usa-2019/the-future-of-securing-intelligent-electronic-devices-using-the-iec-62351-7-standard-for-monitoring>.
- [16] J. Gilles, "Empirical wavelet transform," *IEEE Transactions on Signal Processing*, vol. 61, pp. 3999–4010, 2013, doi: 10.1109/TSP.2013.2265222. Online Available: <https://ieeexplore.ieee.org/document/6522142>.
- [17] M. J. Li, C. K. Tse, D. Liu and X. Zhang, "Cascading Failure Propagation and Mitigation Strategies in Power Systems," in *IEEE Systems Journal*, vol. 17, no. 2, pp. 3282-3293, June 2023, doi: 10.1109/JSYST.2023.3248044. Online Available: <https://ieeexplore.ieee.org/document/10066154>.
- [18] TwinEU, Assessing the Cyber and Physical Resilience of the Grid with TwinEU DT, Deliverable D5.2, 2026. Online Available: [D5.2](#)