



Assessing the cyber and physical resilience of the grid with TwinEU DT

Deliverable No: D5.2

Work package: WP5

Official delivery date: 30.06.2026

Actual delivery date: 29.06.2026 (v1), 28.09.2026 (v2)

Dissemination level: Public



Project: 101136119 | HORIZON-CL5-2023-D3-01 | www.twineu.net

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	
Markos Asprou (University of Cyprus)	David Herve (RTE)
Lenos Hadjidemetriou (University of Cyprus)	May Myat Thwe (TUD)
Geethu Joseph (CRESYM)	Shafiulla Syed (TUD)
Lucas Saludjian (RTE)	Abhishek Saini (TUD)
Olivier Bretteville (RTE)	Alexandru Ștefanov (TUD)
Thibaut Vermeulen (RTE)	Peter Palensky (TUD)

Version	Date	Author(s)	Notes
0.1	28.11.2024	Markos Asprou	first draft
0.2	27.05.2025	Markos Asprou	2nd draft
0.3	13.05.2026	Markos Asprou	3 rd draft
0.4	15.06.2026	Shafiulla Syed	4 th draft
0.5	24.06.2026	Markos Asprou	5 th draft
0.6	26.06.2026	Geethu Joseph	6 th draft
0.9	28.06.2026	Alexandru Stefanov	Final v1 draft
1.1	21.09.2026	Alexandru Stefanov	1 st v2 draft
1.2	22.09.2026	Markos Asprou	Final v2 version

Responsible Partner	UCY (University of Cyprus)
Checked by WP leader	Alexandru Ștefanov (TUD), 28.06.2026 (v1), 21.09.2026 (v2)
Verified by the appointed Reviewers	Szucs Gabor (MAVIR), 14.09.2026 Rui Pestana (REN), 14.09.2026
Approved by Project Coordinator	Padraic McKeever (Fraunhofer), 29.06.2026 (v1); 28.09.2026 (v2)

Table of Contents

Executive Summary	8
1 Introduction	11
1.1 Tasks 5.2, 5.3, and 5.5	11
1.2 Objectives of the Work Reported in this Deliverable	12
1.3 Outline of the Deliverable	13
1.4 How to Read this Document	13
2 Cyber and Physical Resilience and Reliability in Power Systems	14
2.1 Definition of Resilience and Reliability	14
2.1.1 Power System Resilience	14
2.1.2 Power System Reliability	16
2.2 Key Challenges	16
2.2.1 Key Challenges in Ensuring Resilience	16
2.2.2 Key Challenges in Ensuring Reliability	18
2.3 Role of Digital Twins in Resilience and Reliability Assessment	19
3 Overview of Digital Twin Framework	21
3.1 Description of the Dutch digital twin	21
3.1.1 Introduction	21
3.1.2 Dutch Transmission model	22
3.1.3 Distribution network	26
3.2 Description of the Cypriot digital twin	27
3.2.1 Digital twin architecture	28
3.2.2 Real time simulation model	29
3.2.3 Data management layer and Visualization	30
3.2.4 Hardware in the loop controller	31
3.2.5 Reliability assessment	35
3.3 Description of the French digital twin	36
3.3.1 Introduction	36
3.3.2 Objectives	36
3.3.3 System Architecture	36
4 Approach to Scenario Development	38
4.1 Scenarios in the Dutch digital twin	38
4.1.1 Network Reconnaissance	38

4.1.2	Denial-of-Service Attacks	39
4.1.3	False Data Injection	39
4.2	Scenarios in the Cypriot digital twin	40
4.2.1	Operational scenarios	40
4.2.2	Cyber-Security Scenarios	41
4.3	Scenarios in the French digital twin	41
5	Impact of Stressed Conditions on the Physical Resilience of the Grid	43
5.1	Case Studies of Physical Stress Scenarios	43
5.2	Lessons learned and recommendations	46
6	Impact of Cyber-Attacks on Grid Resilience	48
6.1	Case studies of Cyber-Attack Scenarios in the Cypriot demo	48
6.1.1	False data injection attack on substation measurements	48
6.1.2	False data injection attack on the voltage measurements	49
6.1.3	Battery Setpoint Injection Attack	51
6.1.4	Impact Analysis of cyberattacks on the controller performance and the system operation 52	
6.1.5	Lessons learned and recommendations	53
6.2	Case studies of Cyber Attack Scenarios in the Dutch demo	53
6.2.1	Impact analysis of system performance and Impact on the system	54
6.2.2	Lessons learned and recommendations	65
7	Development of a Digital Twin for Training	66
7.1	Scenarios for training	66
7.2	Description of the training activities	68
7.3	Lessons learned and recommendations	74
7.3.1	Lessons Learned	74
7.3.2	Recommendations	75
8	Conclusion	76
	References	78

List of Figures

Figure 1: Increasing frequency of extreme events worldwide (1980 levels are set at 100%) [6].....	15
Figure 2: Cyber-physical digital twin framework for cybersecurity assessment.	22
Figure 3: Dutch transmission model	25
Figure 4: Bus voltages	26
Figure 5: SLD of Zeeland distribution network	27
Figure 6: Cypriot digital twin architecture	29
Figure 7: Grafana monitoring interface	32
Figure 8: French Digital Twin Architecture	37
Figure 9: The representative MV distribution grid.	43
Figure 10: Experimental results over a 24-hour horizon	46
Figure 11: Multiplicative attack at the substation measurement.	49
Figure 12: Multiplicative attack at the voltage measurement with a factor 0.95.	50
Figure 13: Multiplicative attack at the voltage measurement at Bus 9 with a factor 1.05.	51
Figure 14: Multiplicative attack at BESS 3 active power setpoint.	52
Figure 15: Bus voltage angles and total loads.....	55
Figure 16: RoCoF protection tripping of NDR380_generator	56
Figure 17: RoCoF protection tripping of GNA380 generator	56
Figure 18: Loading shedding and load disconnection of Dutch network	57
Figure 19: Line tripping caused by overloading	57
Figure 20: SLD of Dutch network blackout region	59
Figure 21: Bus voltage angles and total load	59
Figure 22: RoCoF tripping of GNA380 generator	60
Figure 23: Under voltage tripping of IC_Cobra	60
Figure 24: Over frequency tripping of EEM15_3 generator	61
Figure 25: SLD of Dutch network blackout region caused spoofing cyberattack	63
Figure 26: Bus voltage angles and total load caused spoofing attack	63
Figure 27: Over frequency tripping of DIM15 generator	64
Figure 28: Over frequency tripping of wind plant BSL3_4	64
Figure 29: Over frequency tripping of wind plant BSL380	65
Figure 30: Training Session Lobby.....	68
Figure 31: Session Creation Interface	68
Figure 32: Game Master View of the Simulated Substation.....	69

Figure 33: Trainer opens the breaker of two transformers	70
Figure 34: Trainee View	70
Figure 35: Trainee SCADA view during the overload scenario	71
Figure 36: Topological remedial action through busbar-coupler opening	71
Figure 37: DSL Commands	72
Figure 38: Loss of observability event injected through DSL.....	72
Figure 39: Use of DSL function to reduce generation output with a ramp	73
Figure 40: Generation reduction as an alternative remedial action.....	74

List of Tables

Table 3-1: Total number of buses in each zone	23
Table 3-2: Type and number of energy sources	23
Table 3-3: Load flow information.....	24
Table 3-4: Protection schemes implemented in the Dutch	27
Table 5-1: MILP model parameters	44
Table 6-1: Sequence of events during switching cyberattack	55
Table 6-2: Sequence of events during sequence switching cyberattack	58
Table 6-3: Sequence of event caused by spoofing cyberattack.....	62

List of Abbreviations and Acronyms

Acronym	Meaning
AI	Artificial Intelligence
API	Application Programming Interface
ASAI	Average Service Availability Index
AVR	Automatic Voltage Regulator
BESS	Battery Energy Storage Systems
CBM	Condition-Based Monitoring
DERs	Distributed Energy Resources
DG	Distributed Generation
DoS / DDoS	(Distributed) Denial-of-Service
DSL	Domain-Specific Language
DSO	Distribution System Operator
DT	Digital Twin
EENS	Expected Energy Not Supplied
EMS	Energy Management System
EMT	Electromagnetic Transient
ESP	Electrical Sustainable Power
ESS	Energy Storage System
EVs	Electric Vehicles
FDI	False Data Injection
GUI	Graphical User Interface
HIL	Hardware-in-the-Loop
HILF	High Impact, Low Frequency
HILP	High Impact, Low Probability
HV	High Voltage
HVDC	High-Voltage Direct Current
IT	Information Technology
KPI	Key Performance Indicator
LFC	Load Frequency Control
LOLE	Loss of Load Expectation
MILP	Mixed-Integer Linear Programming
MV	Medium Voltage
OT	Operational Technology
PV	Photovoltaics
RES	Renewable Energy Sources
RoCoF	Rate of Change of Frequency
RTS	Real-Time Simulator
RTUs	Remote Terminal Units
SAIDI	System Average Interruption Duration Index
SAIFI	System Average Interruption Frequency Index
SCADA	Supervisory Control and Data Acquisition
SE	State Estimation
SLD	Single Line Diagram
SMTP	Simple Mail Transfer Protocol
TCP	Transmission Control Protocol
TSO	Transmission System Operator

Executive Summary

This deliverable investigates how digital twin technologies can be used to assess and enhance the cyber and physical resilience of modern power systems under increasingly complex operating conditions. The work brings together three complementary Digital Twin implementations developed within the TwinEU project, covering transmission-system cyber security assessment (Netherlands), distribution-system resilience and flexibility management (Cyprus), and operator training under cyber-physical conditions (France). Collectively, these demonstrators provide a comprehensive assessment of how digital twins can support secure, reliable, and resilient operation of future power systems with high penetration of renewable energy sources and increasing reliance on digital technologies.

The Dutch digital twin was developed to evaluate the impact of cyberattacks on a large-scale transmission network with high renewable energy penetration and multiple international interconnections. Several cyberattack scenarios, including coordinated switching attacks and controller spoofing attacks, were simulated to assess their ability to trigger cascading failures and large-scale blackouts. The results demonstrate that cyberattacks targeting a limited number of assets can rapidly propagate throughout the transmission system, causing transmission-line overloads, uncontrolled islanding, generator disconnections, and widespread supply interruptions. Coordinated switching attacks resulted in approximately 36% load loss, while sequential switching attacks produced approximately 48% load loss. Even more severe consequences were observed in spoofing attacks, where malicious manipulation of control setpoints led to approximately 80% load loss and near-total blackout conditions. A particularly important finding was the identification of a “point of no return”, beyond which conventional protection and corrective control actions were no longer capable of preventing system collapse. These results demonstrate the importance of preventive cybersecurity measures and highlight the capability of digital twins to identify vulnerabilities and analyse cascading-failure mechanisms before they occur in real systems.

The Cypriot digital twin focused on a medium-voltage distribution network with high photovoltaic penetration and battery energy storage systems (BESS). A real-time hardware-in-the-loop environment was developed to evaluate advanced congestion-management and voltage-regulation strategies based on coordinated flexibility activation. The proposed optimisation-based controller coordinated four BESS units and successfully maintained substation loading within the imposed 2 MVA operational limit, even under conditions where uncontrolled operation resulted in loading levels of up to 3.5 MVA. In addition, bus voltages were maintained within permissible limits throughout the examined operating horizon. These results demonstrate the effectiveness of coordinated active and reactive power control for managing congestion and voltage violations in future renewable-rich distribution networks.

The Cypriot digital twin was also used to investigate the cyber resilience of optimisation-based control schemes through multiple false-data injection and command-injection attacks. The results showed that relatively small manipulations of measurements and control signals can lead to significant physical consequences. For example, corruption of the substation measurement caused the controller to underestimate network loading, resulting in actual loading levels of approximately 2.4 MVA, exceeding the operational limit despite the controller believing that the system remained within constraints. Similar attacks on voltage measurements produced undetected voltage violations, while malicious modification of BESS setpoints resulted in inappropriate flexibility activation and inefficient use of available resources. These findings reveal an important efficiency-versus-robustness trade-off

in optimisation-driven grid control and demonstrate the critical importance of measurement integrity, anomaly detection, and resilient control architectures.

The French digital twin was developed as a cyber-physical training and validation environment for power-system operators. The platform combines dynamic power-system simulation, telecommunications modelling, SCADA emulation, and scenario orchestration capabilities within a common framework. A key achievement of the demonstrator is its ability to support realistic large-scale operator-training scenarios using transmission-system models comprising more than 6,000 electrical nodes and 13,000 lines and transformers. Demonstrated scenarios included transformer outages, overload management, topology reconfiguration, generation redispatch, and communication-network disturbances leading to loss of observability. The results showed that operator situational awareness and decision-making capabilities are strongly influenced by the quality and availability of operational information. Scenarios involving communication failures demonstrated that degraded observability can significantly affect decision-making even when the physical power system remains stable. Furthermore, the digital twin provides a valuable environment for testing and benchmarking advanced decision-support assistants and future human-AI collaboration approaches before deployment in real operational environments.

Across all three demonstrators, a common observation is that cyber and physical processes are tightly interconnected and must be assessed jointly. Disturbances introduced through communication networks, measurement systems, or control infrastructure can rapidly propagate into physical-system behaviour, while physical events can simultaneously affect cyber infrastructure and operator visibility. The digital twin environments developed within this work successfully captured these interactions and enabled the safe evaluation of scenarios that would be impractical, costly, or unsafe to reproduce on real power systems. The results confirm that Digital Twins can support resilience assessment, vulnerability identification, control-strategy validation, operator training, and cybersecurity evaluation within a unified cyber-physical framework.

Key Findings

- Coordinated cyberattacks on transmission networks can trigger cascading failures resulting in 36% to 80% load loss, depending on the attack type and affected assets.
- A clear “point of no return” exists during cascading failures, beyond which conventional corrective actions become ineffective.
- Coordinated dispatch of four BESS units successfully reduced substation loading from approximately 3.5 MVA to within the 2 MVA operational limit while maintaining acceptable voltage levels.
- Small falsifications of measurements or control commands can produce significant physical consequences, including overloads, voltage violations, and inefficient resource utilisation.
- Loss of observability and communication failures can significantly degrade operator awareness and decision quality even when the physical network remains operational.
- Digital twins provide a safe and effective environment for testing mitigation strategies, validating advanced control solutions, evaluating cybersecurity threats, and training system operators under realistic cyber-physical conditions.

Overall, the deliverable demonstrates that digital twins are a powerful tool for improving the resilience and reliability of future power systems. However, fully exploiting their potential requires stronger integration of cybersecurity mechanisms, enhanced data trustworthiness, resilient control architectures capable of tolerating uncertainty and malicious interference, and continuous operator

training under realistic cyber-physical conditions. The results establish digital twins as a key enabling technology for the secure operation of increasingly digitalised, decentralized, and renewable-based power systems.

1 Introduction

As the energy sector accelerates its transition towards decentralization, electrification, and decarbonization, power systems are becoming increasingly complex, data-driven, and cyber-dependent. This transformation, while essential for achieving climate and energy goals, presents new challenges for the resilience and reliability of grid infrastructures. Extreme weather events, high penetration of renewable energy sources (RES), and evolving cybersecurity threats are testing the ability of system operators to ensure uninterrupted, stable, and secure power delivery.

To address these challenges, digital twins (DTs) have emerged as a strategic enabler. A digital twin is a dynamic, real-time virtual representation of a physical system, capable of simulating, monitoring, and predicting its behavior under normal and contingency conditions. Within the WP5 of the TwinEU project, digital twin frameworks will be deployed in three national pilots, the Netherlands, Cyprus, and France to explore how these technologies can enhance both cyber and physical resilience in power systems.

This deliverable includes the outcomes of Task 5.2 and Task 5.3 and T5.5, focusing on the assessment of system performance and response to both operational stress and cybersecurity incidents and the effective training of power system control center personnel in case of complex and critical situations. Each national digital twin serves a different purpose:

- The Dutch digital twin focuses on high-fidelity transmission system modeling for analyzing cascading failures, protection schemes, and the impact of cyberattacks at scale.
- The Cypriot digital twin demonstrates real-time congestion management in a medium-voltage distribution grid, coordinating flexibility from distributed energy resources (DERs) such as BESS and PV systems, while also enabling cyber-resilience testing.
- The French digital twin supports training and decision-support functions for system operators, combining SCADA interfaces, cyber-physical simulators, and scenario-based exercises.

Together, these digital twin implementations offer a comprehensive view of how DTs can support the planning, operation, and protection of future power systems.

1.1 Tasks 5.2, 5.3, and 5.5

This deliverable summarizes the outcomes of three tasks within the WP5 of the TwinEU project, Task 5.2, Task 5.3, and Task 5.5, each contributing to the development, simulation, and validation of digital twin frameworks for assessing cyber and physical resilience of power systems. While each task addresses different aspects of resilience and reliability, they collectively explore how digital twins can support secure and stable grid operations under extreme or uncertain conditions. Below a summary of each task scope is provided.

Task 5.2: Digital Twin for Cybersecurity of Cyber-Physical Systems with High Penetration of RES

Task 5.2 focuses on the development of an operational digital twin of the power system with a high share of renewable energy sources (RES), specifically targeting cybersecurity assessment. The digital twin is deployed within the Electrical Sustainable Power (ESP) Lab in Delft and is powered by TenneT system data. In this task, advanced cyberattack scenarios are simulated in real time, including false data injection and coordinated intrusions, to study their cascading impact on system stability.

Task 5.3: Scenarios for Assessing the Cyber and Physical Resilience of the Grid

Task 5.3 builds on the Cypriot MV digital twin to explore "what-if" scenarios for reliability assessment and cyberattack scenarios for resilience assessment. These scenarios are designed to test the power grid's response to both physical disturbances (e.g. increased RES penetration, congestion, or voltage instability) and cybersecurity threats. The digital twins simulate these situations using real and forecasted data, evaluating the system's ability to maintain service continuity and operational integrity.

Task 5.5: A Power System Training Simulator for Complex and Critical Situations

Task 5.5 introduces a training-oriented digital twin designed to support operator decision-making in complex and critical system conditions. This simulator which will be developed as a part of the French demo combines several technical modules:

- A cyber-physical simulator built with Dynawo and Dynaflo for modeling power system dynamics
- A SCADA and telecommunications network simulator to represent realistic grid operations and data exchange
- A game master module for generating interactive, closed-loop scenarios

The training environment aims to prepare operators for real-time responses under high stress or threat situations, evaluate human-machine interactions in managing cascading failures and cyberattacks, and foster the discovery of new preventive and curative operational strategies

1.2 Objectives of the Work Reported in this Deliverable

The primary objective of this deliverable is to assess the **cyber and physical resilience** of power systems through the development, simulation, and validation of digital twin (DT) frameworks under a variety of operational and adversarial scenarios. Specifically, the work presented aims to:

- **Develop and deploy digital twins** of both transmission and distribution networks to support real-time simulation, control testing, and scenario analysis under realistic conditions.
- **Evaluate the impact of cyber threats** such as false data injection and man-in-the-middle attacks on system stability, control efficiency, and the integrity of monitoring and communication layers.
- **Design and simulate "what-if" operational scenarios** involving future grid conditions, extreme operating states, and high penetration of RES, to assess the system's ability to handle physical stress (e.g., congestion, instability).
- **Demonstrate real-time coordination of flexibility resources** (such as BESS and controllable DERs) through hardware-in-the-loop (HIL) integration with the digital twin to relieve congestion and maintain voltage stability in distribution networks.
- **Quantify resilience and reliability performance using defined KPIs**, including metrics related to overload reduction, voltage compliance, control responsiveness, communication reliability, and response to cyber incidents.
- **Develop and apply a cyber-physical training simulator** for power system operators, allowing for immersive, scenario-based training and decision-making under complex, critical, and potentially compromised conditions.

1.3 Outline of the Deliverable

Chapter 1 introduces the context, objectives, and scope of the work, including a description of the tasks addressed in this deliverable. Chapter 2 provides the conceptual foundation by discussing cyber and physical resilience and reliability in power systems, highlighting key challenges and introducing the role of digital twins in supporting resilience assessment. Chapter 3 presents the developed digital twin frameworks across the Dutch, Cypriot, and French implementations, describing their architectures, modelling approaches, and capabilities for real-time simulation, control, and training applications.

Chapter 4 outlines the methodology for the development of operational and cybersecurity scenarios across the three digital twin environments. Chapters 5 and 6 then analyse the impact of stressed physical conditions and cyberattacks on system performance through detailed case studies at both distribution and transmission levels, including lessons learned and recommendations. Chapter 7 presents the development and application of the training-oriented digital twin, focusing on operator training under cyber-physical conditions. Finally, Chapter 8 concludes the work by providing key insights, recommendations, and perspectives on the role of digital twins in enhancing grid resilience.

1.4 How to Read this Document

This document builds upon previous work within the TwinEU project and is best understood in conjunction with Deliverables D2.2 [1] and D5.1 [2]. Readers interested in the broader digital twin (DT) concept, stakeholder requirements, and the overall TwinEU architecture are encouraged to consult D2.2, particularly the sections on the DT concept and TwinEU approach (Chapter 3), pilot technologies and technical requirements (Chapter 4), and use case definitions and KPIs (Chapter 5), which provide the conceptual and methodological foundation for the DT implementations analysed here. For a detailed understanding of the technical development of the DTs used in this work, including cybersecurity threat modelling, architectures, and early implementation results, D5.1 is particularly relevant. Specifically, Chapters 2 and 3–6 of D5.1 describe the cyber-physical threats considered, the design and development of the DT frameworks across Tasks 5.2, 5.3, and 5.5, and the initial validation activities, which directly underpin the simulations and analyses presented in this document. Together, these deliverables provide the necessary context to interpret the results and insights derived from the resilience assessment performed in this work.

2 Cyber and Physical Resilience and Reliability in Power Systems

This section provides an overview of the key concepts of resilience and reliability in power systems, focusing on their role in maintaining secure and stable operation and supply during day-to-day operation as well as during unexpected contingencies. It distinguishes the role of resilience, which concerns the system's ability to withstand and recover from high impact, low probability events (HILP), and reliability, which focuses on providing a continuous and stable electricity supply during normal operation and under routine disturbances. This section also outlines the main challenges in ensuring resilience and reliability in power systems, including the impact of extreme weather, cybersecurity risks due to the growing digitization of power grid and the increasing complexity of modern power systems with high penetration of distributed generation and increased load. Finally, it highlights the contribution of digital twins as a practical tool for supporting resilience and reliability assessment through scenario analysis to assist in decision-making.

2.1 Definition of Resilience and Reliability

2.1.1 Power System Resilience

Power system resilience is generally defined as the system's ability to predict extreme events, maintain critical operations during such disruptions, being able to rapidly recover from them and adapt its operation and structure by gaining lessons, in order to be more well-prepared for similar scenarios in the future [3], [4].

According to CIGRE WG C4.47, "Power system resilience is the ability to limit the extent, severity, and duration of system degradation following an extreme event" [3]. Resilience, unlike reliability, which is discussed later, is concerned with addressing more unpredictable and high-impact events, such as natural disasters (earthquakes, floods etc.) or cyberattacks, capable of causing multiple faults on the network and resulting in the disconnection of customers for long periods of time. These scenarios are often characterized as high impact, low frequency (HILF) [3] or high impact, low probability (HILP) events [4].

Further, resilience is typically evaluated using two metrics, namely qualitative (attribute-based) and quantitative (performance-based). Qualitative metrics focus on intrinsic system characteristics that describe its resilience relative to other systems. These include robustness, recoverability, adaptability and resourcefulness, and are applied by reviewing the system and noting which attributes are present. However, these metrics usually offer just a broad understanding of the system's resilience but lack precision, because they rely on expert judgement and assessments rather than data [3].

On the other hand, quantitative metrics aim to assess the system's resilience using data-driven performance indicators. These include factors such as outage duration, energy not served, number of disconnected customers and financial consequences due to damaged infrastructure and interrupted energy sales. Unlike qualitative metrics, they provide a more objective resilience assessment based on data and metrics, but their accuracy depends on the availability of historical data and how precisely the system behavior can be modeled during extreme events [3].

Ensuring power system resilience is especially important now because of the increasingly frequent and severe natural disasters, mainly due to the continuously unfolding consequences of climate change [5]. Figure 1 illustrates the increased frequency of extreme climatic events in recent years, highlighting the need to certify that power systems are capable to handle such events with minimal impact on its performance while also ensuring a swift recovery.

In addition, the increasing digitization of power systems has introduced new vulnerabilities, making cyber resilience more critical than ever. Modern grids rely heavily on IT and telecommunication networks for real-time monitoring, control, and automation, but this also increases their exposure to cyber threats. The increase in cyberattacks targeting power infrastructure, including incidents like the 2015 Ukraine blackout, highlights the risks posed by these vulnerabilities. As grids become more interconnected and data-driven, resilience must incorporate **cyber resilience**, defined as the capability to limit the extent, severity, and duration of system degradation following cyber-related events. Achieving this requires stronger risk assessment, enhanced system monitoring, and faster response measures to mitigate the impacts of cyber incidents effectively [3].

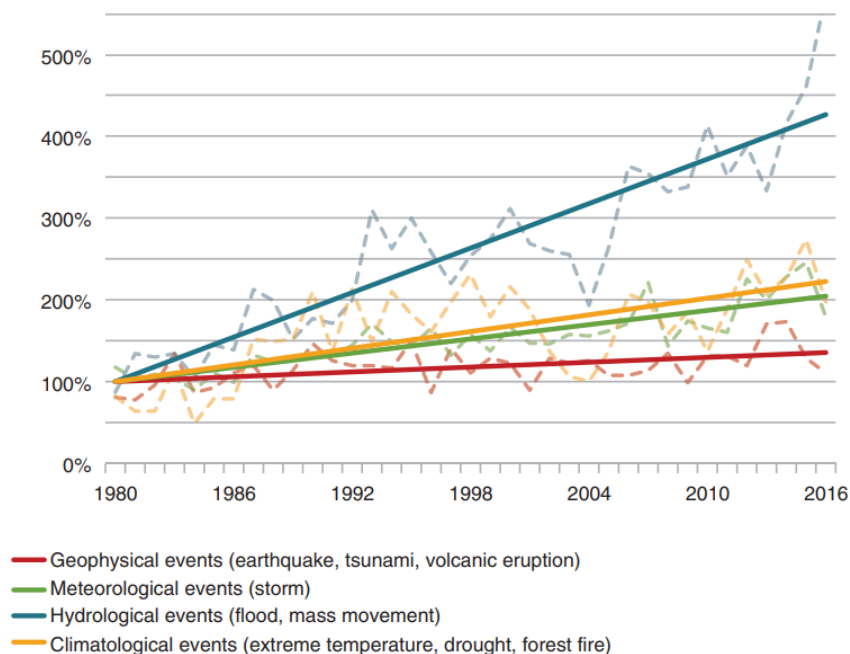


Figure 1: Increasing frequency of extreme events worldwide (1980 levels are set at 100%) [6].

Resilience can be further divided into infrastructure resilience and operational resilience. Infrastructure resilience involves any actions taken to harden the network's infrastructure. This involves a long-term timeline that includes the investment, planning, design and commissioning aspects that are considered during this process and take place before an extreme event occurs [3]. Examples of infrastructure hardening measures include the use of stronger materials for transmission and distribution towers and lines and burying essential transmission corridors underground to protect against harsh weather conditions [4].

On the other hand, operational resilience refers to the system's resilience much closer to an extreme event, covering both the pre-fault and post-fault conditions until the system has recovered. At this stage, mitigating measures can be performed almost in real-time and as the event unfolds. This is done to provide operational flexibility and increased responsiveness to allow for higher control and enable corrective actions to be taken to mitigate the impact of the event as it is happening [4].

Specifically, operational resilience involves a four-step approach that helps system operators manage extreme events while minimizing disruption. It begins with anticipation and preparation, where potential threats are identified using forecasting tools to support proactive measures like generation re-dispatch and resource allocation [4]. During an event, the focus shifts to absorption and mitigation, relying on system flexibility, demand-side management, distributed generation and adaptive protection schemes to limit damage and maintain supply to critical services. This is followed by restoration, where automated systems and prioritization of essential loads enable a swift return to normal operation. Finally, the system adapts by analysing performance during the event, implementing improvements, and using simulation-based training to enhance preparedness for future disruptions [3].

2.1.2 Power System Reliability

Power system reliability is defined as the ability of the system to continuously supply electricity to consumers while maintaining the required quality and performance standards. It is generally divided into adequacy, which ensures that sufficient generation and transmission capacity is available to meet demand under normal operating conditions, and security, which refers to the system's ability to withstand sudden disturbances such as faults, equipment failures, and load or renewable energy output fluctuations [7].

Reliability is typically assessed using probabilistic and deterministic methods, through the use of indices such as Loss of Load Expectation (LOLE), Expected Energy Not Supplied (EENS), and System Average Interruption Duration Index (SAIDI) to quantify system performance [8]. The increasing penetration of power electronics and renewable energy sources has introduced new challenges in reliability assessment, as traditional models often do not fully capture the dynamic behavior of inverter-based generation or cyber-physical interactions within modern grids [7].

Reliability is influenced by various factors, including system design, the integration of renewable energy sources, and the performance of power electronic components. With the increasing use of power electronics in modern grids, challenges such as component wear-out, electromagnetic interactions, and reduced short-circuit capacity have become critical reliability concerns [7]. Additionally, distributed generation (DG) and microgrid integration introduce new complexities in reliability assessment, requiring advanced control strategies for power balancing and protection coordination [8].

Even though reliability and resilience are often used interchangeably, they address different aspects of power system performance. Reliability focuses on maintaining normal operation during high-probability, low-impact events that usually have limited impact. In contrast, as mentioned earlier, resilience is concerned with unexpected high-impact, low-probability (HILP) events that can lead to significant damage to network infrastructure.

2.2 Key Challenges

2.2.1 Key Challenges in Ensuring Resilience

Ensuring operational resilience in power systems comes with several challenges, particularly as grids become more complicated and exposed to a broader range of disruptive events compared to before. One of the key issues is the increasing frequency and severity of natural disasters, mainly because of climate change [3]. Extreme events such as wildfires, earthquakes, storms and floods are

occurring more often and with greater intensity, causing severe damage to the network's infrastructure and affecting consumers. Even though contingency plans are in place for when a natural disaster occurs, as these events worsen, many systems may find it hard to cope with, especially when facing multi-event disturbances where multiple failures occur across the grid at the same time [3].

Moreover, another major challenge is cybersecurity, since the growing digitization of power systems has made them more vulnerable to cyberattacks [3]. Modern power systems are becoming heavily dependent on automation, control and communication through IT infrastructure, making ensuring protection against cyber threats vital for the system's stability and smooth operation. The increasing use of Supervisory Control and Data Acquisition (SCADA) systems, Energy Management Systems (EMS), and remote monitoring technologies have improved grid efficiency and responsiveness but has also introduced new vulnerabilities[1]. A cyberattack on these systems can compromise control functions, disrupt grid stability, and even lead to widespread blackouts. Unlike physical threats, which are usually localized and have a clear recovery path, cyber intrusions can spread rapidly, remain undetected for extended periods, and affect multiple layers of the grid's infrastructure [3].

One example of this is 2015 Ukraine cyberattack. During this attack, hackers gained unauthorized access to control systems, manipulated circuit breakers, and intentionally cut power to nearly 250,000 consumers. The attackers also disabled backup systems, making recovery more difficult and prolonging the outage. This event demonstrated how cyber threats can cause real-world disruptions and emphasized the need for stronger cybersecurity frameworks, real-time monitoring, and faster incident response strategies. One of the challenges in managing cyber resilience is that network operators often lack full visibility regarding potential threats. Many utilities rely on conventional IT security measures that focus on protecting corporate networks but may not be sufficient for Operational Technology (OT) systems, which are utilized to control physical grid infrastructure. SCADA and EMS systems were not originally designed with cybersecurity in mind, meaning they usually lack robust encryption, multi-factor authentication, or real-time intrusion detection. As a result, attackers can exploit software vulnerabilities or unpatched systems to gain unauthorized access to critical grid operations [3].

Another concern is the possibility of coordinated cyber-physical attacks, where cyberattacks coincide with infrastructure disturbances such as severe weather events or equipment failures. For instance, an attacker could target a substation's protection relays or disrupt communication between grid control centers during a natural disaster, making the situation much harder to manage. Such combined threats require more advanced risk assessment frameworks that integrate cybersecurity considerations into operational resilience planning [3].

Moreover, operator training and emergency preparedness must constantly improve to stay up to date with evolving threats faced by the network. Current training programs do not fully cover cyber-physical threats, leaving operators unprepared and systems vulnerable to such hybrid attacks. This once again highlights the need for emergency scenarios and simulations to improve the operators' performance and enhance their decision-making abilities under stress so that they can perform as required during contingencies.

Interestingly, the absence of regulatory and policy frameworks also poses a challenge, since there is no standardized approach to define and enforce operational resilience in power systems. Existing regulations primarily focus on reliability instead, meaning that they do not address high impact, low

frequency events and their consequences. In fact, according to a survey, only about 42% of countries that participated have regulations specifically targeted on operational resilience, creating gaps in preparedness and leaving the system vulnerable to events that pose significant threat to its operation.

2.2.2 Key Challenges in Ensuring Reliability

The increasing integration of power electronics and renewable energy sources (RESs) is reshaping power systems, introducing new reliability challenges. Unlike conventional, centralized networks, modern grids rely more on distributed generation, microgrids, and digital control systems, all of which add complexity to system operation and planning [7].

One of the key challenges is microgrid operation. While microgrids improve local reliability by enabling islanded operation, they also introduce new technical requirements. Maintaining a stable balance between generation and demand in an islanded system is more difficult, especially when relying on RESs with variable output. In addition, microgrids depend heavily on information and communication technologies (ICTs) for real-time monitoring and control, making them more susceptible to cyber threats, hardware failures, and data loss. As power systems become more digitized, the risk of cyberattacks disrupting grid stability is increasing [7].

Moreover, the widespread adoption of RESs further complicates system reliability. Solar and wind power introduce uncertainty due to their variable output, which impacts conventional reliability assessment methods that were originally designed for dispatchable generation in the conventional power grid. Managing supply-demand imbalances requires improved forecasting, enhanced system planning, and new approaches to frequency regulation, especially since replacing synchronous generators with inverter-based RESs reduces system inertia [7].

Another major factor affecting reliability is the growing reliance on power electronic converters. These devices are essential for integrating RESs, enabling high-voltage direct current (HVDC) transmission, and supporting flexible grid operation, but they also introduce new stability concerns. Interactions between power converters, passive components, and mechanical systems can lead to resonance, voltage instability, and unpredictable system behavior. Unlike synchronous generators, converters have limited short-circuit current capability, making overcurrent protection methods less effective, particularly in microgrid and inverter-dominated networks. This creates the need for adaptive protection strategies that take into consideration the evolving grid structure [7].

In addition, Energy Storage System (ESS) sizing is another critical factor. Over-sizing an ESS leads to unnecessary investment costs, while under-sizing may result in inadequate energy storage capacity, limiting its ability to support grid operations. Several approaches have been proposed to optimize ESS sizing, including methods that consider factors like renewable energy curtailment, grid resilience, and cost-effectiveness [9].

Moreover, the increasing electrification of the transportation sector, particularly through the adoption of electric vehicles (EVs), introduces several challenges for power system reliability. As EV penetration grows, the additional electricity demand from charging infrastructure places new stresses on power networks, requiring enhancements in grid flexibility, energy storage, and demand-side management [9]. One of the primary concerns related to this is the rise in electricity demand caused by the widespread deployment of EV charging stations. Fast-charging infrastructure, especially in urban areas, can lead to localized grid congestion, voltage instability, and peak load issues. The intermittent and unpredictable nature of EV charging patterns makes load forecasting and demand-

side management more complex [9]. The intermittent participation of EVs in grid services also introduces uncertainty in power system planning, making it difficult to rely on them as a stable energy resource [7].

Furthermore, the integration of HVDC technology, which is becoming more prevalent in modern power systems, poses several challenges. HVDC failures can cause severe power imbalances in interconnected systems, as there is fewer alternative transmission paths compared to AC networks. If an HVDC link goes offline unexpectedly, the receiving end may experience sudden power imbalance, leading to frequency instability. Contingency planning and redundancy measures are essential to mitigate these risks [10]. Also, unlike AC transmission, where synchronous generators inherently contribute inertia, HVDC systems rely on power electronics that do not provide natural inertia. This makes frequency control more challenging, especially in grids with high-RES penetration.

Aging transmission and distribution infrastructure is another major challenge affecting power system reliability. Many power networks were designed decades ago and now operate beyond their intended lifespan, increasing the probability of component failure, unplanned outages, and reduced system efficiency [8]. As equipment ages, issues such as insulation degradation in transformers, corrosion in overhead lines, and mechanical wear in circuit breakers become more frequent, leading to higher maintenance costs and system downtime. This impact of aging infrastructure is further magnified by increasing electricity demand and the integration of new generation sources. Traditional grid components were not designed to accommodate high levels of intermittent renewable generation, leading to compatibility issues that can affect system stability and reliability [8]. To address this, utilities must implement condition-based maintenance (CBM) and predictive analysis to identify potential failures before they occur.

2.3 Role of Digital Twins in Resilience and Reliability Assessment

Digital twins (DTs) are increasingly used to assess and improve the resilience and reliability of power systems by integrating real-time data, advanced simulations, and predictive analysis. Unlike conventional reliability models, DTs provide a dynamic representation of the grid, which allows operators to analyze and respond to disruptions more effectively.

According to work in [11], digital twins facilitate resilience by creating realistic simulations of cyber incidents, allowing operators and organizations to improve their situational awareness. By simulating incidents in a controlled, virtual environment, it is possible to validate the effectiveness of cybersecurity measures, refine incident management procedures, and improve response times during real cyber-attacks. An essential aspect of this framework involves using digital twins to build situational awareness and support a common operational picture, creating a common understanding of the system's condition for all interested parties. The integration of these capabilities within digital twins provides a powerful tool for scenario planning, anomaly detection, and training of personnel, significantly reducing response times and limiting the impact of cyber-attacks. Additionally, DTs provide a valuable platform for learning within organizations and utilities, enabling operators to refine and improve contingency strategies based on insights gained from simulated events.

Furthermore, in [12], digital twins are utilized to model a distribution system through the use of electromagnetic transient (EMT) simulations along with realistic models of the communication network. Specifically, this study addresses how DTs can enhance the resilience of power distribution systems, particularly those incorporating distributed energy resources (DERs), such as solar PV and

battery energy storage systems (BESS). In their research, which involves the Virginia Tech Electric Service, the digital twin simulates both the electrical and cyber layers of the distribution network, providing a realistic environment for cybersecurity testing, including simulations of advanced cyber threats like coordinated denial-of-service (DoS) attacks. This dual-layer DT model enables operators to identify vulnerabilities, evaluate potential impacts of cyberattacks on physical infrastructure, and develop and validate comprehensive resilience plans. Additionally, this DT framework supports innovative machine learning-based methods for intrusion detection, enabling utilities to identify and mitigate cyber threats proactively. Overall, their approach demonstrates that DTs significantly contribute to resilience enhancement by providing detailed simulations for critical scenarios and helping distribution networks quickly recover service during and after disruptive events and adapting their real-world response strategies based on simulation results.

In [13], the integration of digital twin technology in distribution networks enables a more effective reliability assessment by shifting from traditional, post-event evaluation of the system's performance to real-time and predictive analysis. Instead of relying solely on outage data, the digital twin replicates the real-time state of the network, incorporating grid topology, equipment parameters, switch status, and load data. This allows for continuous calculation of reliability indices such as SAIFI, SAIDI, and ASAI, enabling earlier identification of weak areas across the network.

Beyond real-time assessment, the system also supports forecasting and planning. Through data-driven modelling and holographic visualizations, areas with reduced reliability can be clearly highlighted, helping operators perform more targeted improvements and maintenance. The digital twin framework also allows for quick evaluation of different operational scenarios, quantifying the potential impact of changes like switching configurations or equipment upgrades. Practically, this results in more targeted reliability improvement efforts and supports a more resilient and well-managed distribution network.

Furthermore, digital twins provide a powerful framework for evaluating new components and testing "what-if" scenarios in power systems without disrupting real-world operations. By creating a virtual replica of the grid, utilities can assess the performance of new equipment, such as transformers, protection relays, and power electronic devices before deployment through a hardware in the loop configuration. This approach allows for early identification of potential integration challenges, optimization of control parameters, and validation of performance under real-world operating conditions.

Overall, the findings of the above studies highlight the importance of digital twins as a valuable tool for resilience and reliability assessment, offering the ability to realistically simulate complex cyber-physical systems, test new methodologies and "what-if" scenarios, dynamically assess vulnerabilities and implement measures to mitigate their impact. Thus, digital twins offer a useful approach in modern power systems, addressing both cybersecurity concerns and ensuring continuous operation against different types of events.

3 Overview of Digital Twin Framework

This section presents an overview of the digital twin implementations developed under Tasks 5.2, 5.3, and 5.5, which were carried out in the Netherlands, Cyprus, and France respectively. Each digital twin was designed with a distinct focus, contributing to a comprehensive and multi-layered framework for assessing the reliability and resilience of power systems at both the transmission and distribution levels.

The Dutch and Cypriot digital twins focus on real-time simulation of the power grid under high renewable energy penetration and evolving operational conditions, with particular attention to congestion management, voltage stability, and cybersecurity threats.

Recognizing the critical role of human decision-making in mitigating severe physical or cyber contingencies, the French digital twin, developed in Task 5.5, serves as a training simulator for system operators. This environment enables immersive, scenario-based exercises that integrate cyber-physical dynamics, SCADA emulation, and real-time response simulations, supporting the development of more robust operational strategies.

3.1 Description of the Dutch digital twin

3.1.1 Introduction

Recognizing the challenge of developing separate digital twins for the transmission and distribution systems and their applications, Dutch pilot develops a unified, integrated digital twin for the manageability and effectiveness of DT applications. Due to the significant computational resources and limited access required to accurately depict the complete Dutch electrical power system, the task applies dynamic model reduction techniques. These methods are designed to refine the models, particularly to enhance details in key areas such as the integration points of significant variable renewable energy sources (RES). To achieve comprehensive system models, the partners in Dutch pilot collaborate closely, beginning with developing models for the transmission system. It will be followed by integrating dynamic, reduced models of the remaining system components, thereby providing a detailed and realistic presentation of the physical system. This involves using specialized equivalent models to effectively represent interconnections with adjacent networks, ensuring a cohesive and interconnected digital twin ecosystem. This task aims to understand the operational dynamics of future power systems, particularly in evaluating the impact of cyber-attacks and propose method to prevent the cyberattacks. This is crucial for ensuring the resilience and reliability of power systems against evolving cyber threats. The Dutch digital twin architecture is shown in Figure 2.

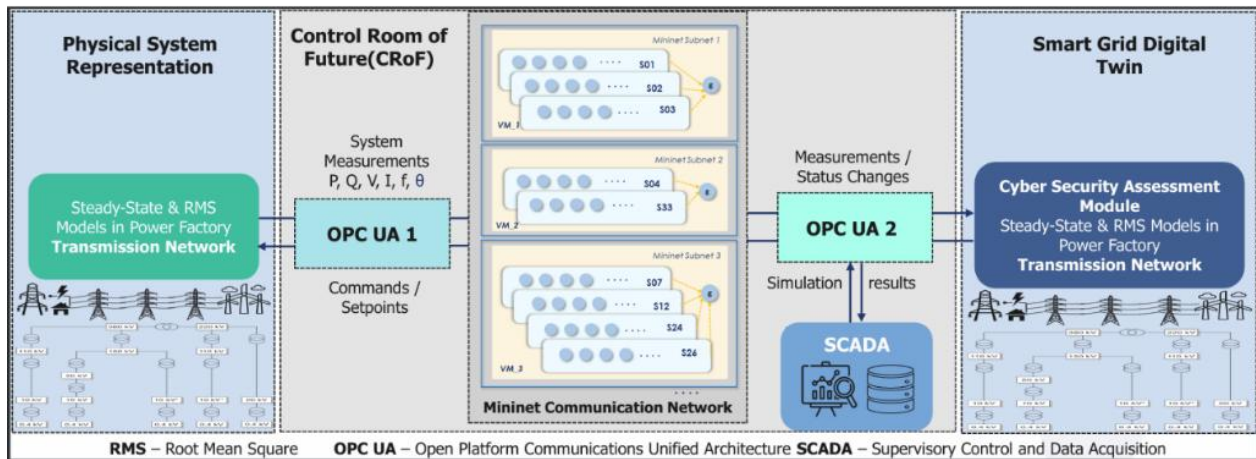


Figure 2: Cyber-physical digital twin framework for cybersecurity assessment.

3.1.2 Dutch Transmission model

The main focus of this task is to develop a digital twin for the power system with high penetration of RES for cybersecurity applications. Cyberattacks, leading to cascading failures and blackouts, will be simulated in real time on the operational digital twin. The analysis will focus on how cyberattacks can cause N-K contingencies, which impact power system stability and significantly accelerate reaching the point of no return. This can be achieved in the following steps:

1. Dynamic modelling of the Dutch transmission system
2. Modelling of the various protection schemes in the network
3. Studying the impacts of cyberattacks in the network and analysing the cascading events caused by the cyberattacks through N-K contingency
4. Analysing the cascading trend and differentiating between slow and fast cascades by quantifying the point of no return

For this analysis, the first and foremost part is the modelling of the Dutch transmission system. The synthetic model of the Dutch transmission network is in progress. The dynamic model of the Dutch transmission system includes various controllers with inverter-based resources, wind generation, and various protection schemes. The overall modelling of the Dutch system is explained below.

Zone: There are in total 16 zones in the Dutch transmission model, those are:

- | | |
|-------------------------|-------------------------------------|
| 1. Gelder Flevo Utrecht | 2. Groningen en Drenthe |
| 3. IC_BE_ELIA_VYK | 4. IC_BE_ELLIA_ZVL |
| 5. IC_DE_Amprion_HGL | 6. IC_DE_Amprion_NDR |
| 7. IC_DE_OBZ | 8. IC_DK_Cobra_EOS and EOS offshore |
| 9. IC_GB_BrittNet_MVL | 10. IC_NO_StattNet_EEM380 |
| 11. Limburg | 12. Noord_Brabant |
| 13. Noord-Holland | 14. Overijssel en Noordoostpolder |
| 15. Zeeland | 16. Zuid Holland |

All these zones have a voltage rating of 380 kV. Each interconnection point is considered a single zone in the model. The interconnectors in the zones are referred to as IC, with the second term in the zone name indicating the origin of the interconnection point along with the TSO operators, such as DE_Amprion, where "DE" represents Germany and the operator is Amprion. The last part of the interconnector zone names refers to different location points in the Netherlands. For example, IC_DE_Amprion_NDR refers to the interconnection line connecting to the Netherlands at point NDR from Germany, with the operator being Amprion. Similarly, the Denmark (DK) to Netherlands (NL) interconnector is referred to as IC_DK, the Norway interconnector as NO, Belgium as BE, and the British interconnector as GB. If the interconnection points are not considered as zones, then primarily eight zones are modelled in the network.

Buses: There is a total of 65 buses, including the generator buses. These buses have three different voltage ratings. The buses directly connected to generators have a voltage rating of 15 kV. Buses connected to static generators, such as wind plants, have a voltage rating of 0.69 kV. All remaining buses have a voltage rating of 380 kV in the model, obtained through step-up voltage transformers and voltage regulators.

Table 3-1: Total number of buses in each zone

Zones	Total number of buses in that zone.
Zuid-Holland	14
Zeeland	6
Overijssel en Noordoostpolder	3
Noord-Holland	6
Noord-Brabant	3
Limburg	3
Gelder Flevo Utrecht	5
Groningen en Drenthe	12

Generation: The entire network mainly has three types of power sources:

1. Synchronous machine generation
2. Wind power generation
3. Interconnection sources

The synchronous machines are primarily gas generation plants. The interconnectors include both HVDC and HVAC links; however, they are currently modelled as a combination of generation and load models to represent the dynamic behaviour of the interconnectors. In the next steps, these interconnectors will be remodelled with HVDC connection links.

Table 3-2: Type and number of energy sources

Type of Source	No. of sources
Gas Generation Synchronous plant	12
Wind plants	10
Interconnectors	9

Shunt Compensators: The network has two types of shunt compensators which support the reactive power demand in the grid and helps in maintaining the grid voltage levels within the specified threshold values. This shunt compensators are two types 1. Capacitive compensation (total 2 compensators) and 2. Inductive compensation (total 18 compensators).

Load: There are in total 30 loads, with these loads having different load profile. Some of the loads are consuming the active and reactive power from the grid and some of the loads are consuming active power from the grid and providing the reactive power supply to the grid. The loads classified into two types those are Electrolyser (Total 3 loads) and Conventional loads. The Electrolyser loads are modelled as the constant power loads and remaining all loads are modelled as the ZIP loads where active power represents the constant current and reactive power represents the constant impedance model dynamics.

Transformers, Lines: The Dutch transmission model network majorly have step up transformer whose secondary voltage is 380kV and primary voltage rating is 0.69kV/ 15kV depending upon the connection to the generation source. The network also connected with the step voltage regulators which are connected at the interconnection point to maintain the constant voltage throughout the network and avoid voltage fluctuations due to the power exchange by the interconnectors. One of the important components in the network is Transmission lines. There are in total 82 lines and these lines have different number of parallel lines in the network with different line length and various current ratings.

Steady State Model: The load flow analysis is performed on the developed model. The system voltage, frequency, and equipment loading are within the specified limits. The load flow equations converge within 2 iterations, indicating that the system is in a highly stable condition, as shown in the Figure 3. The total power generation and supply are as follows:

Table 3-3: Load flow information

	Generations	Load	Losses
Active power (MW)	24997	24885.5	111.5
Reactive power (Mvar)	-473.1	-1237.1	-249.3



Figure 3: Dutch transmission model

The standard voltage limit for extra high voltage transmission systems is typically around $\pm 5\%$, which means that the voltage must be between 0.95 p.u and 1.05 p.u. The Figure 4 shows that all bus voltages are within the specified limits. The complete dynamic model of the network with various controls, protection scheme will be modelled in the upcoming months.

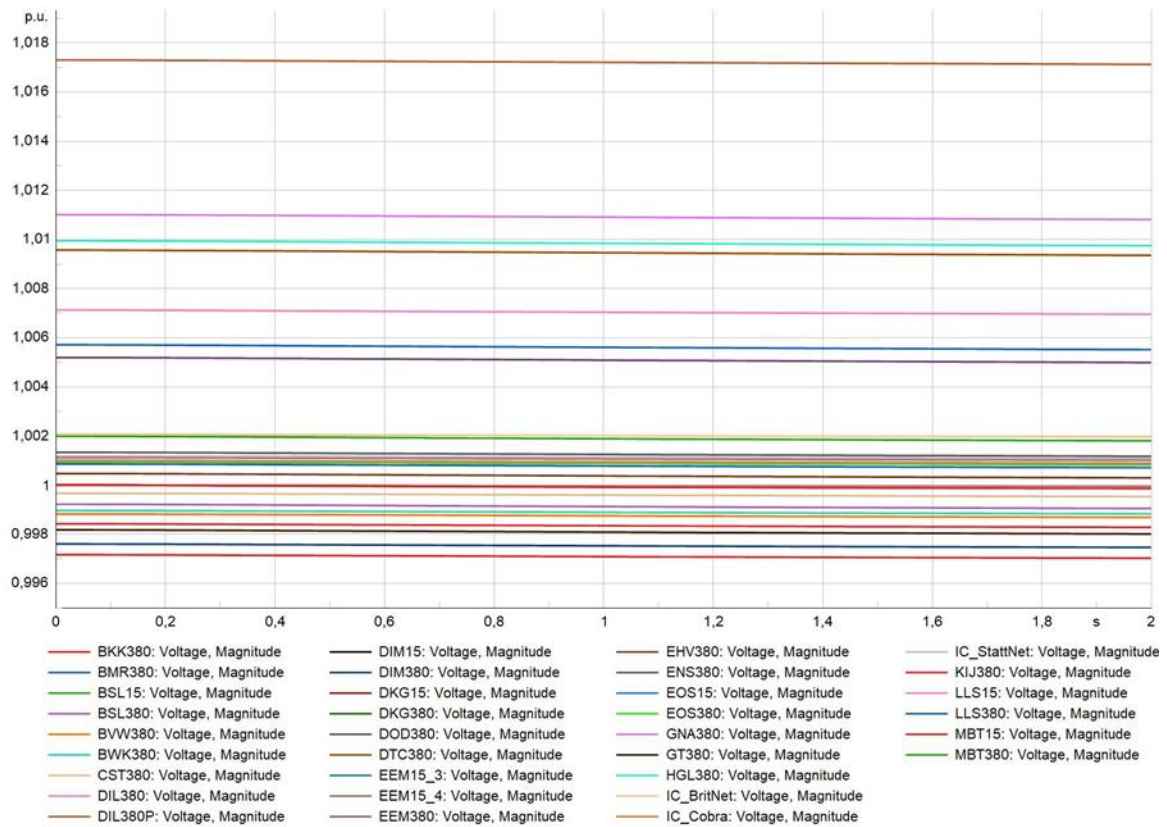


Figure 4: Bus voltages

3.1.3 Distribution network

The 380 kV transmission network is integrated with the Zeeland low-voltage distribution network. The network primarily comprises asynchronous generators, modelled as doubly fed induction generators (DFIGs) with appropriate DFIG control systems. The distribution network is configured as a ring-main distribution network with double busbar connections.

The Zeeland transmission network area is dynamically integrated with the distribution network and includes various control and protection schemes. For the development of coordinated protection mechanisms, relevant grid codes and standard protection practices have been considered. The generators are modelled with Automatic Voltage Regulators (AVRs), turbine governors (GOVs), and Power System Stabilizers (PSSs). For wind turbine dynamic modelling, the standard PowerFactory 2023 WECC Type 4A model is utilized. The asynchronous generators are modelled using DFIG grid controllers equipped with multiple control functions, including turbine, pitch, shaft, and speed controllers.

The SLD of the transmission network is shown in Figure 5. Various coordinated protection schemes have been implemented in the model, including over- and under-voltage protection, frequency protection, overflux protection, out-of-step protection, and Rate of Change of Frequency (RoCoF) protection for synchronous generators. The interconnectors are similarly equipped with frequency and RoCoF protection schemes. The wind plants also incorporate these protection functions along with voltage ride-through capabilities. The loads are equipped with under-voltage and under-frequency load-shedding protection schemes, while the transmission lines are primarily protected

using distance protection, with overload protection implemented as a backup. The implemented protection schemes are summarized in Table 3-4. All protection schemes implemented in the models are based on standard grid codes and established practices [14], [15]. Deviating from these standardized protection settings is not considered standard practice and can significantly affect cascading failure scenarios across different test cases. The overall details of the Dutch digital twin model and its architecture are extensively reported in Deliverable D5.1.

Table 3-4: Protection schemes implemented in the Dutch

Component	Protection scheme
Synchronous generator	Frequency, RoCoF, Voltage, Overflux, and Out of step
Asynchronous generator	Under-, over voltage, frequency
Interconnectors	Frequency, RoCoF, Voltage
Wind plants	Frequency, RoCoF, Voltage with ride through setting
Loads	Under voltage and Under frequency, load shedding
Lines	Distance and Overloading

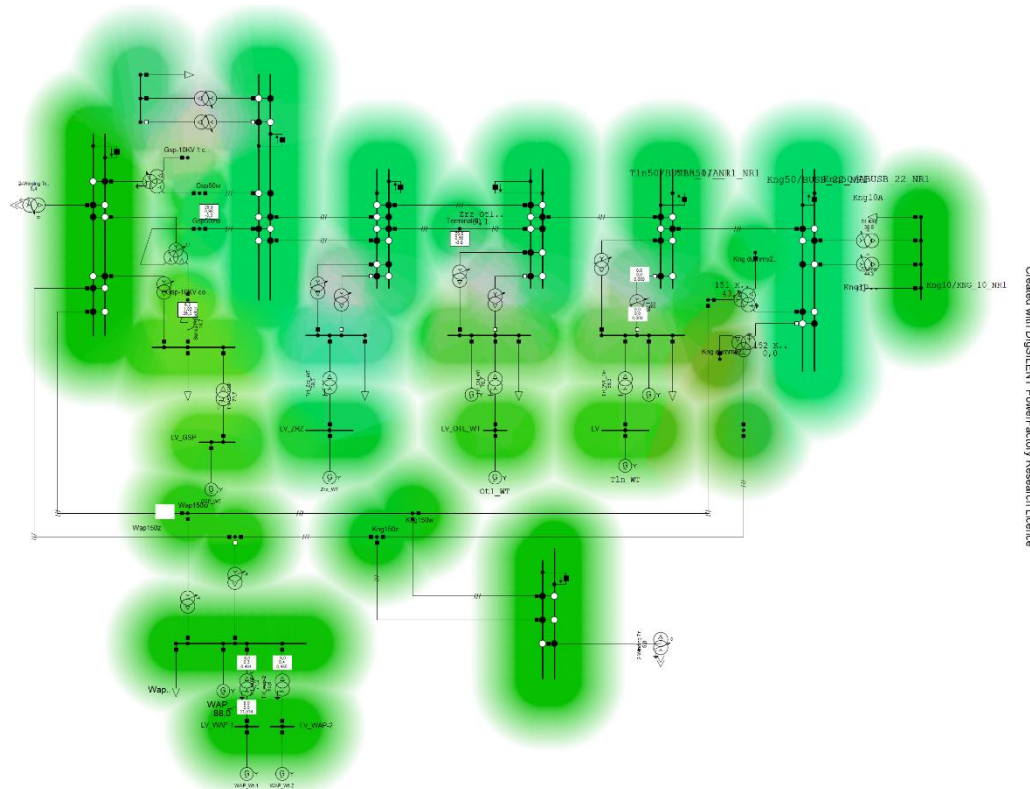


Figure 5: SLD of Zeeland distribution network

3.2 Description of the Cypriot digital twin

The Cypriot digital twin is designed to assess and enhance the cyber and physical resilience of the Cyprus power system under high penetration of Renewable Energy Sources (RES). In particular, the increasing deployment of Photovoltaic (PV) installations has led to localized congestion and voltage rise issues. To mitigate these challenges, Battery Energy Storage Systems (BESS) are utilized to provide flexibility services through advanced control algorithms. This demonstration not only highlights the

enhanced operational efficiency of the Cyprus power system under these control strategies but also evaluates potential cybersecurity threats and vulnerabilities.

Developed as part of Task 5.3, the Cypriot digital twin replicates the behavior of the real distribution network by integrating real grid data and measurements, real-time simulation environment, and hardware in the loop controller. Its primary objectives are to improve grid resilience, improve localized congestion, improve voltage management, and analyze cyber vulnerabilities through advanced modeling and scenario-based assessments. This section provides a comprehensive overview of the Cypriot digital twin architecture, data gathering methods, real-time simulation, data management, and reliability assessment.

3.2.1 Digital twin architecture

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 behavior 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, cybersecurity and mitigation measures.

A high-level diagram of the Cypriot digital twin architecture is shown in Figure 6. 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 30-second intervals to reflect real-time variability in solar generation.

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

- **Cybersecurity 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.

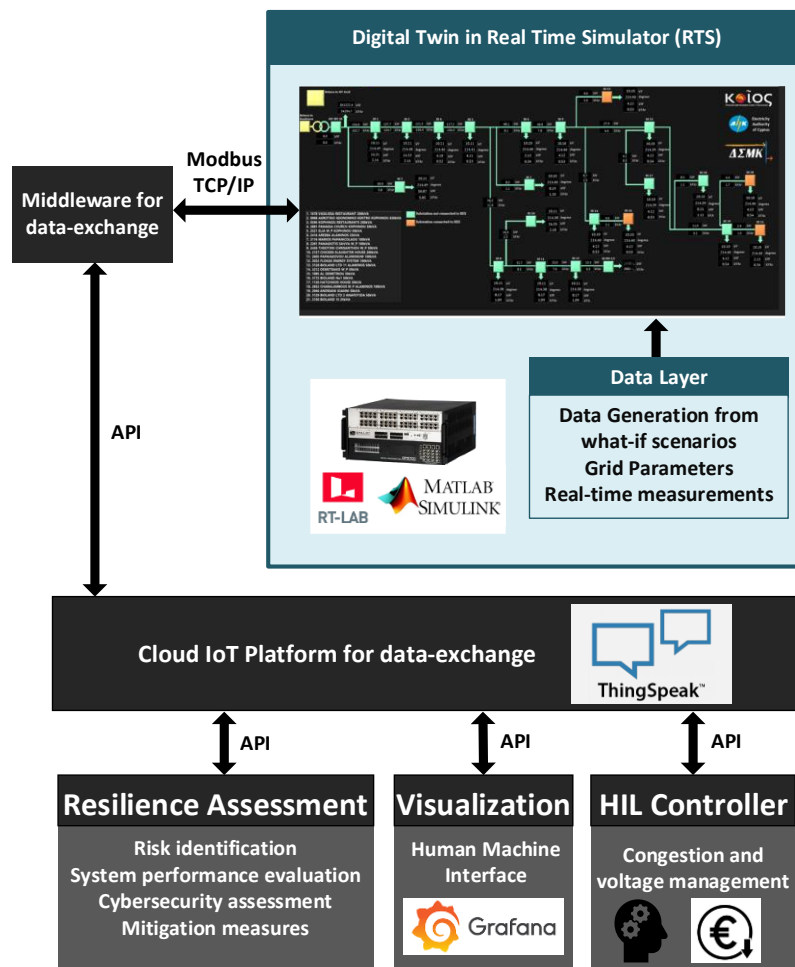


Figure 6: Cypriot digital twin architecture

3.2.2 Real time simulation model

Using the collected data, a detailed electromagnetic transient (EMT) simulation model of the medium-voltage (MV) distribution grid has been developed in MATLAB/Simulink. The model leverages components from the *Simscape Electrical* and *SimPowerSystems* libraries by MathWorks, ensuring a high-fidelity representation of the system's dynamic electrical behavior. To enable compatibility with the RTS and to capture fast transient phenomena, the simulation employs a fixed-step discrete solver with microsecond-level resolution.

The modeled MV network adopts a three-phase, three-wire configuration with a solidly grounded neutral at the high-voltage (HV)/MV transformer, and follows an open-ring topology. Distribution line parameters were sourced directly from the Electricity Authority of Cyprus (EAC), ensuring consistency with the real-world grid infrastructure. Electrical loads are represented as three-phase dynamic models, driven by pre-loaded timeseries of real measurements of active and reactive power or streamed in real-time via communication interfaces.

To achieve full observability, multiple virtual measurement devices are integrated into the MV network model. These devices monitor key electrical quantities, such as active power, reactive power, and voltage, at critical nodes across the grid. For example, measurement at the HV/MV transformer is essential for monitoring total power flow into the MV network and plays a vital role in congestion management. These real-time measurements serve two main purposes: they feed directly into the control logic to enable dynamic management of the grid, and they are also visualized through the digital twin's monitoring interface, supporting situational awareness and operator insights. This comprehensive setup ensures the simulation reflects system behavior accurately under various operational and contingency scenarios.

Detailed models of the PV and BESS units are implemented using grid-following inverters. These models include switching components, control systems, and communication interfaces to facilitate the exchange of control commands and monitoring data in real time. The PV controller supports $\cos\phi(P)$ functionality, enabling dynamic reactive power regulation to enhance local voltage management. Four PV systems are interfaced with the MV network through MV/LV transformers and four BESS units are also connected with the MV network using the same common coupling as the PV systems. This configuration allows for coordinated control of both active and reactive power, contributing to grid stability and flexibility under varying operating conditions.

To enable real-time simulation, the Opal-RT OP5 has been used, a cutting-edge multi-core simulation engine. The OP5707 is a multi-core computational engine enhanced with dedicated FPGA (field-programmable gate array) cards, providing high-speed processing and enabling precise modeling of complex power system dynamics. It is equipped with various peripherals, including analog and digital input/output cards, to facilitate seamless integration with external hardware devices and software applications. This setup allows for real-time digital twin modeling, enabling HIL configurations where the digital twin interacts dynamically with physical equipment or software-based applications, enabling comprehensive investigations such as distributed energy resource management, grid stability analysis, and cybersecurity resilience testing. For real-time operation, the simulation model of the MV distribution grid with the integrated PVs and BESS is adapted for the OPAL-RT platform using ARTEMIS library and RT-LAB software. This adaptation involves partitioning the model into smaller subsystems, replacing MATLAB/Simulink components with ARTEMIS components, and optimizing execution across multiple cores. The modified model is compiled and loaded into the simulator (OPAL-RT OP5707) through the RT-LAB software for real-time execution. Finally, the real-time model is designed to interact with a digital controller for congestion and voltage management using TCP/IP communication protocol.

3.2.3 Data management layer and Visualization

The data management layer is responsible for facilitating seamless data exchange between the RTS, implemented on OPAL-RT, and the digital controller, as well as between the database platform and the monitoring interface. Communication between the real-time model and external systems is handled via the TCP/IP protocol, with data exchange occurring at 5-second intervals.

A dedicated middleware layer has been developed to manage this interaction. It receives real-time measurements from the simulator and transmits control commands to the BESS units modeled within the RTS. The middleware also acts as a bridge to the cloud-based database by using API calls to send the collected measurements to ThingSpeak. Control setpoints for active and reactive power are

retrieved from ThingSpeak and subsequently broadcast to the BESS systems via TCP/IP every 5 seconds.

ThingSpeak serves as the cloud-based database platform for managing real-time data exchange within the digital twin architecture. Measurements such as voltage, active power, and reactive power are continuously stored in dedicated channels, with each channel corresponding to specific nodes or components of the MV distribution grid. The use of structured channels ensures organized data management and supports the implementation of dynamic control strategies. The digital controller retrieves the latest measurements from these channels and processes them to compute reference signals for the BESS units. These control setpoints, such as active and reactive power references, are then written back to ThingSpeak, allowing for seamless closed-loop operation between data acquisition, control decision-making, and actuation.

Grafana is employed as the monitoring interface of the digital twin to provide a user-friendly visualization of the measurements stored in ThingSpeak. Through API integration, Grafana retrieves real-time data from the ThingSpeak channels and displays KPIs such as voltage levels, and power flows. This visualization supports situational awareness for operators and facilitates the analysis of system behaviour under normal and contingency conditions, enhancing both monitoring and decision-making capabilities. A snapshot of the dashboard in Grafana is shown in Figure 7. This architecture ensures efficient, reliable, and near real-time bidirectional communication between the simulation environment, control logic, and visualization tools.

3.2.4 Hardware in the loop controller

The hardware in the loop (HiL) controller plays a central role in managing congestion and maintaining voltage stability within the MV distribution grid. It utilizes real-time active and reactive power measurements, particularly at the HV/MV transformer, to monitor the apparent power and ensure that it remains within operational limits. To perform optimal control, the controller also receives market-related inputs for each BESS unit, including availability, activation costs, and maximum flexibility for the cleared market period. By combining this market data with real-time measurements from the HV/MV transformer and other critical nodes, the controller computes the required active and reactive power deviations for each BESS unit. These reference values are used to mitigate congestion and maintain acceptable voltage levels across the grid, enabling coordinated flexibility management in alignment with market and grid conditions.

The digital controller is integrated into the real-time simulation loop through a dedicated middleware layer that facilitates data exchange between the real-time simulator (OPAL-RT), the controller, and the cloud-based database (ThingSpeak). Real-time measurements from the MV grid model, such as voltage and power at the HV/MV transformer and other critical nodes, are transmitted from the simulator to the middleware via TCP/IP communication, with a 5-second refresh interval. The middleware forwards these measurements to ThingSpeak using API calls, from which the digital controller retrieves the latest data. Based on these inputs and market-cleared flexibility parameters, the controller computes reference signals for active and reactive power for each BESS unit. These references are then written back to ThingSpeak and subsequently retrieved by the middleware, which sends them to the simulator to update the control behaviour of the BESS models. This closed-loop integration ensures synchronized and responsive operation for real-time congestion and voltage management.

The MV distribution grid comprises a set of monitored buses $\mathcal{N} = \{1, 2, \dots, N\}$ and a set of BESS units $\mathcal{B} = \{1, 2, \dots, B\}$. Each monitored bus is equipped with a metering device that measures the local voltage magnitude, denoted as V_n , for $n \in \mathcal{N}$. In addition, the active and reactive power flow at the HV/MV substation, denoted P_s and Q_s , are measured at the feeder head and used to compute the substation apparent power $S_s = \sqrt{P_s^2 + Q_s^2}$. PV-BESS units and passive consumers are connected at lateral branches along the feeder, where monitoring is restricted to critical buses.



Figure 7: Grafana monitoring interface

The proposed HiL controller receives three categories of inputs: bus voltage and power measurements from the HV/MV substation and monitored buses, active and reactive power measurements from each BESS unit, and local distribution grid market data reflecting the available capacity and activation cost of the participating BESS units for providing congestion management and voltage regulation services. The DSO imposes an apparent power limit S_{lim} at the HV/MV substation, reflecting its rated thermal capacity. On the voltage side, the DSO specifies an admissible band $[V_{min}, V_{max}]$ at each monitored MV bus $b \in \mathcal{N}$, where V_{min} and V_{max} denote the lower and upper voltage bounds imposed by grid codes and power quality standards. Based on these inputs, the controller solves an optimization problem at each control interval to determine the cost-optimal activation of active and reactive power set-points dispatched to each BESS unit, with the objective that with the minimum operational cost to maintain $S_s \leq S_{lim}$ and keeping the voltage magnitude at each monitored bus within the permissible range.

Each BESS unit is characterized by a rated apparent power S_b^{max} and a minimum power factor $\cos\phi_{min}$, from which the maximum permissible active and reactive power are derived as,

$$P_b^{max} = S_b^{max} \cos\phi_{min}, \quad Q_b^{max} = S_b^{max} \sqrt{1 - \cos^2\phi_{min}}. \quad (1)$$

These limits define the feasible operating region of each BESS unit and are enforced as hard constraints within the optimization problem.

The relationship between BESS power injections and bus voltage deviations is captured through an approximate linear voltage sensitivity model. Specifically, the voltage V_n at bus n is approximated as a function $f(\Delta\mathbf{P}, \Delta\mathbf{Q})$ of the active and reactive power increment vectors $\Delta\mathbf{P} = [\Delta P_1, \dots, \Delta P_B]^T$ and $\Delta\mathbf{Q} = [\Delta Q_1, \dots, \Delta Q_B]^T$, which collect the dispatched increments of all available BESS units. This function relies on the entries $S_P(n, b)$ and $S_Q(n, b)$ of the voltage sensitivity matrices $\mathbf{S}_P \in \mathbb{R}^{N \times B}$ and $\mathbf{S}_Q \in \mathbb{R}^{N \times B}$, respectively. These matrices are derived offline via power flow perturbation studies on the feeder model, where each column corresponds to the voltage response across all monitored buses to a unit active or reactive power injection at the corresponding BESS bus. The sensitivity matrices are assumed to remain constant within each control interval, a standard linearisation assumption that is valid under the slowly varying operating conditions typical of MV distribution feeders. This linear approximation enables voltage constraints to be embedded in the mixed integer linear programming (MILP) formulation.

The HiL controller solves the objective function that minimizes the total BESS activation cost subject to congestion and voltage regulation requirements. Soft constraints are introduced for both the apparent power limit and the voltage bounds violation, penalized by large weights to prioritize constraint satisfaction over cost minimization, while preserving solution's feasibility. The objective function is defined as,

$$\begin{aligned} \min \sum_{b \in \mathcal{B}} (c_P^+ \Delta P_b^+ + c_P^- \Delta P_b^- + c_Q^+ \Delta Q_b^+ + c_Q^- \Delta Q_b^-) \\ + \lambda_s \xi_s + \lambda_v \sum_{n \in \mathcal{N}} (\xi_n^{V+} + \xi_n^{V-}) + \alpha \sum_{b \in \mathcal{B}} (z_b^P + z_b^Q), \end{aligned} \quad (2)$$

where ΔP_b^+ and ΔP_b^- denote the upward and downward active power regulation increments of BESS unit b , respectively, and ΔQ_b^+ and ΔQ_b^- denote the corresponding reactive power regulation increments. The asymmetric cost coefficients c_P^+ and c_P^- reflect the different activation costs associated with upward and downward active power regulation, as resulted by the local distribution grid market for congestion and voltage management, while c_Q^+ and c_Q^- reflects the activation cost for upward and downward reactive power regulation. The variable $\xi_s \geq 0$ is a slack variable reflecting the substation power limit violations, penalised by the weight λ_s to enforce thermal limits through a soft constraint approach. Similarly, the variables $\xi_n^{V+} \geq 0$ and $\xi_n^{V-} \geq 0$ are slack voltage variables per-bus representing the upper and lower voltage limit violations at the bus n , respectively, penalized by weight λ_v . The penalty hierarchy $\lambda_s > \lambda_v$ ensures that substation congestion relief is prioritized over voltage regulation in cases where both constraints cannot be satisfied simultaneously.

The final term in (2) introduces a fairness penalty that promotes an equitable distribution of the regulation effort across the participating BESS units. The fairness weight α scales the penalty applied to the deviation of each unit's dispatch from the fleet average. The mean active and reactive power increments are defined as $\mu_P = \frac{1}{B} \sum_{b \in \mathcal{B}} \Delta P_b$ and $\mu_Q = \frac{1}{B} \sum_{b \in \mathcal{B}} \Delta Q_b$, and the non-negative auxiliary variables z_b^P and z_b^Q bound the absolute deviation of each unit from these means, $z_b^P \geq |\Delta P_b - \mu_P|$ and $z_b^Q \geq |\Delta Q_b - \mu_Q|$, with each absolute value linearised through the standard pair of inequalities. Penalising z_b^P and z_b^Q in the objective drives the dispatched increments toward the fleet average,

distributing the regulation burden more evenly rather than concentrating it on the lowest-cost or most voltage-sensitive units. The weight α is kept well below the constraint penalties λ_s and λ_v , so that fairness shapes the dispatch only among solutions that already satisfy the congestion and voltage requirements, trading a marginal increase in activation cost for a more balanced utilisation of the BESS fleet.

The optimization problem is subject to a set of physical and operational constraints that ensure feasible and secure operation of the distribution system and the participating BESS units.

1) Power Activation and Complementarity: To ensure the practical operation of each BESS unit $b \in \mathcal{B}$, binary variables $b_{b,P}, b_{b,Q} \in \{0,1\}$ are introduced to prevent simultaneous upward and downward regulation. The power regulation increments are accordingly bounded as:

$$0 \leq \Delta P_b^+ \leq \bar{P}_b^+ b_{b,P}, \quad \forall b \in \mathcal{B}, \quad (3a)$$

$$0 \leq \Delta P_b^- \leq \bar{P}_b^- (1 - b_{b,P}), \quad \forall b \in \mathcal{B}, \quad (3b)$$

$$0 \leq \Delta Q_b^+ \leq \bar{Q}_b^+ b_{b,Q}, \quad \forall b \in \mathcal{B}, \quad (3c)$$

$$0 \leq \Delta Q_b^- \leq \bar{Q}_b^- (1 - b_{b,Q}), \quad \forall b \in \mathcal{B}, \quad (3d)$$

where $\bar{P}_b^\pm$ and $\bar{Q}_b^\pm$ denote the upward and downward regulation capacities declared by BESS unit b at the local flexibility market level. These constraints enforce that only one direction of regulation is active per service (active or reactive) at any given time step. The net power injections are defined as:

$$\Delta P_b = \Delta P_b^+ - \Delta P_b^-, \quad \Delta Q_b = \Delta Q_b^+ - \Delta Q_b^-, \quad \forall b \in \mathcal{B}. \quad (4)$$

2) BESS Power Capability Limits: Each BESS unit operates within its feasible power capability region, derived from its apparent power rating and minimum power factor. The limits are imposed as:

$$-P_b^{\max} \leq \Delta P_b \leq P_b^{\max}, \quad \forall b \in \mathcal{B}, \quad (5a)$$

$$-Q_b^{\max} \leq \Delta Q_b \leq Q_b^{\max}, \quad \forall b \in \mathcal{B}. \quad (5b)$$

3) Substation Apparent Power Constraint: The post-dispatch active and reactive power at the substation are expressed as:

$$P_s = P_s^0 + \sum_{b \in \mathcal{B}} \Delta P_b, \quad Q_s = Q_s^0 + \sum_{b \in \mathcal{B}} \Delta Q_b, \quad (6)$$

where, P_s^0 and Q_s^0 denote the pre-dispatch active and reactive power at the HV/MV substation, respectively. To preserve linearity while accurately approximating the circular apparent power limit, an octagonal relaxation is adopted. The octagonal approximation represents a trade-off between modeling accuracy and computational tractability. Compared to quadratic formulations, it enables real-time implementation while significantly reducing approximation errors.

The apparent power constraint is enforced through the following set of linear inequalities, where ξ_s is a slack variable representing the substation power limits violation.

$$|P_s| \leq a S_{\text{lim}} + \xi_s, \quad (7a)$$

$$|Q_s| \leq a S_{\text{lim}} + \xi_s, \quad (7b)$$

$$|P_s + Q_s| \leq a\sqrt{2} S_{\text{lim}} + \xi_s, \quad (7c)$$

$$|P_s - Q_s| \leq a\sqrt{2} S_{\text{lim}} + \xi_s, \quad (7d)$$

where $a = \cos(\pi/8)$. These constraints define an octagonal feasible region that more closely approximates the circular limit $P_s^2 + Q_s^2 \leq S_{\text{lim}}^2$ while maintaining compatibility with MILP formulations. The octagonal approximation can be interpreted as a discretization of the circular apparent power limit using directional linear constraints of the form $P_s \cos \theta_k + Q_s \sin \theta_k \leq a S_{\text{lim}}$, with $\theta_k = (k - 1)\pi/4$, and $k = 1, 2, \dots, 8$. The resulting formulation simplifies to the set of inequalities in (7). Each absolute value term is linearized using standard auxiliary variable techniques.

4) *Voltage Constraints*: The voltage magnitude at each monitored bus is added as equality constraint. Specifically, the voltage at bus n resulting from the active and reactive power dispatch of all BESS units is approximated as,

$$V_n = V_n^0 + \sum_{b \in \mathcal{B}} S_P(n, b) \Delta P_b + \sum_{b \in \mathcal{B}} S_Q(n, b) \Delta Q_b, \quad (8)$$

where V_n^0 is the pre-dispatch voltage at bus n . The soft voltage limits are enforced by introducing slack variables ξ_n^{V+} and ξ_n^{V-} as,

$$V_n \leq V_{\text{max}} + \xi_n^{V+}, \quad \forall n \in \mathcal{N}, \quad (9a)$$

$$V_n \geq V_{\text{min}} - \xi_n^{V-}, \quad \forall n \in \mathcal{N}. \quad (9b)$$

5) *Slack Variable Constraints*: Soft constraints are enforced through the introduction of non-negative slack variables, which permit controlled violation of the apparent power and voltage limits when no strictly feasible solution exists. This is particularly important under high PV generation scenarios, where simultaneous satisfaction of all hard constraints may be infeasible within a single control period. Rather than rendering the optimization problem infeasible, the slack variables absorb constraint violations and their magnitudes are penalized in the objective function. All slack variables are constrained to be non-negative, preventing the solver from exploiting negative violations to artificially reduce the objective:

$$\xi_s \geq 0, \quad \xi_n^{V+} \geq 0, \quad \xi_n^{V-} \geq 0, \quad \forall n \in \mathcal{N}. \quad (10)$$

3.2.5 Reliability assessment

The reliability and resilience of the MV distribution grid are evaluated by extracting and analyzing data from multiple operational scenarios. These scenarios include normal operation, congestion, high penetration of renewable energy sources, and cyberattack emulation such as false data injection attacks. By analyzing system performance under these conditions, key metrics such as voltage stability, congestion, and response to disturbances are assessed. The digital twin framework enables systematic comparison of results across various scenarios, allowing the identification of vulnerabilities and the validation of control strategies. This approach supports a more robust and resilient grid design capable of withstanding both physical and cyber-related disruptions.

3.3 Description of the French digital twin

3.3.1 Introduction

Task 5.5 aims to develop a Digital Twin for power system operators, integrating both physical power networks and cyber-communication networks. The primary goal is to enhance operator training and enable system testing under real-world conditions. The system will be event-driven, where trainees can interact with SCADA and network models while dealing with simulated operational challenges.

3.3.2 Objectives

- **Training System Operators:** Improve operator readiness by simulating realistic network scenarios, including power system contingencies and cyber events.
- **Testing New Components:** Provide a testbed for software and hardware modules, such as automation systems, and decision-support tools.
- **Scenario Execution & Analysis:** Develop a system that plays predefined scenarios, records trainee responses, and enables debriefing.
- **Performance monitoring:** Implement Key Performance Indicator (KPI) tracking and logging for post-training analysis.

3.3.3 System Architecture

The project consists of multiple interconnected modules, as shown in Figure 8, that facilitate real-time simulation and event driven interactions:

Game Master

- Oversees scenario execution and operator training
- Configured system modules (grid model, asset mapping, telecom characteristics)
- Provides a State View for trainers (unfiltered network visibility)
- Includes Game Master KPI functionality for monitoring system performance and decision-making during simulation.

Cyber-Physical Simulator

This component consists of three sub-modules:

- **Grid Simulator:** Models the physical power network using Dynawo, ensuring dynamic simulation of electrical events
- **Asset Simulator:** Maps physical system states to Cyber representations for SCADA-based control

- Information Flow Model: Simulates telecommunication behavior and cyber contingencies, including data delays and loss.

SCADA

SCADA acts as an 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.

Orchestrator

Acts as the central event handler, coordinating actions from the Game Master, SCADA and external systems.

- Ensures event-based execution with real-time updates every second
- Interfaces with SCADA and external replay for KPI analysis
- Logs all system interactions, enabling replay for KPI analysis

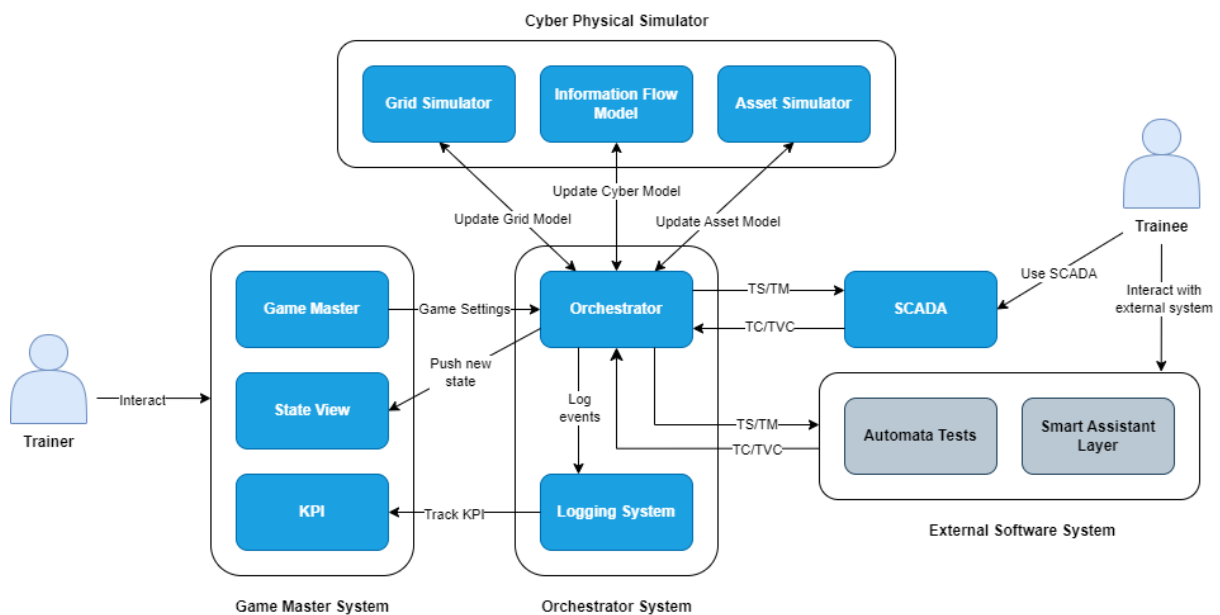


Figure 8: French Digital Twin Architecture

4 Approach to Scenario Development

This chapter presents the scenarios developed and demonstrated within the digital twins created under Tasks 5.2, 5.3, and 5.5. These scenarios are designed to comprehensively assess the cyber and physical resilience of power systems at both the transmission and distribution levels.

The Dutch and Cypriot digital twins focus on simulating operational and cyberattack scenarios, enabling the evaluation of system behavior under conditions such as high renewable penetration, congestion, and cybersecurity breaches. In parallel, the French digital twin is developed as a training-oriented simulator for power system operators. It supports immersive, event-driven scenarios that combine grid dynamics with cyber-physical interactions. Together, these scenario-based demonstrations provide a robust testing ground for resilience and reliability assessment.

4.1 Scenarios in the Dutch digital twin

The goal of Dutch DT is to develop and use digital twin to assess cybersecurity on interconnected power grids. This will include the cyberattack scenarios as follows:

4.1.1 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 will 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 cyberattacks 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 center 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.

4.1.2 Denial-of-Service Attacks

A Denial-of-Service (DDoS) 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 Denial-of-Service (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 focus 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. Second one aim 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 and risks to Supervisory Control and Data Acquisition (SCADA) systems, especially those pertinent to power grid operations [11]. 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 [11]. 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 [12]. 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 [13].

4.1.3 False Data Injection

The dominant research focus regarding cyberattacks on power systems is false data injection (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 center. 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 [8]. 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 analyze 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 machine learning perspectives [9], [10].

4.2 Scenarios in the Cypriot digital twin

In order to assess the reliability and resilience of the Cypriot distribution grid a series of what-if and cyber-security scenarios will be designed and executed using the digital twin framework. In the case of the reliability of the distribution grid the what-if scenarios allow for the assessment of the Cypriot distribution grid under different future scenarios and the impact of the designed controllers to manage congestion and voltage stability issues. Further, the resilience of the Cypriot distribution grid in different cyberattack scenarios will be also assessed considering mainly false data injection attacks. The two types of scenarios that will be used in the Cypriot digital twin are described below:

4.2.1 Operational scenarios

To comprehensively evaluate the digital twin framework and the associated congestion management strategy, two main operating scenarios will be simulated:

Baseline Scenario

This scenario represents the current operational state of the Cyprus distribution grid, as characterized by data provided by the Electricity Authority of Cyprus (EAC). It includes:

- Present-day levels of photovoltaic (PV) penetration
- Typical daily and seasonal load profiles
- Existing grid topology and constraints (e.g., transformer and line capacity limits)

The baseline scenario serves as a reference point for system behavior under current conditions, allowing for the validation of the digital twin model and providing a benchmark for comparison with future grid states.

Future Scenario

The future scenario explores a more challenging grid configuration, assuming significantly higher penetration of PV systems in the medium-voltage (MV) network. It simulates a projected evolution of the distribution grid aligned with national renewable energy targets and increased decentralization of energy resources. This scenario is designed to:

- Stress-test the congestion management mechanisms

- Evaluate the controller's ability to coordinate distributed flexibility resources (e.g., BESS, controllable PV inverters)
- Assess the impact on voltage and thermal loading in feeders with high DER concentration
- Through this scenario, the use case demonstrates how advanced control and flexibility coordination can prevent overloads and maintain grid stability even under future, more demanding operating conditions.

4.2.2 Cyber-Security Scenarios

This scenario introduces malicious interventions in the communication infrastructure to evaluate the resilience of the system under cyberattack. Two specific threat vectors are simulated:

False Data Injection (FDI):

Unauthorized alteration of control reference signals sent to battery energy storage systems (BESS). This manipulation can cause incorrect charging/discharging behavior, leading to inadequate congestion relief or unintended stress on the grid.

Measurement Tampering:

Compromise of data integrity at key monitoring points, such as the HV/MV transformer and the BESS units. Attackers inject misleading data, e.g., falsified voltage or current values—aiming to deceive the controller and disrupt its decision-making process. This can result in incorrect flexibility activation or failure to respond to actual grid events. These simulations are conducted within a sandboxed environment using tools like Ettercap, allowing for a safe and controlled assessment of system behavior under adversarial conditions.

By evaluating these cybersecurity scenarios, the use case not only demonstrates the digital twin's capability to detect and respond to attacks but also contributes to the development of more robust, cyber-resilient grid management solutions.

4.3 Scenarios in the French digital twin

The scenario development process is structured into **two project phases** to gradually build and refine the simulator while ensuring its reliability and effectiveness. The objective is to create realistic, event-driven training scenarios that integrate both **physical power networks** and **cyber-communication networks**, with a focus on system reliability, operator decision-making, and automation testing.

Phase 1: Proof of Concept Development (Targeted for June 2025)

The first phase focuses on establishing a functional digital twin prototype that integrates basic event-driven scenarios. The goal is to develop and validate core system components, ensuring seamless interaction between different modules.

Key Activities in Phase 1

Define and Implement a Basic Training Scenario

- Develop a fundamental scenario based on daily operations of a system operator to validate the simulator's capability.
- Example Scenario: Load increase leading to overload
- Simulate a case where a load increase on a transformer causes an overload condition.
- The scenario will be used to evaluate trainee response time and effectiveness in mitigating the issue.

Implement Game Master Functionality

- Develop the Game Master's ability to configure scenarios and monitor system events in real time.
- Implement basic scenario actions:
- Modification of load & generation
- Topological modifications (e.g., switching operations, reconfiguring the grid)

Develop Simulation Components

- Implement a SCADA emulator to visualize network states and receive operator inputs.
- Establish the Cyber-Physical Simulator, including:
- Grid Simulator (dynamic simulations using Dynawo).
- Asset Simulator (maps physical network changes to cyber interactions).
- Information Flow Model (simulates telecom delays and data loss).

Orchestrator Development

- Implement the event-driven orchestrator to synchronize all system components.
- Ensure one-second simulation updates while allowing event-based interactions between Game Master, SCADA, and the Cyber-Physical Simulator.

Outcome of Phase 1

- A working Proof of Concept demonstrating the core functionalities of the digital twin, ensuring real-time interactions between system modules.
- Validation of basic operator training scenarios.
- Identification of technical challenges for Phase 2 development.

5 Impact of Stressed Conditions on the Physical Resilience of the Grid

This section presents a set of representative case studies designed to evaluate the performance of the proposed coordination framework that was developed for the Cypriot digital twin framework under physically challenging operating conditions in distribution networks with high photovoltaic (PV) penetration. The analysis focuses on scenarios that induce stress on key system constraints, including substation thermal limits and nodal voltage bounds, driven by temporal variations in demand and renewable generation. By examining both baseline (uncontrolled) and optimized (coordinated) operation of a radial medium-voltage feeder equipped with distributed battery energy storage systems (BESS), the study highlights the effectiveness of the proposed MILP-based control strategy in mitigating congestion and maintaining voltage compliance under partial observability.

5.1 Case Studies of Physical Stress Scenarios

The studied network for the demonstration activities of the Cypriot digital twin, consists of a radial MV feeder with multiple PV-BESS units and passive consumers, as illustrated in Figure 9. This network was extracted by data provided by EAC related to the feeders in Cyprus. Voltage measurements are collected at a subset of critical buses defined as $\mathcal{N} = \{5, 9, 15\}$, selected based on their sensitivity to voltage deviations under high PV generation, thereby enabling effective voltage regulation under partial observability. The apparent power at the HV/MV substation is continuously monitored and constrained to remain below the predefined limit S_{lim} , which reflects the thermal capacity of the substation transformer as imposed by the DSO.

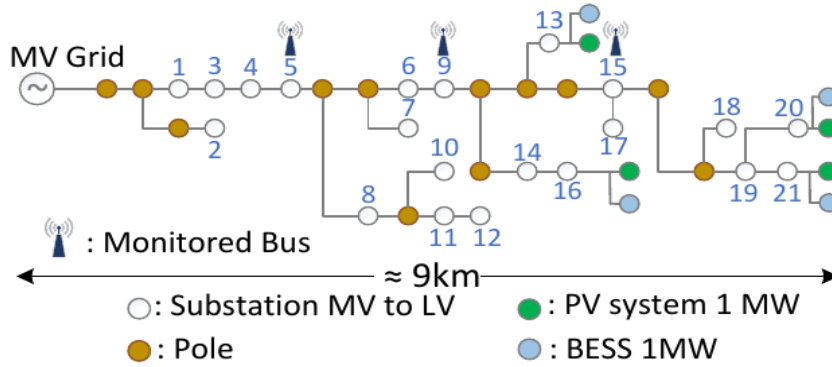


Figure 9: The representative MV distribution grid.

In the baseline scenario, the PV systems connected along the feeder operate under the $\cos\varphi(P)$ control mode, as required by the grid regulations, in which the power factor of the grid-side inverter is adjusted as a function of the active power output. Specifically, the inverter operates at unity power factor under low generation conditions and progressively absorbs reactive power as the active power output increases, according to a predefined piecewise-linear characteristic. This local reactive power absorption provides a degree of passive voltage regulation during periods of high irradiance. However, under sustained high PV generation, the $\cos\varphi(P)$ response is insufficient to prevent substation congestion or to maintain bus voltages within the permissible range $[V_{min}, V_{max}]$, which motivates the coordinated BESS dispatch proposed in this work. The rated apparent power of each PV inverter is

$S_{PV} = 1$ MVA, with a minimum power factor of $\cos\phi_{\min}^{PV} = 0.9$, yielding a maximum reactive power absorption of $Q_{\max}^{PV} = 0.436$ MVar.

A total of $B = 4$ BESS units are deployed across the feeder, co-located with the large PV parks, to provide, in addition to their businesses as usual operation, flexibility services for congestion management and voltage regulation through the local distribution grid market. Each unit is characterized by a rated apparent power of $S_{\max} = 1$ MVA and a minimum power factor of $\cos\phi_{\min} = 0.9$, from which the active and reactive power limits are derived as $P_{\max} = \bar{P}_b^{\pm} = 0.9$ MW and $Q_{\max} = \bar{Q}_b^{\pm} = 0.436$ MVar, respectively. State-of-charge dynamics are not modeled in this work, as the focus is on short-term operational flexibility within each control interval. The numerical values of all cost coefficients and penalty weights are summarized in Table 5-1.

The coordination controller solves the MILP problem formulated in Section 3.2.4 at a fixed control period of $\Delta T = 15$ s, reflecting practical communication and computation constraints in distribution systems. At each control interval, the controller collects updated substation, bus and BESS measurements, reconstructs the baseline operating point by removing the contribution of the previous BESS set-points, and solves the optimization problem using MATLAB's intlinprog solver. The computed active and reactive power increments are then dispatched to the BESS units.

Table 5-1: MILP model parameters

Symbol	Description	Value	Unit
BESS specifications			
$ B $	Number of BESS units	4	–
$S_{\max}$	Rated apparent power	1.0	MVA
$\cos\phi_{\min}$	Minimum power factor	0.9	–
$P_{\max}$	Active power limit	0.9	MW
$Q_{\max}$	Reactive power limit	0.436	MVar
$\bar{P}_b^{\pm}$	Upward/Downward active power cap.	0.9	MW
$\bar{Q}_b^{\pm}$	Upward/Downward reactive power cap.	0.436	MVar
Network			
V_{base}	Nominal line-to-line voltage	11	kV
$ N $	Monitored buses	3	–
$V_{\min}$	Lower voltage bound	0.95	pu
$V_{\max}$	Upper voltage bound	1.05	pu
Cost coefficients			
c_P^+	Upward active regulation	320	€/MW
c_P^-	Downward active regulation	180	€/MW
c_Q^+	Upward reactive regulation	82	€/MVar
c_Q^-	Downward reactive regulation	82	€/MVar
Penalty weights and constants			
α	Fairness weight	3	–
λ	Apparent-power slack penalty	10^8	–
β	Voltage slack penalty	10^7	–
k	Octagon half-planes	8	–

The performance of the proposed coordination scheme is evaluated under two scenarios. In the baseline scenario, no coordinated control is applied and the BESS units remain inactive, allowing the

network to operate under natural load and PV generation conditions. In the optimized scenario, the proposed MILP-based coordination controller is activated and integrated in a real-time control-HiL framework, dispatching active and reactive power set-points to the BESS units at every control interval to mitigate substation congestion and regulate bus voltages.

Figure 10 presents the 24-hour simulation results for the proposed MILP-based BESS coordination controller, showing the substation apparent-power loading, critical bus voltage profiles, and active and reactive power dispatch for each BESS unit. The top subplot of Figure 10 shows the substation apparent power S_s for the baseline and for the proposed coordination controller. For the baseline scenario (S_s^{base}), three distinct congestion windows are observed: a morning peak between approximately 02:00–06:00 h, a severe midday exceedance between 10:00–15:00 h driven by peak PV reverse power flow, during which S_s reaches approximately 3.5 MVA, and an afternoon peak between 17:00–21:00 h associated with the evening demand increase following PV generation. In all three windows, S_s^{base} exceeds the imposed limit $S_{\text{lim}} = 2$ MVA. Following controller activation (S_s^{opt}), the substation loading is maintained at or below S_{lim} throughout the entire 24-hour horizon, confirming the effectiveness of the octagonal apparent-power constraint in enforcing the thermal limit within the MILP framework.

The second subplot of Figure 10 shows the monitored voltage profiles at buses 5, 9, and 15. In the baseline scenario, bus voltages rise sharply during the midday PV generation peak, approaching the upper limit $V_{\text{max}} = 1.05$ pu. Under coordinated control, the voltages are slightly elevated by the reactive power that the BESS units inject to enforce the substation apparent power limit S_{lim} , yet they remain within the permissible band $[V_{\text{min}}, V_{\text{max}}] = [0.95, 1.05]$ p.u throughout the simulation horizon. The soft-constraint formulation preserves problem feasibility during peak PV injection by penalizing, rather than prohibiting, slack variable activation.

The active and reactive power dispatch profiles in Figure 10 reveal the control strategy adopted by the optimization problem. During the morning congestion window (02:00–06:00 h), all BESS units inject the same active power, due to the fairness weight, to reduce substation loading below S_{lim} . The exclusive use of active power during this period is consistent with the cost structure of the objective function: although reactive power injection carries a lower penalty coefficient, the active power adjustment required to bring the operating point within the inscribed octagon is sufficiently small that reactive power support is not warranted. During the midday window (10:00–14:00 h), the controller activates a coordinated response across multiple BESS units. BESS 3 and BESS 4 absorb active power to counteract reverse power flow driven by peak PV generation, while simultaneously injecting reactive power to suppress bus voltage rise at the remote buses. The reactive power dispatch reaches approximately 0.436 MVAR during the peak interval, confirming that voltage regulation is the dominant driver of the control action during this period. The greater influence of BESS 3 and BESS 4 on the voltage profiles is consistent with their proximity to buses 9 and 15. A similar pattern as in the morning window can be observed in the afternoon window (16:00–23:00 h) in which all BESS units share the same active power due to the fairness weight. Outside both congestion windows, all BESS units return to zero dispatch, confirming that the controller does not activate unnecessary and costly regulation actions when no constraint violations are detected.

In the baseline case, the BESS fleet is inactive and the feeder operates under the native effect of the PV generation. During the midday generation peak the substation apparent power rises to approximately 3.5 MVA, exceeding the 2 MVA loading limit by roughly 75% and producing a sustained congestion condition over several hours. The same reverse-power conditions drive the bus voltages

to the upper limit at the PV peak, while the evening demand period brings the voltages toward the 0.95 pu lower limit. The baseline therefore violates both the congestion and the voltage constraints, at different times of day and through distinct physical mechanisms.

Under the optimized MILP controller, the substation apparent power is held at or below the loading limit throughout the horizon, and all monitored bus voltages remain within the admissible band. This is achieved by coordinating active and reactive power across the four BESS units: the units absorb power during the midday peak to curtail reverse flow and over-voltage, and inject power during the evening congestion valley. The controller thus resolves the two constraints simultaneously, using the same fleet, by exploiting the temporal separation between the over-voltage/over-loading period and the under-voltage period.

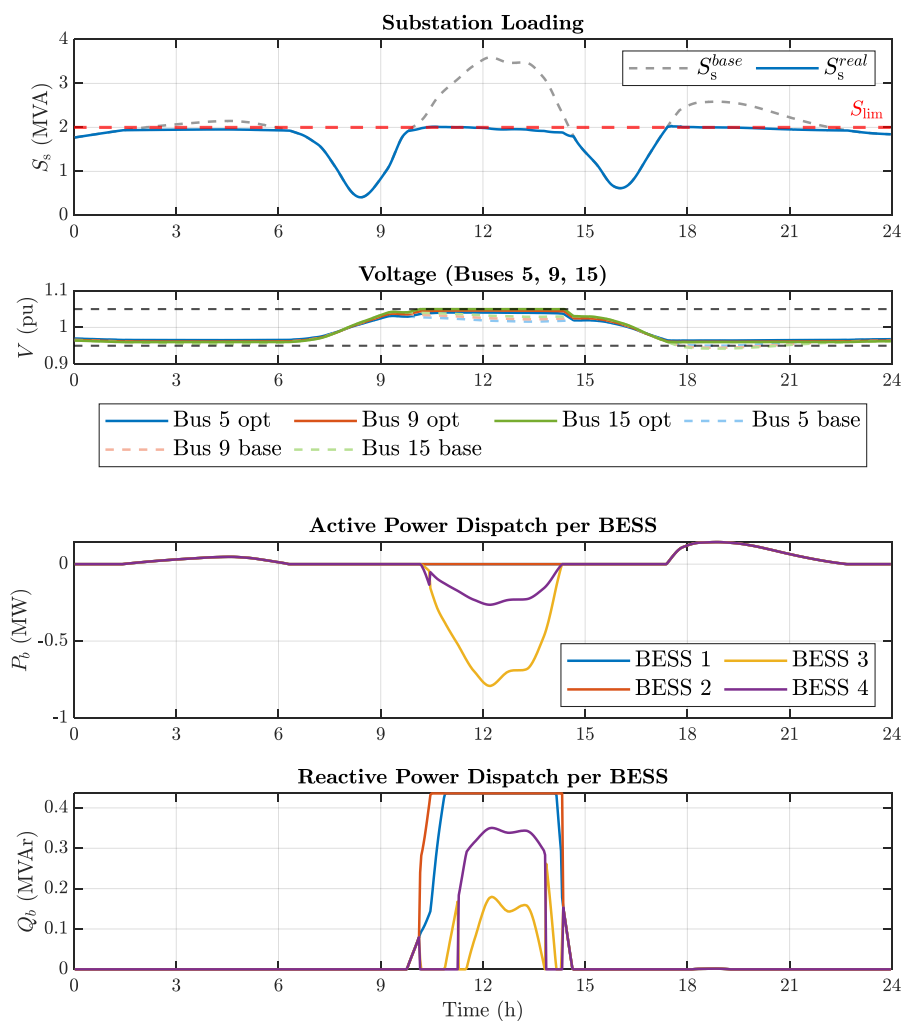


Figure 10: Experimental results over a 24-hour horizon

5.2 Lessons learned and recommendations

The principal observation is that congestion management and voltage regulation can be satisfied concurrently with the available BESS capacity, provided that active and reactive power are dispatched in a coordinated manner. Neither degree of freedom alone is sufficient at this level of PV penetration: reactive support addresses voltage but has limited authority over substation throughput, while active

curtailment addresses loading but is energy-constrained. The two-tier penalty hierarchy, which prioritizes the substation loading limit over the voltage limits, produced the intended behavior, with the controller relieving congestion as the dominant objective and treating voltage as secondary when the two competed.

6 Impact of Cyber-Attacks on Grid Resilience

This section presents a comprehensive evaluation of cybersecurity threats through case studies conducted on two distinct digital twin environments. Section 6.1 focuses on the Cypriot digital twin, examining the resilience of the proposed coordination framework under false-data and command-injection attacks that target critical measurements and control actions in distribution system operation. Section 6.2 complements this analysis by investigating large-scale cyberattack scenarios in the Dutch digital twin, including switching and spoofing attacks that emulate transmission-level disturbances and cascading failures. Together, these case studies provide a multi-scale assessment of cyber-physical vulnerabilities, illustrating how localized data manipulation and coordinated system-level attacks can propagate through control loops and network dynamics, ultimately impacting system stability, operational security, and resilience.

6.1 Case studies of Cyber-Attack Scenarios in the Cypriot demo

This section presents the cybersecurity validation of the proposed coordination framework within the Cypriot digital twin environment, focusing on its resilience under representative false-data and command-injection attacks. By emulating realistic cyber-physical threat scenarios on critical measurements and control signals, including substation power, nodal voltage readings, and BESS setpoints, the study evaluates how data manipulation propagates through the control loop and affects system-level objectives such as congestion management and voltage regulation. The following case studies systematically assess the controller's behavior under compromised observability and actuation, highlighting both its inherent limitations and the operational risks associated with undetected data corruption in real-time distribution system control.

6.1.1 False data injection attack on substation measurements

In the first case study, the controller behaviour under a false-data injection attack on the substation power measurement, activated at $t = 12:00\text{h}$, is evaluated. The results of this attack are illustrated in Figure 11. The attack is multiplicative, i.e., the measured substation active and reactive power are scaled by a factor of 0.8, i.e., $P_s^{\text{attacked}} = 0.8 P_s^{\text{real}}$ and $Q_s^{\text{attacked}} = 0.8 Q_s^{\text{real}}$ in p.u, so the apparent power seen by the controller is likewise reduced, $S_s^{\text{attacked}} = 0.8 S_s^{\text{real}}$. Prior to the attack the two traces coincide, and the controller holds the loading at S_{lim} , as in the optimal scenario of Figure 10. After the attack, the controller continues to regulate the quantity it observes, driving S_s^{attacked} to approximately 1.95MVA, while the true loading S_s^{real} rises toward $S_{\text{lim}}/0.8 \approx 2.5\text{MVA}$, reaching about 2.4MVA, as shown in Figure 11, and thereby exceeding the limit by roughly 0.4MVA ($\approx 20\%$) throughout the midday (12:00–14:30 h) and evening (17:00–21:00 h) congestion windows.

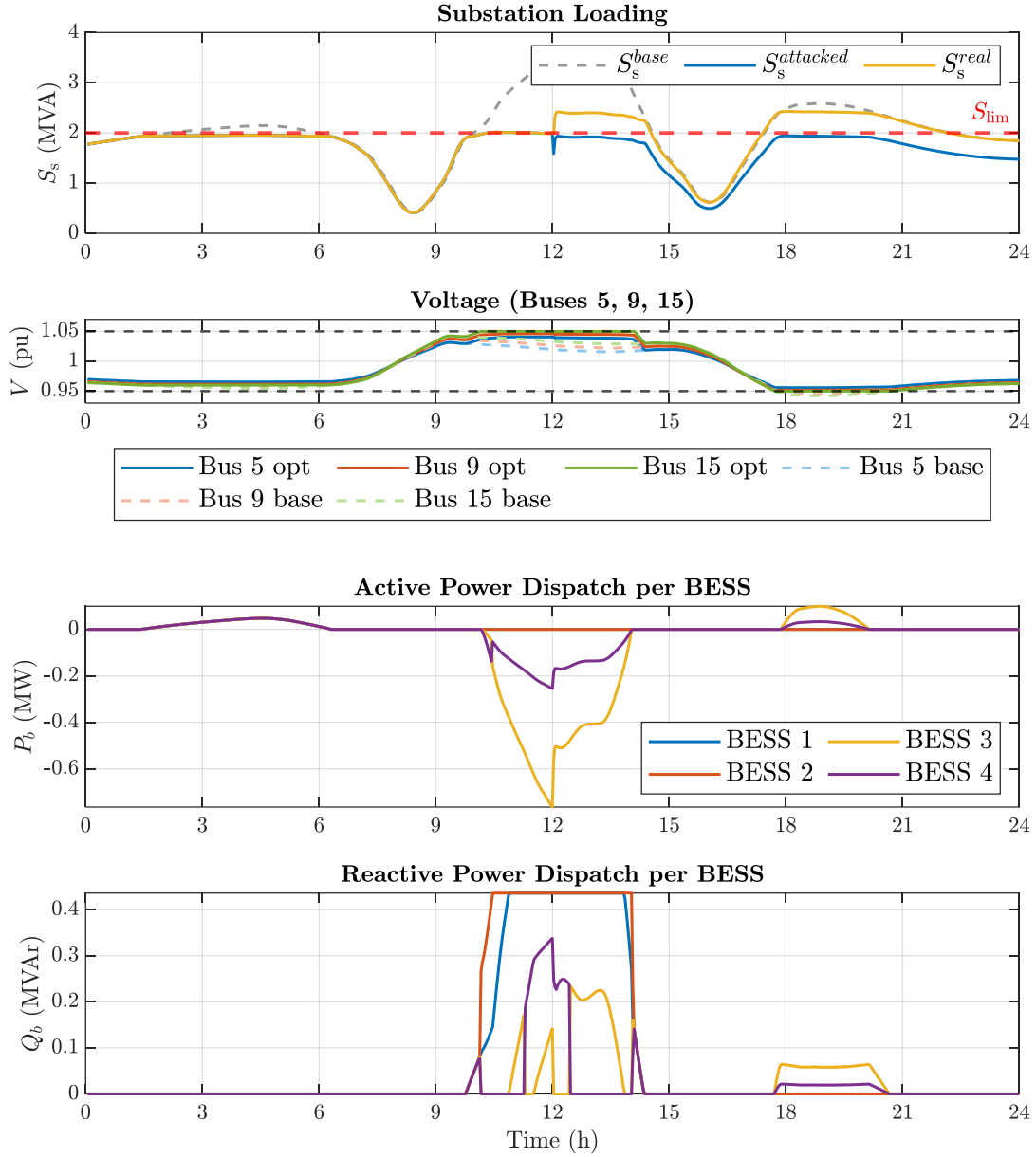


Figure 11: Multiplicative attack at the substation measurement.

6.1.2 False data injection attack on the voltage measurements

In this case study, a multiplicative attack on the voltage measurement of Bus 15, in which the reported value is scaled by a factor of 0.95 from 12:00 onward is showcased in Figure 12. As shown in the second subplot, the corrupted measurement reduces the voltage observed by the controller from 1.05 pu to 1.0 pu. Therefore, the resulting margin as available voltage headroom is interrupted and the controller curtails the active and reactive power absorbed by BESS 3 and 4. The reduced absorption drives the true voltage above the 1.05 pu upper limit, yielding a violation that the controller cannot detect. The converse behavior is observed at 16:00, when the corrupted measurement reaches the 0.95 pu lower limit. In response, the controller dispatches active and reactive power to raise the perceived voltage, although the actual voltage remains within the admissible band. Consequently, the attack induces erroneous control actions in both directions, an undetected limit violation in the first

case and an unnecessary dispatch of resources in the second, irrespective of the true operating state of the network.

Figure 13 presents the complementary scenario, in which the voltage measurement of Bus 9 is corrupted by a multiplicative factor of 1.05 from 12:00 onward. The inflated measurement leads the controller to observe a voltage that exceeds the 1.05 pu upper limit, prompting it to engage the BESS units in order to return the perceived voltage to the admissible range. Since the over-voltage is fictitious, however, the additional dispatch is unwarranted: the increased BESS activity depresses the true voltage below its required level and consumes battery capacity without any corresponding operational need.

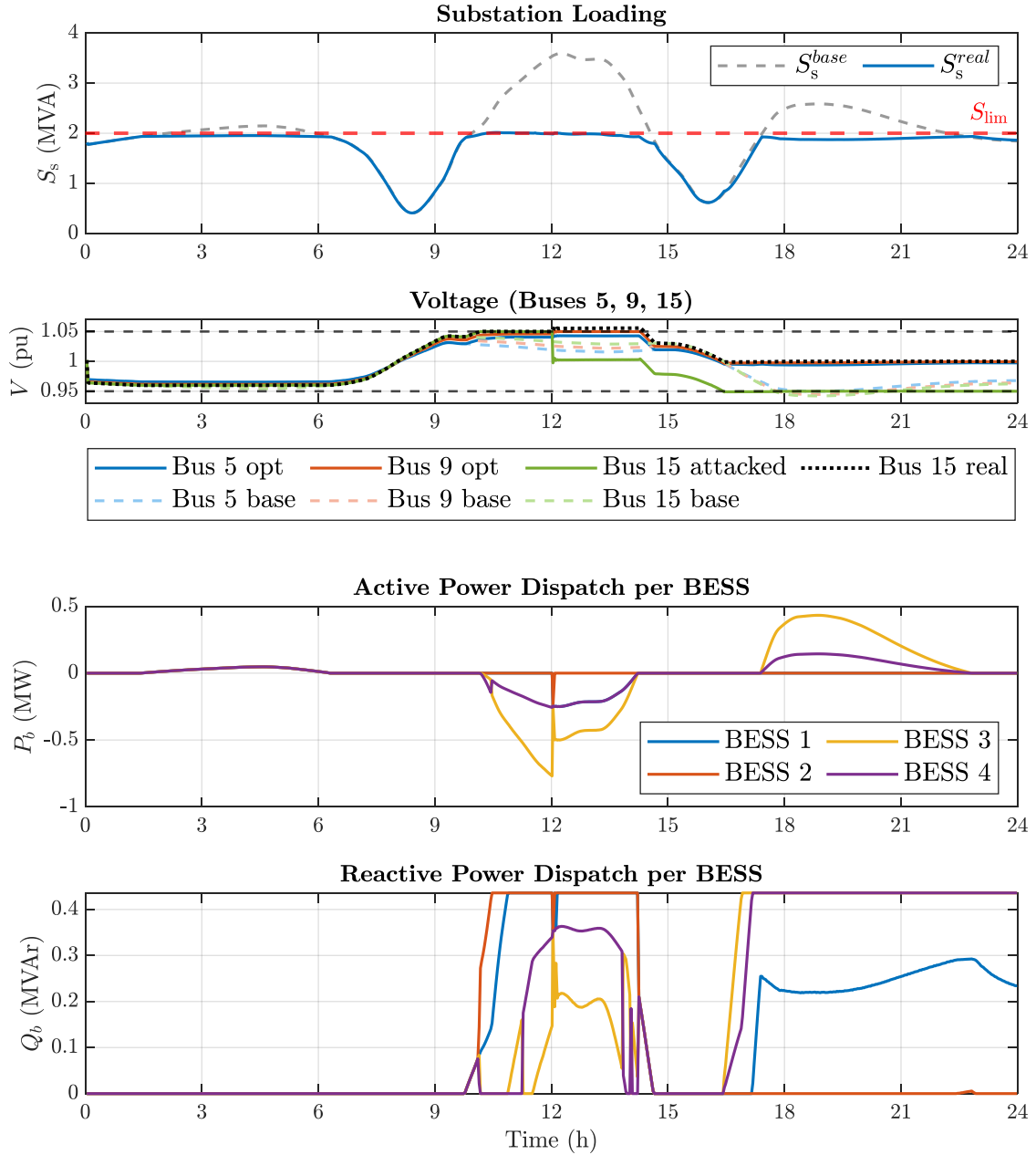


Figure 12: Multiplicative attack at the voltage measurement with a factor 0.95.

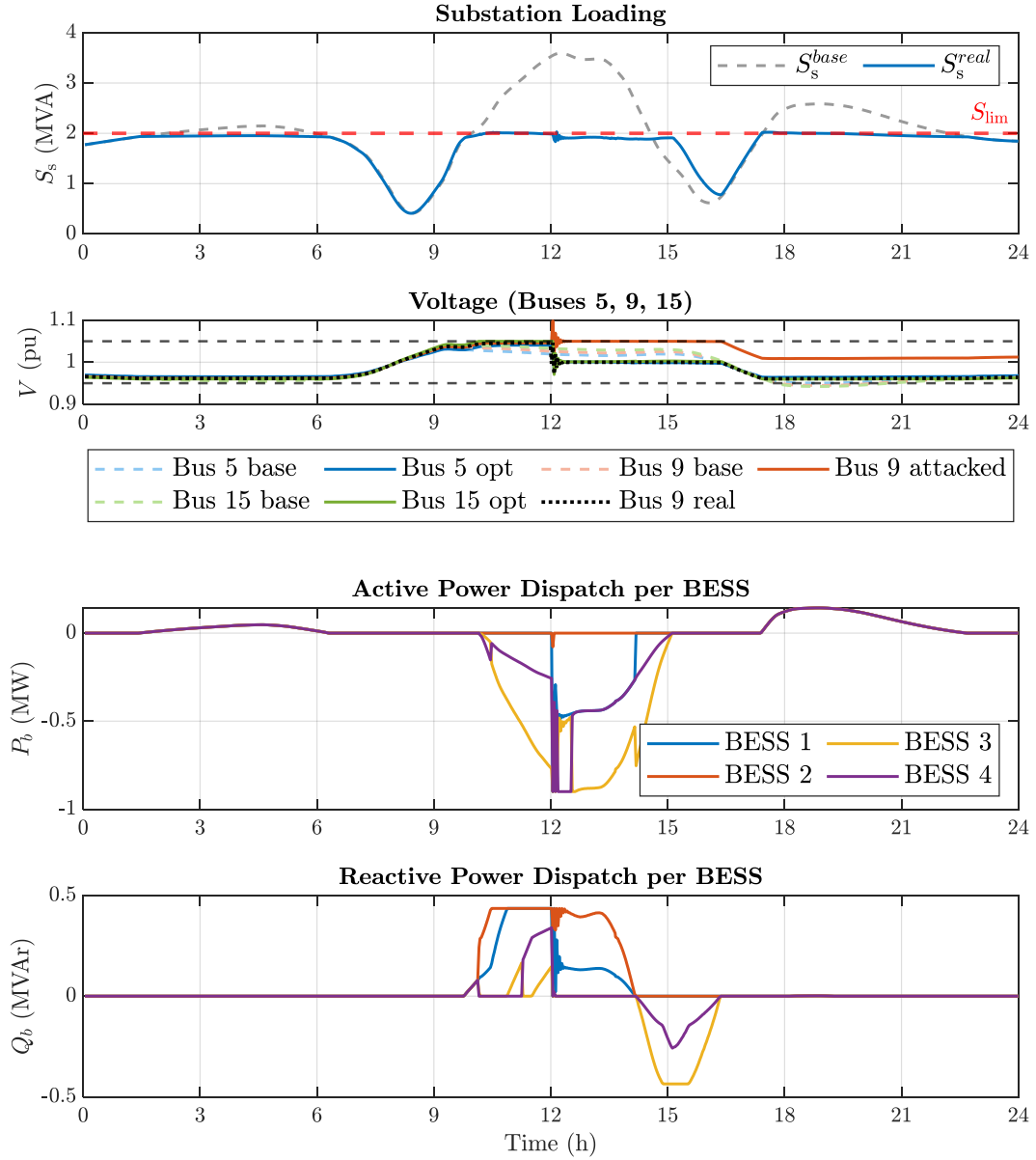


Figure 13: Multiplicative attack at the voltage measurement at Bus 9 with a factor 1.05.

6.1.3 Battery Setpoint Injection Attack

A setpoint-injection attack on BESS 3 is illustrated in Figure 14, initiated at 12:00 and modeled as a multiplicative corruption of active power with a gain of -1 , such that the unit delivers active power of equal magnitude but opposite sign to its dispatched value. As shown in the dispatch subplot, the response observed by the controller is the negative of the unit's true output, so the controller perceives correct tracking while BESS 3 in fact counteracts the intended dispatch. To resolve the resulting congestion and voltage deviations, the remaining BESS units are driven to their active-power limits, leading to a system-wide over-utilization of resources as they attempt to offset the corrupted unit. The mismatch also produces a transient spike in the substation apparent power above S_{lim} , which persists until the controller recomputes the setpoints at the subsequent control step.

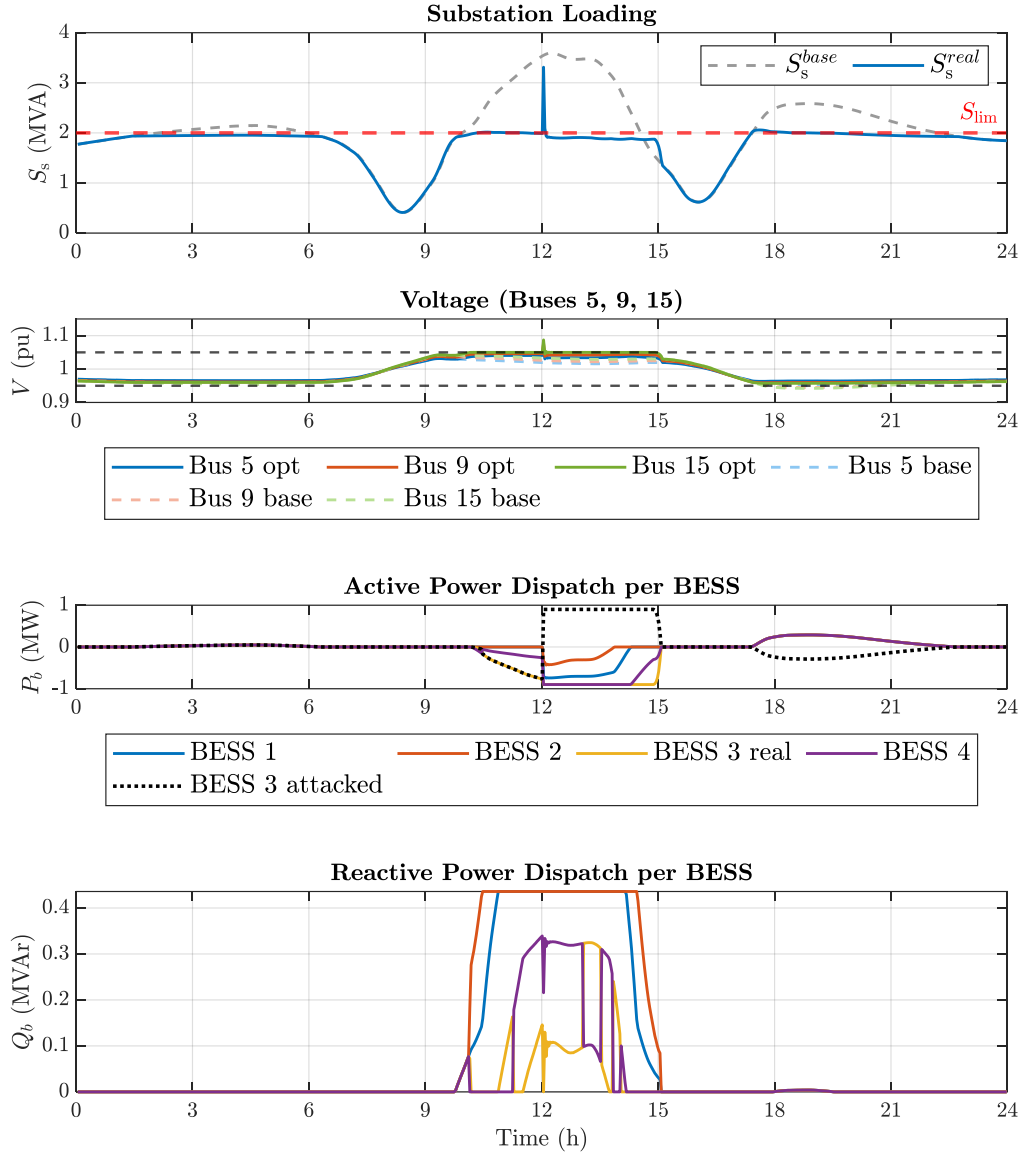


Figure 14: Multiplicative attack at BESS 3 active power setpoint.

6.1.4 Impact Analysis of cyberattacks on the controller performance and the system operation

Four false-data injection attacks were evaluated, spanning the measurement and command paths and both controlled objectives. A deflation of the substation apparent-power measurement leads the controller to perceive a feasible operating point and under-dispatch, so the true loading rises to about 2.4 MVA and exceeds the 2 MVA limit by roughly 0.4 MVA ($\approx 20\%$) congestion window. A deflation of the Bus 15 voltage measurement similarly relaxes the dispatch and drives the true voltage above the 1.05 pu limit, while the dual inflation of the Bus 9 measurement causes the controller to over-actuate against a fictitious over-voltage, depressing the true voltage and wasting battery capacity without violating any limit. Finally, a command-path attack inverting the BESS 3 active-power setpoint makes the unit counteract its dispatch; the remaining units saturate to compensate and a transient spike in substation apparent power exceeds the loading limit until the setpoints are recomputed.

The common feature across all four cases is that small data corruptions translate into real, physical constraint violations, on both the voltage and the congestion objectives. The closed-loop structure compounds this because the controller acts on the corrupted information, the error propagates into the physical state of the network rather than remaining confined to the measurement, and in three of the four cases the resulting violation is entirely invisible to the controller.

6.1.5 Lessons learned and recommendations

The attacks revealed an efficiency–robustness trade-off intrinsic to constraint-tight optimization. In particular, holding the system at its operational limits leaves no buffer to absorb undetected bias, so the very behavior that makes the optimized scenario attractive is what makes it fragile under data corruption. The measurement-path scenarios further showed that the vulnerability spans both objectives, a corrupted voltage measurement defeats voltage regulation, and a corrupted substation measurement defeats congestion management. Therefore, a defense limited to one signal class is insufficient. The substation case is particularly significant, since a single aggregated measurement governs the highest-priority objective and therefore concentrates risk at one node.

An important observation from the conducted experiments is that all examined operating scenarios remained solvable with the available flexibility resources. Consequently, the controller was able to satisfy both congestion-management and voltage-regulation objectives simultaneously under normal operating conditions. Future investigations should therefore consider stressed operating scenarios with insufficient flexibility capacity, such as reduced BESS availability, state-of-charge limitations, or higher levels of PV penetration. Such conditions would force the optimization framework to prioritize between competing objectives and would enable a more quantitative evaluation of the penalty hierarchy embedded within the MILP formulation.

Similarly, the cyber-security assessment focused on representative false-data injection attacks in which corrupted measurements and control signals were directly accepted by the controller. Future work should investigate more sophisticated attack scenarios that attempt to evade basic bad-data validation, anomaly-detection, or consistency-checking mechanisms. Such scenarios would enable a more comprehensive assessment of the trade-off between operational efficiency, controller performance, and cyber resilience under adversarial conditions. In particular, the controller currently treats all telemetry and all actuation as trusted, so none of the four attacks is flagged. In the three measurement-path cases the controller has no awareness of the corruption, and only the command-path case is partially self-correcting, where the periodic re-computation bounds the duration of the transient but does not prevent it. The command-path attack also confirmed that actuation integrity is as critical as measurement integrity. The impact analysis of the cyberattacks indicates the importance of effective cyberattack detection schemes that could possibly alleviate the negative impact of the attacks to the performance of the controller and to the system operation.

6.2 Case studies of Cyber Attack Scenarios in the Dutch demo

Two major types of cyberattack scenarios were considered to analyse their impact on the Dutch grid namely the switching attacks and the spoofing attacks. Different combinations of switching attack scenarios were developed by disconnecting multiple transmission lines simultaneously at substations, as well as disconnecting multiple transmission lines sequentially and randomly to represent worst-case grid conditions. These scenarios replicate use cases similar to the Ukrainian cyberattack incidents. For the spoofing attack scenario, it is assumed that an attacker gains unauthorised remote access to

a substation and can remotely alter the set points of controllers, such as the Automatic Voltage Regulator (AVR), Load Frequency Controller (LFC), and interconnector power set points. Such manipulations can create disturbances that lead to cascading failures, resulting in either partial or complete grid blackouts. Furthermore, the cascading failure dynamics resulting from these cyberattacks are analysed to provide valuable insights for the development of effective control and mitigation strategies in the future.

6.2.1 Impact analysis of system performance and Impact on the system

6.2.1.1 Switching attack use case

In this attack scenario, the transmission lines connected to the MEE380 substation are abruptly disconnected while the grid is operating under stable conditions. The cyberattack is initiated at $t = 15$ s, causing the immediate disconnection (isolation) of the DE_HVDC interconnector by the under-voltage protection scheme, as the targeted substation is located close to the interconnector area.

The loss of the interconnector creates a significant generation–load imbalance and frequency instability. To stabilize the system, the automatic load-shedding protection scheme is immediately activated, shedding approximately 7% of the total system load. Although the cyberattack is performed at a single location, it propagates rapidly and results in system-wide instability.

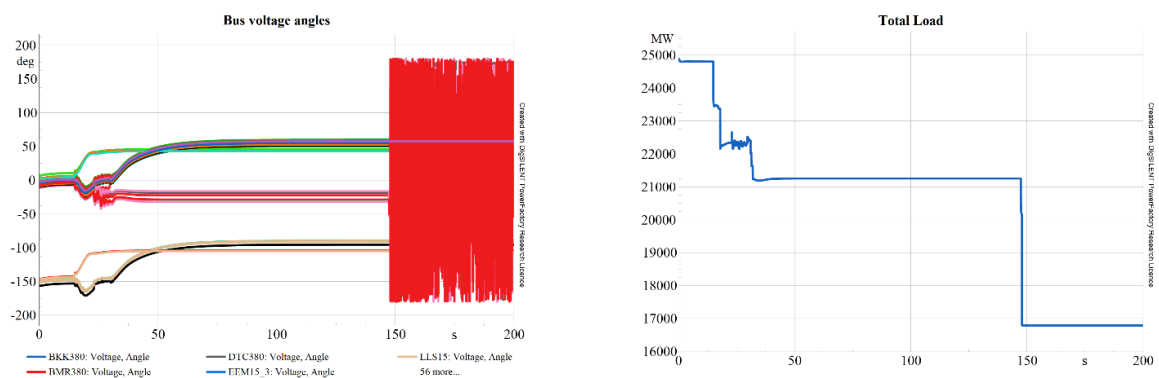
The redistribution of power flows causes several transmission lines to become overloaded, leading to their immediate tripping by overload protection schemes before corrective control actions can be implemented. The subsequent line disconnections result in the formation of multiple uncontrolled and unstable electrical islands. The severe frequency deviations and high Rate of Change of Frequency (RoCoF) further trigger the disconnection of multiple German interconnectors, ultimately resulting in approximately 36% load loss, as shown in Figure 15.

The cyberattack creates instability in the system, leading to the formation of uncontrolled islands. This results in high rates of change of frequency (RoCoF) in multiple generators, causing them to be disconnected by the RoCoF protection scheme. The generators NDR380_G, supplying approximately 3 GW of power, and GNA380_G, supplying approximately 1.5 GW, exhibit stable voltage and frequency responses. However, both generators experience high RoCoF values and are consequently disconnected by the RoCoF protection scheme, as shown in Figure 16, Figure 17.

The transmission line disconnections caused by overload conditions are shown in Figure 19, while the load-shedding operations are illustrated in Figure 18. while the chronological sequence of events is summarized in Table 6-1.

Table 6-1: Sequence of events during switching cyberattack

Time (s)	Events	System Impact
15	Multiple transmission lines at the MEE 380 kV substation were disconnected due to a coordinated cyberattack.	Initiated severe network disturbances and power flow redistribution.
15.25	The HVDC_DIL380 interconnector was disconnected by the under-voltage protection scheme	Reduced power transfer capability and aggravated the generation-load imbalance.
18	Automatic load shedding of 7% was performed across the system to stabilize the network and recover system frequency.	Temporarily improved the generation-load balance and frequency response.
23	The DIM380_LLS380 transmission line and several other lines were disconnected by overload protection schemes.	Triggered cascading outages and resulted in the formation of multiple uncontrolled islands.
31	An additional 7% load shedding was performed in the cyber-attacked vicinity.	Reduced local demand and attempted to mitigate further instability.
140	The system reached the point of no return due to severe voltage, frequency, and dynamic instabilities.	System-wide instability became irreversible.
147	Multiple generators and interconnectors were disconnected by frequency and Rate of Change of Frequency (RoCoF) protection schemes	Significant loss of generation and further system fragmentation occurred.
150	Total system load decreased from approximately 25 GW to 16 GW.(36% load loss)	Resulted in widespread service interruptions and partial system blackout conditions.

**Figure 15: Bus voltage angles and total loads**

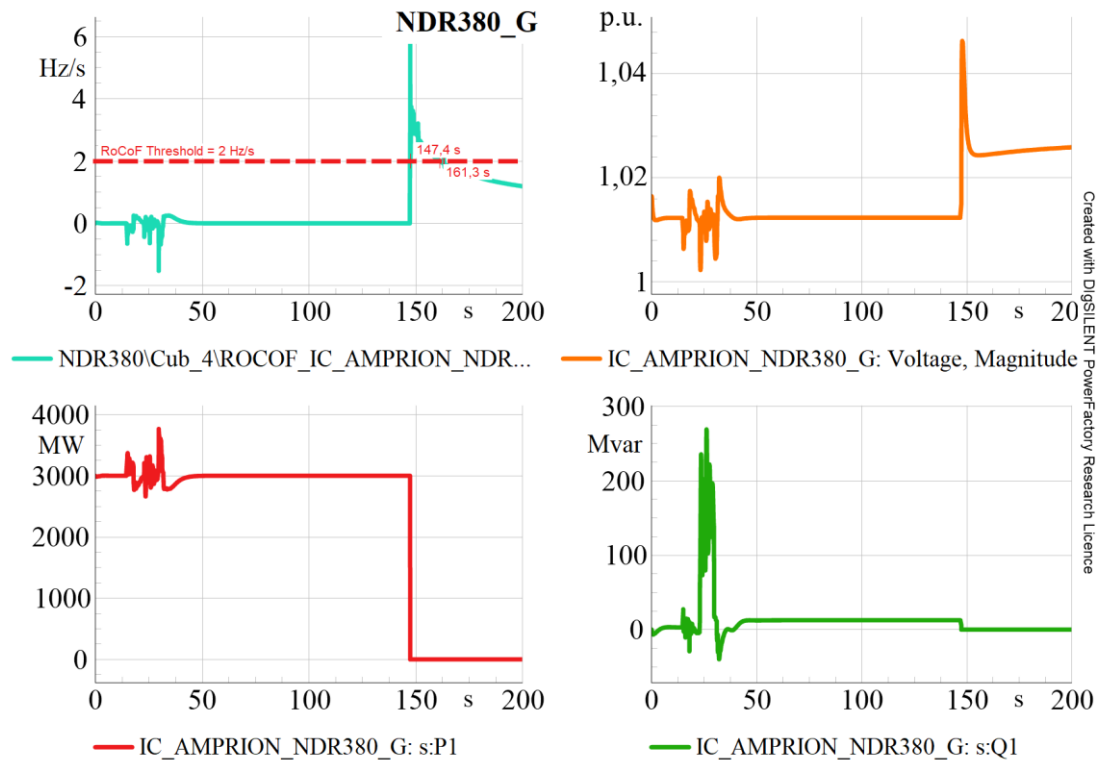


Figure 16: RoCoF protection tripping of NDR380_generator

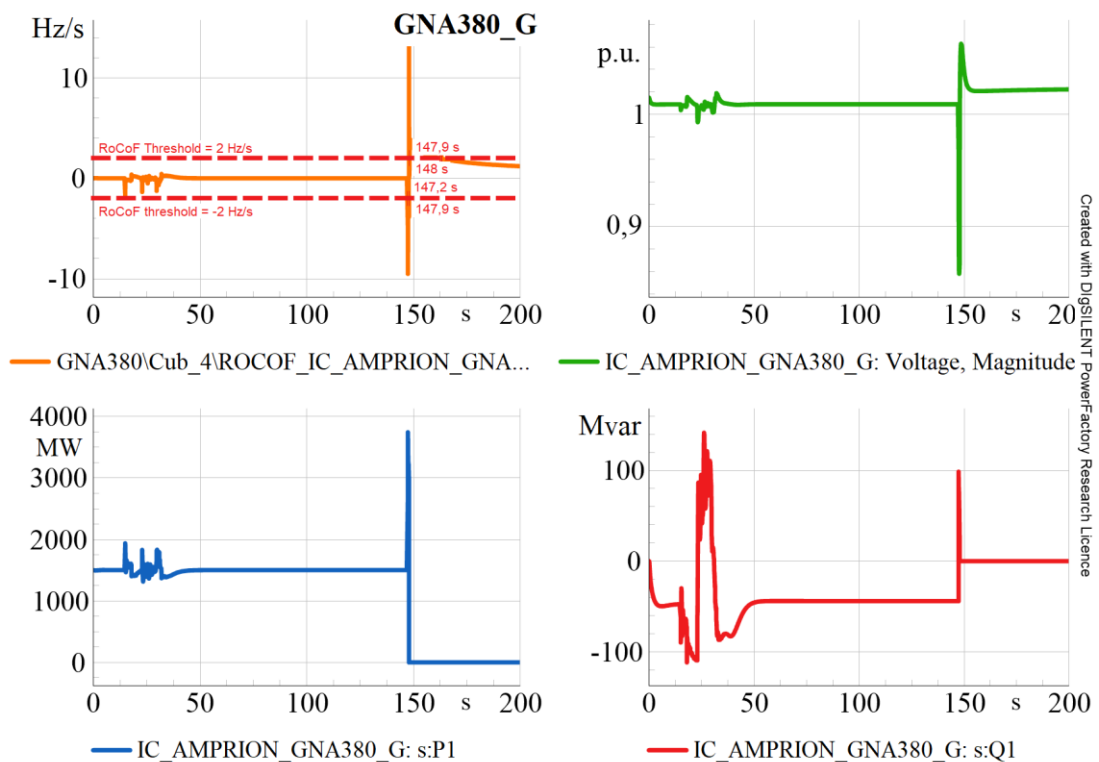


Figure 17: RoCoF protection tripping of GNA380 generator

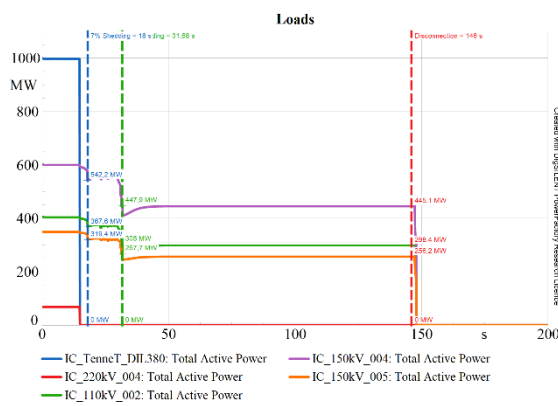


Figure 18: Loading shedding and load disconnection of Dutch network

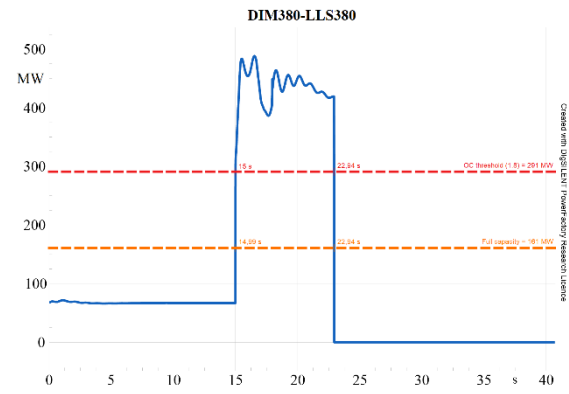


Figure 19: Line tripping caused by overloading

6.2.1.2 Switching cyberattack (sequence):

This scenario is similar to the previous use case; however, instead of disconnecting all transmission lines simultaneously, the transmission lines are maliciously disconnected in a random sequence to more closely replicate a realistic cyberattack scenario. In this case, multiple transmission lines connected to the ENS380 kV bus are disconnected between $t = 15$ s and $t = 18$ s at intervals of 0.5 s. These disconnections result in the overloading of several transmission lines, which are subsequently disconnected by the overload protection schemes. Following the initial cyberattack event, multiple uncontrolled electrical islands are formed, resulting in severe system instability. Consequently, several generating sources within these unstable islands are disconnected by various protection mechanisms.

Multiple generators within the same islands are tripped by either the Rate of Change of Frequency (RoCoF) protection or over-frequency protection schemes. The loss of generation further drives additional instabilities, such as load shedding in certain areas and high-frequency operation in others, as summarized in Table 6-2. The high-frequency instability eventually leads to the sudden disconnection of a generating unit, which subsequently triggers the rapid tripping of multiple generators and wind turbines. This cascading failure results in an overall load loss of approximately 48%, corresponding to nearly half of the country's demand being affected by blackout conditions, as shown in Figure 20.

Figure 21 illustrates the system bus voltage angles and the total load demand, which decreases from 25 GW to approximately 14 GW as a result of the initial cyberattack event.

The cyberattack event triggered multiple protection schemes. For example, generator GNA380_G was disconnected by the RoCoF protection scheme, as shown in Figure 22. The IC_Cobra interconnector was disconnected by the undervoltage protection scheme, as shown in Figure 23, and generator EEM15_3 was tripped by the over-frequency protection scheme as shown in Figure 24.

Table 6-2: Sequence of events during sequence switching cyberattack

Time(s)	Events	System Impact
15-18	A sequence of coordinated cyberattack events was initiated, resulting in the disconnection of multiple transmission lines of bus ENS380.	Triggered severe disturbances and abnormal power flow redistribution across the network.
18	Multiple transmission lines, including the MBT380–DOD380 line, were disconnected by overload protection schemes.	Led to cascading outages and the formation of multiple uncontrolled electrical islands.
21	The GNA380 generator was disconnected by the Rate of Change of Frequency (RoCoF) protection scheme. Additional generators, including EEM15_3, EEM15_4, and DKG15, were disconnected by RoCoF and over-frequency protection schemes.	Caused significant generation loss and further destabilized the isolated network islands.
22	Most wind turbines operated beyond their permissible frequency limits.	Increased the risk of widespread wind turbine tripping due to over-frequency protection.
22.5	Automatic load shedding of 7% was performed across the entire system, including loads such as IC_150kV 024-026, etc.	Temporarily reduced the generation–load imbalance and attempted to stabilize system frequency.
160	The NDR380 element was disconnected by protection schemes, and additional wind turbines were disconnected by over-frequency protection.	Resulted in further loss of network support and renewable generation capacity.
161	System demand decreased significantly, with the load level changing from approximately 25 GW to 13 GW which is 48% of load loss, approximately half of the grid	Led to widespread supply interruptions and severe system degradation approaching blackout conditions.

Digital Twin Power System Model

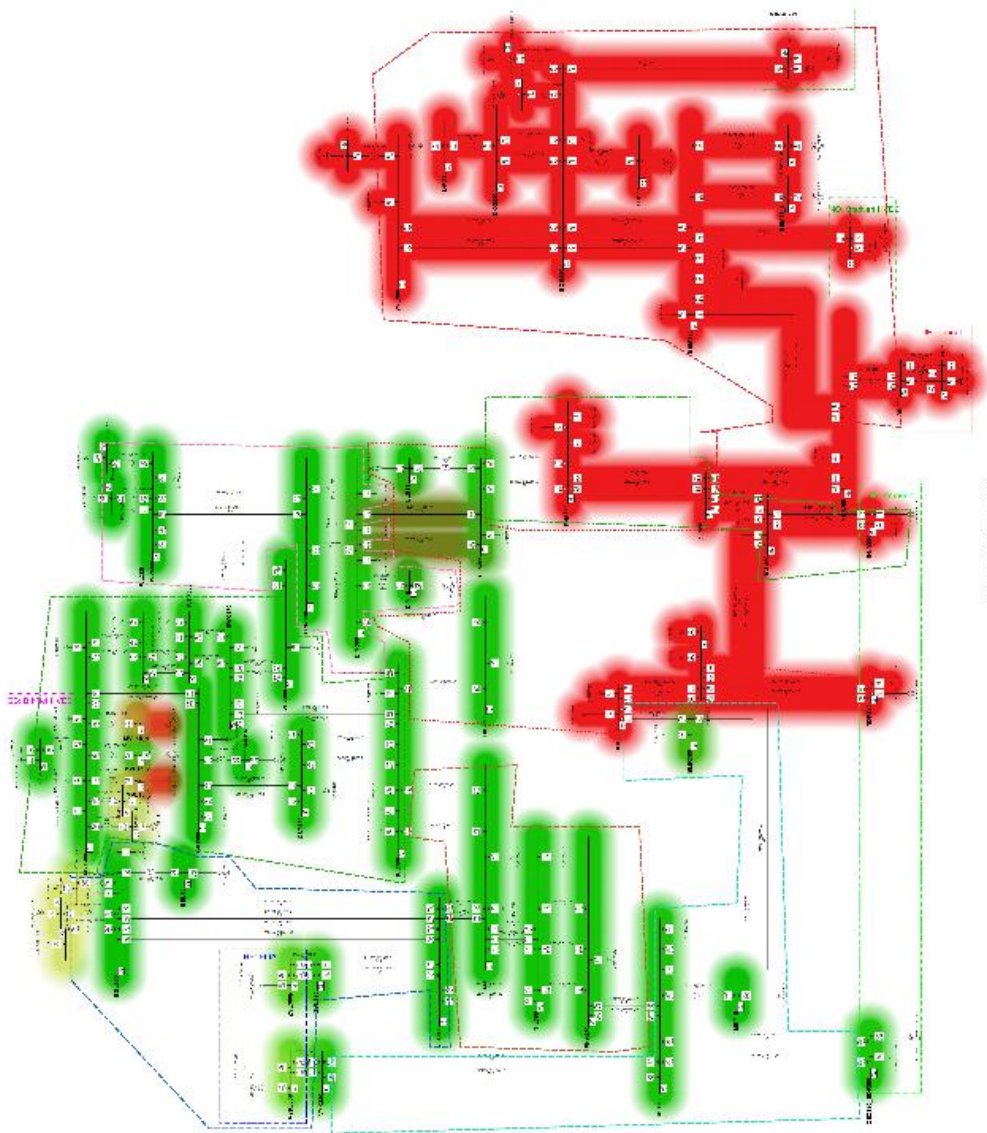


Figure 20: SLD of Dutch network blackout region

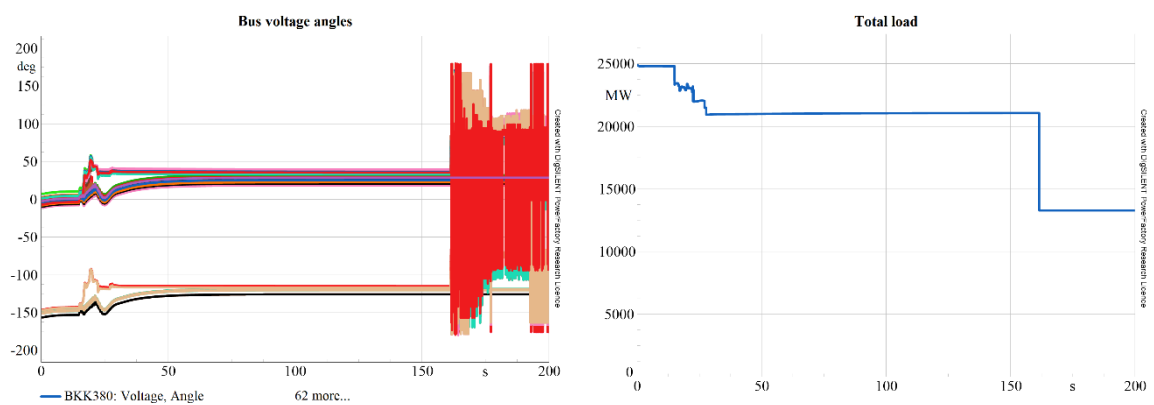


Figure 21: Bus voltage angles and total load

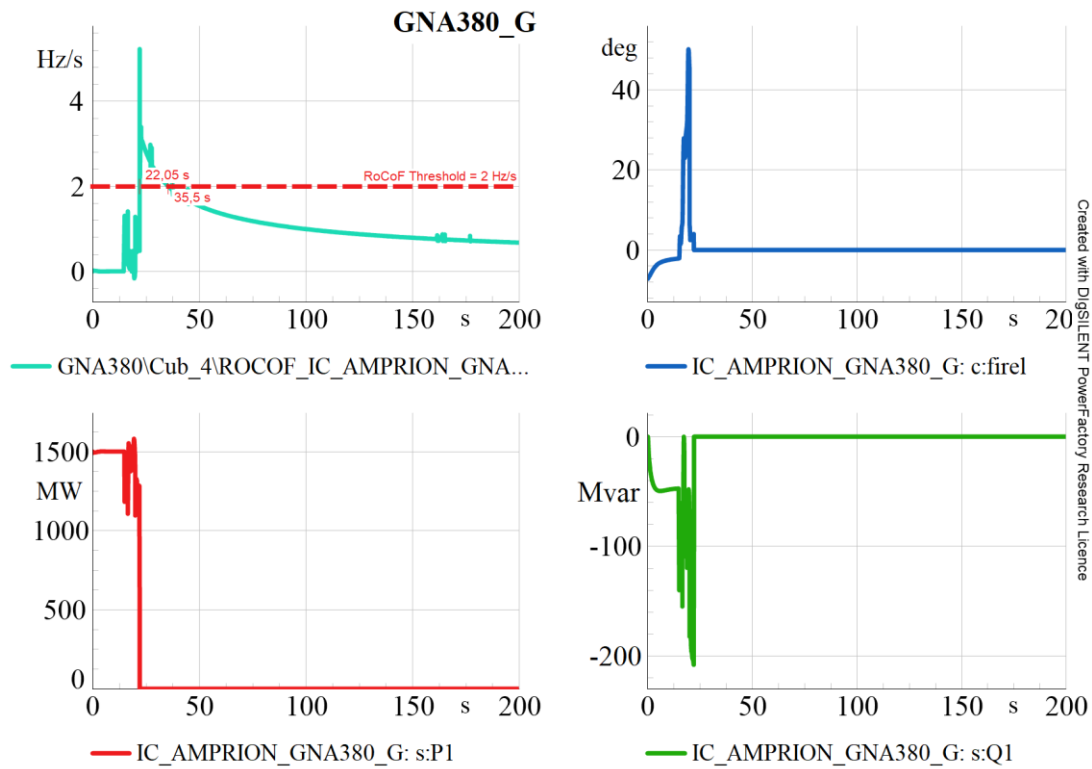


Figure 22: RoCoF tripping of GNA380 generator

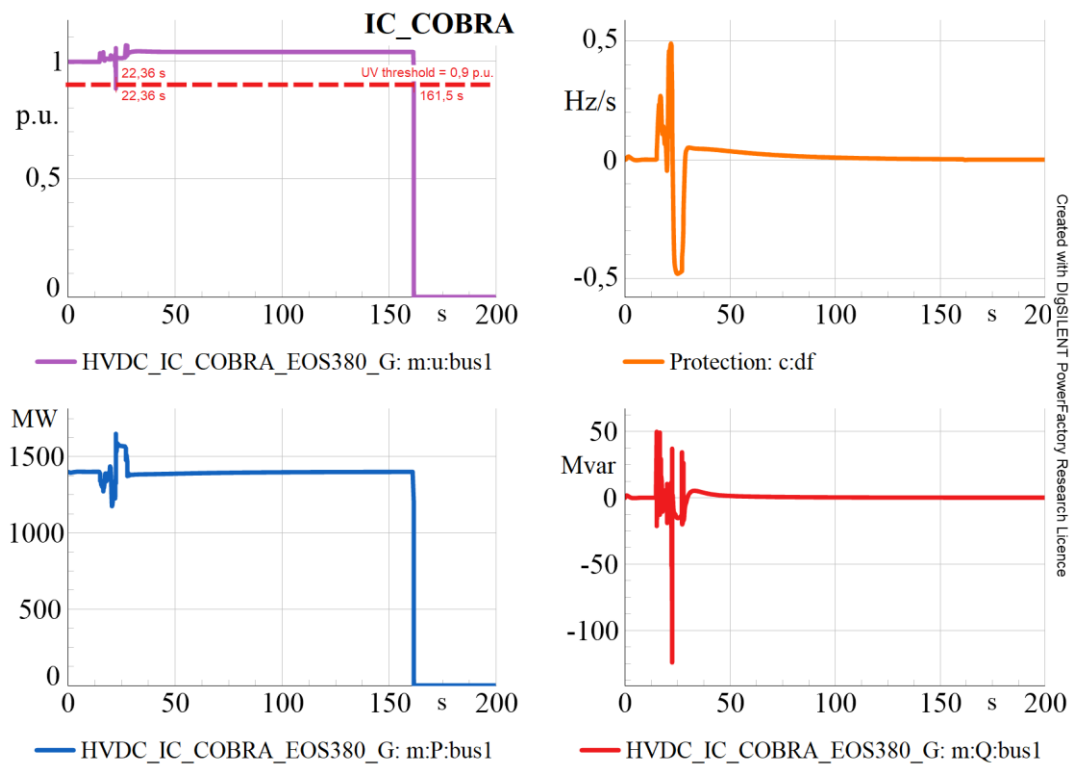


Figure 23: Under voltage tripping of IC_Cobra

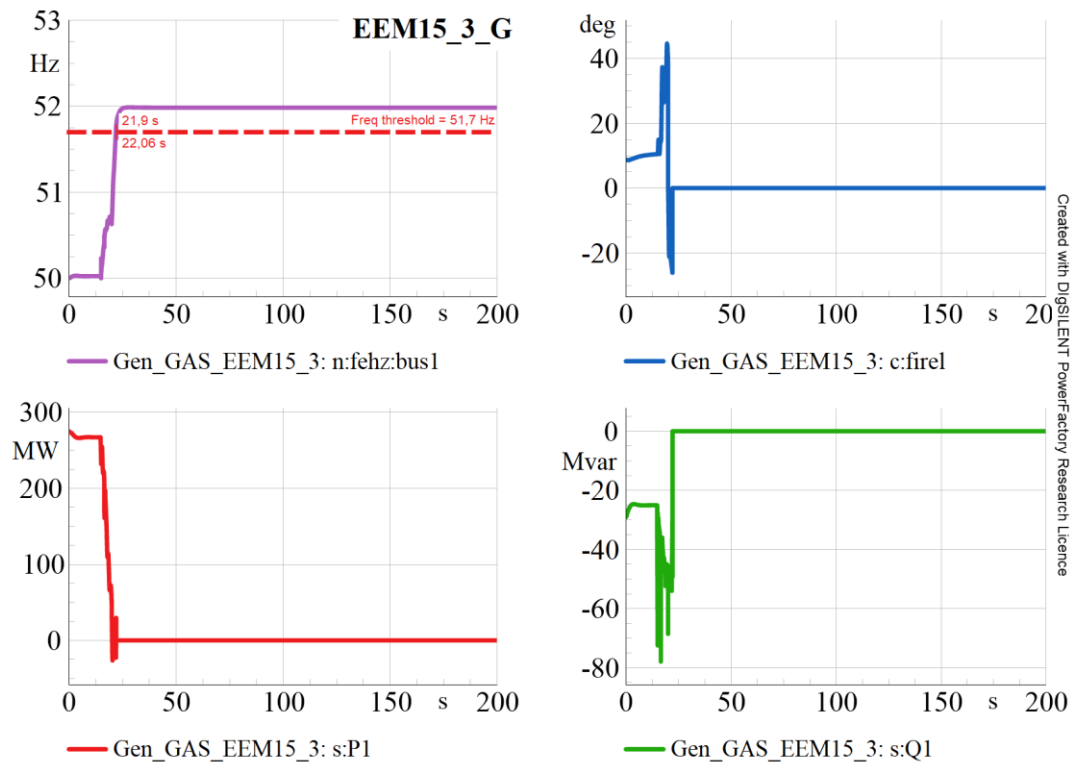


Figure 24: Over frequency tripping of EEM15_3 generator

6.2.1.3 Spoofing attack use case

In this attack scenario, it is assumed that the cyberattacker has gained unauthorized access to the system by exploiting existing vulnerabilities and can manipulate system parameters, such as disabling protection settings or changing controller reference set points. In this use case, the attacker modifies the reference set point of the Automatic Voltage Regulator (AVR) of the NDR380 generating unit, introducing voltage instabilities into the system before the generator is eventually disconnected by the protection scheme.

The attack is initiated at $t = 15$ s, and the affected generator is disconnected by the under-voltage protection scheme at $t = 24$ s, as summarized in Table 6-3. The loss of the generator causes power flow redistribution throughout the network, resulting in the overloading and subsequent tripping of several transmission lines. These outages ultimately lead to the formation of multiple uncontrolled electrical islands.

Once the islands are formed, severe voltage and frequency instabilities develop across the network. Automatic load-shedding operations are initiated to restore system stability; however, these actions inadvertently create further imbalances and accelerate the cascading failure process. Consequently, multiple generating units and wind plants are abruptly disconnected by frequency- and voltage-based protection schemes, resulting in approximately 80% load loss across the network as shown in Figure 26. As a result, almost the entire grid enters a blackout state, as shown in Figure 25. Figures 27–29 illustrate the cascading failure dynamics of generators and wind plants at different locations. The figures present the tripping of DIM15, BSL3_4, and BSL380 due to voltage and frequency

protection schemes, together with their corresponding power, voltage, frequency, and RoCoF responses.

Table 6-3: Sequence of event caused by spoofing cyberattack

Time(s)	Event	System Impact
15	The AVR set point of generator NDR380_G was maliciously changed to 0.9 p.u., introducing system disturbances without any immediate element disconnection.	Initiated voltage instability and abnormal operating conditions.
24	The targeted generator was disconnected by the under-voltage protection scheme.	Reduced local generation support and aggravated the generation–load imbalance.
24	Multiple transmission lines, including lines connected to the MBT380 bus, were disconnected by overload protection schemes.	Resulted in the formation of multiple uncontrolled islands with severe voltage and frequency instability.
32	Automatic load shedding of 7% was performed in one affected area to improve system stability.	Stabilized one island, while other areas remained unstable.
33	The system reached the point of no return and entered a rapid cascading failure phase.	Instabilities propagated throughout the network and became irreversible.
34-38	Additional 7% load shedding was performed in a second affected area.	Reduced demand but caused frequency overshoots in certain islands due to generation–load imbalance.
39.8	Multiple generators and wind turbines were disconnected by over-frequency protection schemes.	Triggered significant generation loss and accelerated the cascading failure process.
80	The system load reduced from approximately 25 GW to 5 GW.	Resulted in nearly 80% load loss, corresponding to widespread blackout conditions.

Digital Twin Power System Model

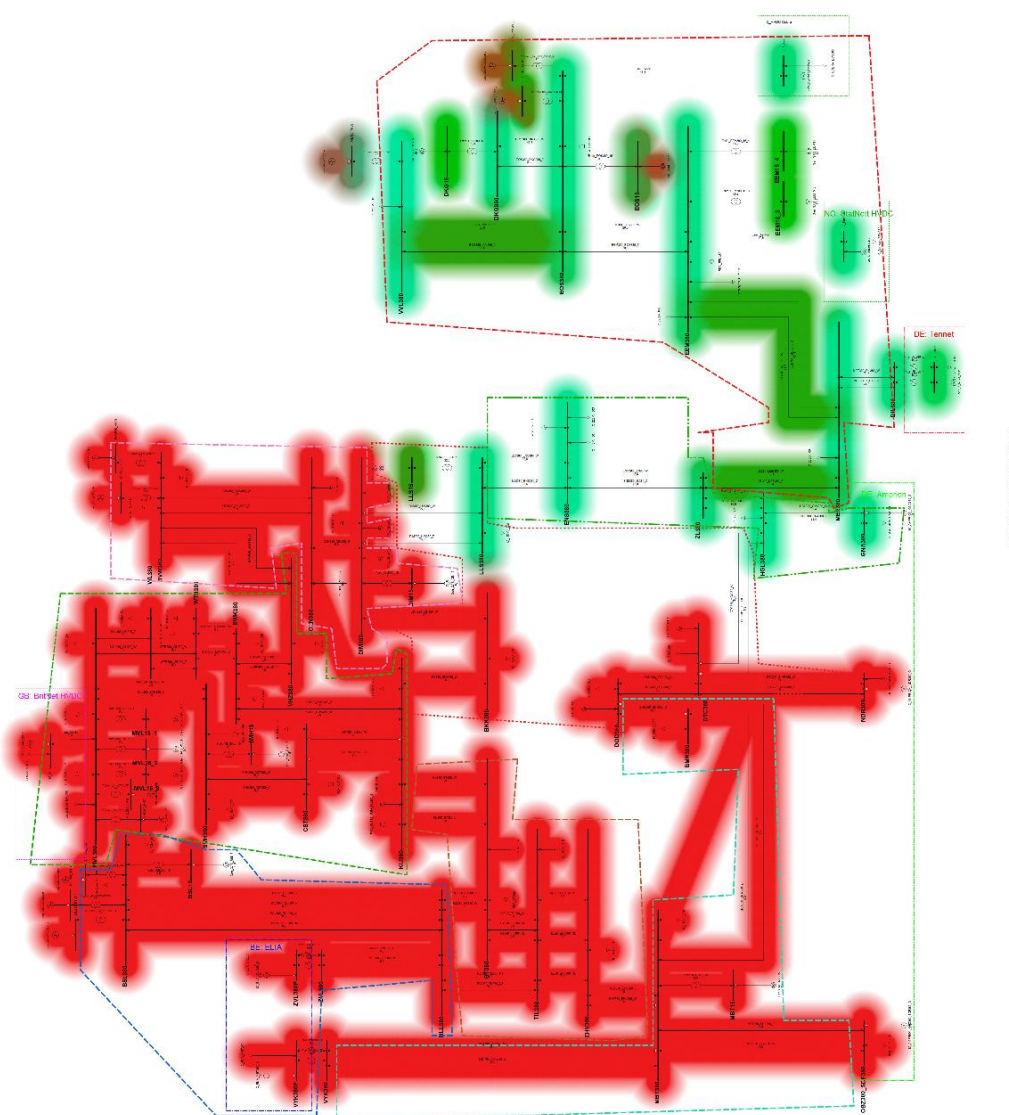


Figure 25: SLD of Dutch network blackout region caused spoofing cyberattack

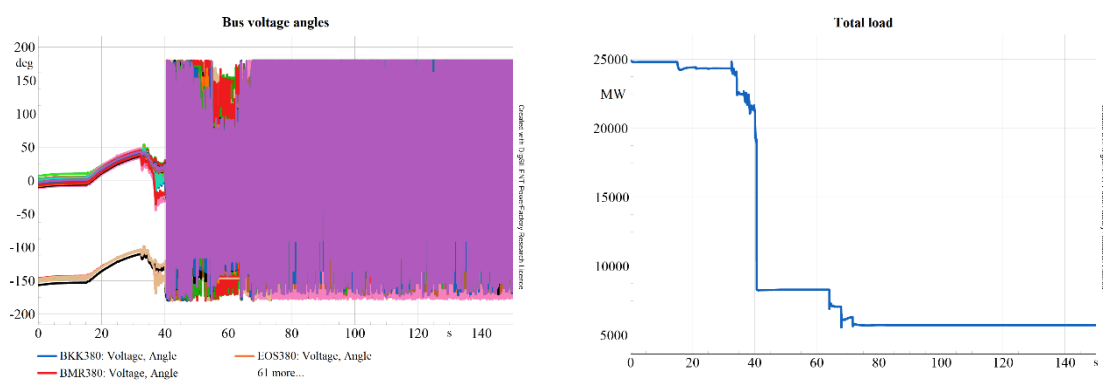


Figure 26: Bus voltage angles and total load caused spoofing attack

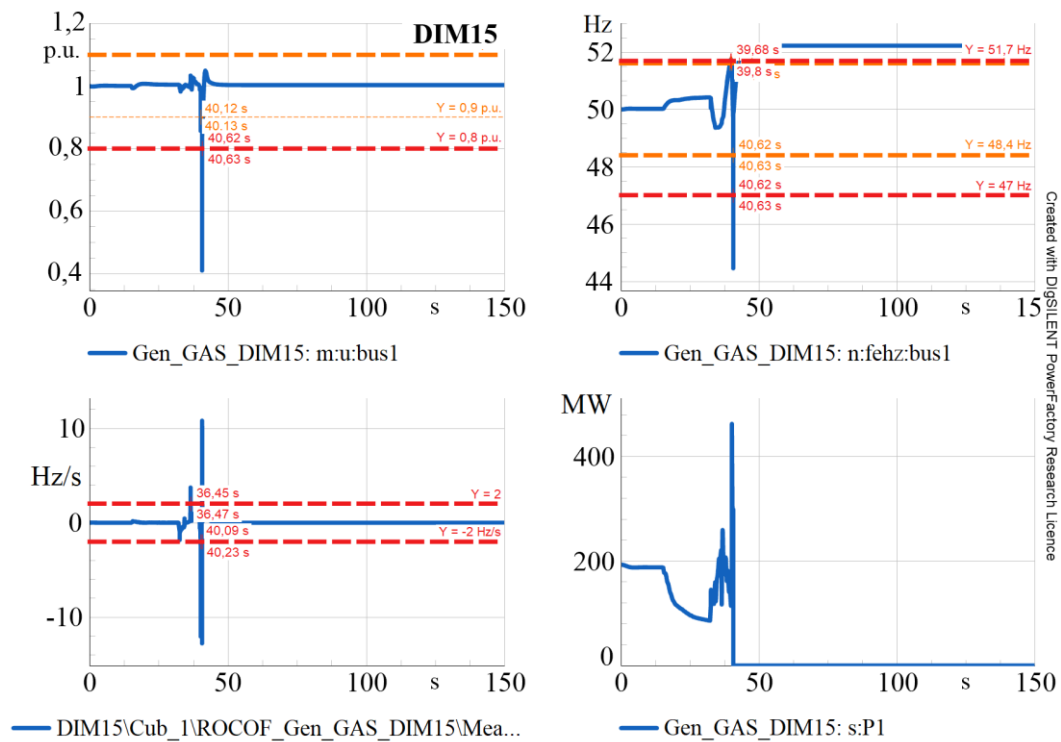


Figure 27: Over frequency tripping of DIM15 generator

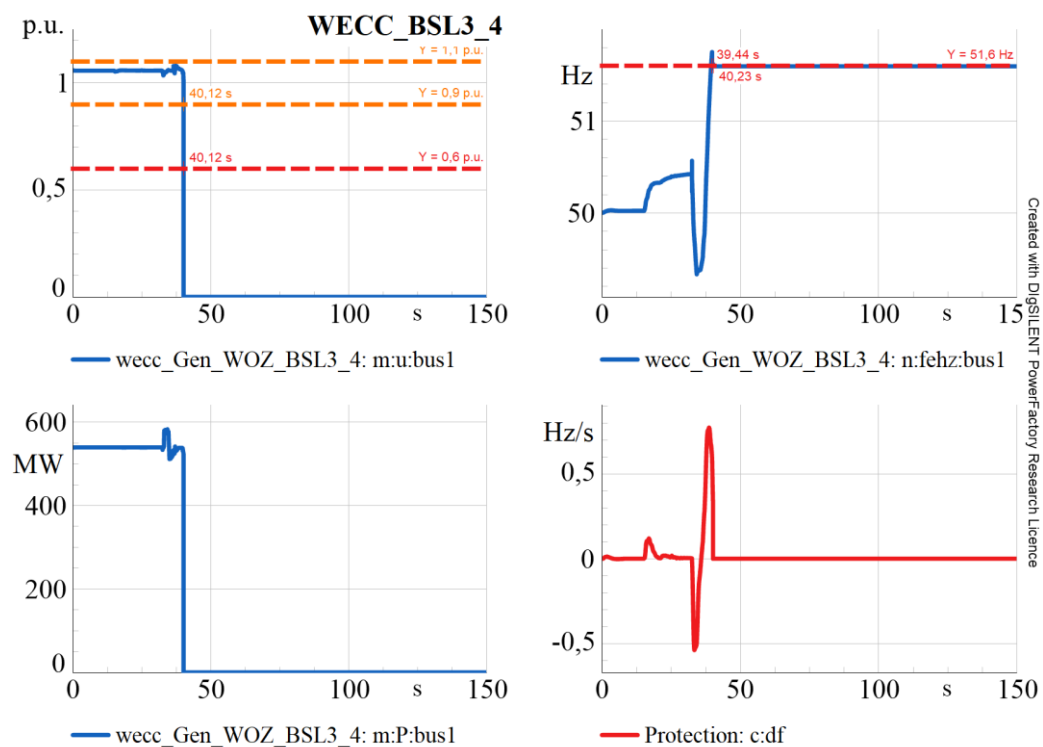


Figure 28: Over frequency tripping of wind plant BSL3_4

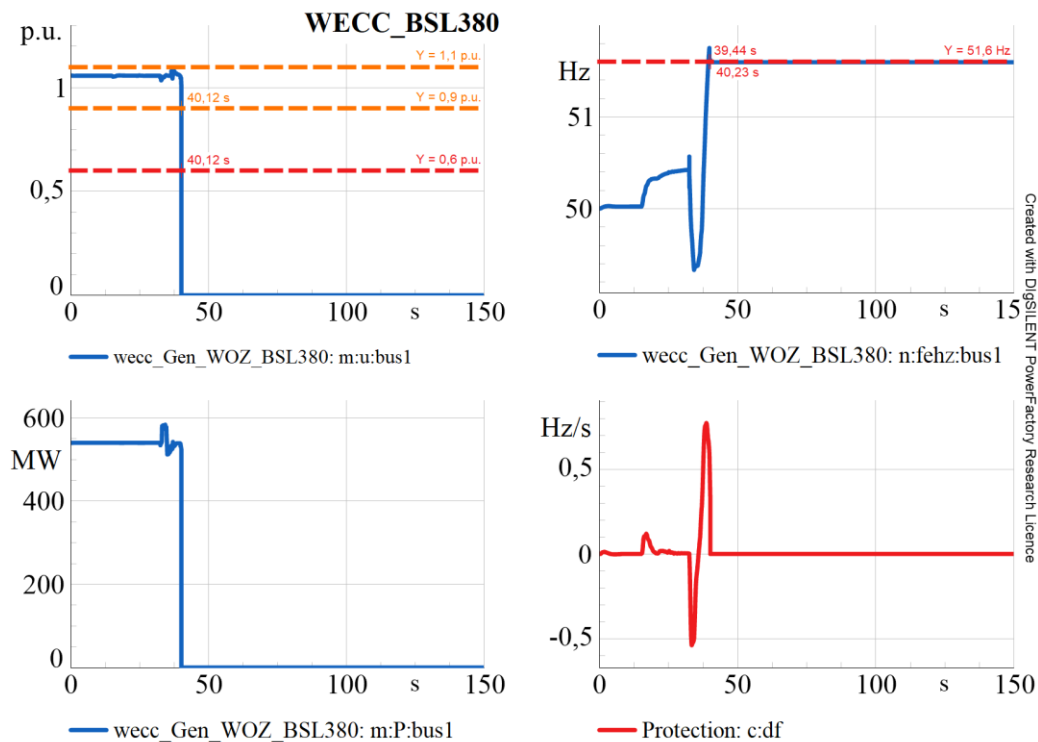


Figure 29: Over frequency tripping of wind plant BSL380

6.2.2 Lessons learned and recommendations

The digital twin can be utilized for a wide range of applications to forecast future operating scenarios by using the latest available measurements within a virtual environment. From the use case scenarios presented above, it is observed that a successful cyberattack at a single location can initiate multiple cascading events, such as transmission line overloading, generator tripping, and uncontrolled islanding, as secondary effects of the initial attack.

The cyberattacks can result in outcomes ranging from partial blackouts to full-scale system blackouts. A large number of cyberattack scenarios were generated and analysed, and the results indicate that cyberattacks can render the grid highly unstable within a very short period, rapidly driving the system into a fast cascading failure phase.

The results further suggest that once a cyberattack has been successfully executed, it is extremely difficult to stabilize or control the system using conventional reactive control strategies alone. Therefore, new control methodologies, advanced cybersecurity mechanisms, and preventive mitigation techniques are required to enhance grid resilience and limit the propagation of cyber-induced cascading failures.

Quantifying the exact operating PNR and differentiating between slow-cascade and fast-cascade pathways would reveal how protection settings and system conditions interact to define irreversibility. These findings would be useful in developing mitigation strategies by establishing quantitative operational limits that maintain safe margins before reaching an irreversible failure state. Understanding this critical transitional point could enable the development of preventive control methodologies and advanced cyber security mechanisms that can trigger early intervention before the system becomes uncontrollable, providing evidence-based recommendations for grid code modifications that enhance overall resilience against cyber-induced cascading failures.

7 Development of a Digital Twin for Training

The French demonstrator focuses on the development of a cyber-physical Digital Twin for training system operators on complex and stability-critical operational situations. The objective is to reproduce a control-room-like environment where operators can be trained on realistic grid and communication-network events, while also enabling the testing of new decision-support assistants and automation modules under representative operating conditions.

The demonstrator addresses both the physical layer of the power system and the cyber layer that supports system operation. The physical layer is represented through a dynamic grid simulator based on Dynawo, while the cyber layer is represented through telecommunication and information-flow modelling, including SCADA-related exchanges, delays, loss of observability, and other communication effects. This enables the training environment to reproduce not only classical power-system disturbances, such as outages and overloads, but also cyber-physical events that affect the information available to operators.

A key ambition of the French demonstrator is to move beyond small test systems and support realistic operational studies on the French transmission network. The platform is designed to operate on large-scale network models, with more than 6000 electrical nodes and more than 13000 lines and transformers. This scalability objective is important because operator training and decision-support validation must be performed under conditions that are representative of real transmission-system operation.

The demonstrator also supports the validation of advanced decision-support assistants developed in R&D activities. These assistants may rely on artificial intelligence, robust optimization, model predictive control, or other advanced techniques to help operators manage uncertainty and operational complexity. The Digital Twin provides a controlled environment where such modules can be connected, tested, compared, and assessed before deployment in real operational contexts.

7.1 Scenarios for training

The training scenarios are designed to expose operators to realistic cyber-physical situations involving both grid events and communication-network events. The scenario demonstrated focuses on an overload management case in a local area of the French network.

The demonstrated area contains a substation with three transformers. During the scenario, the trainer opens two of the transformers. This situation can represent, for example, a planned outage on one transformer combined with a fault or unavailability on a second transformer. As a result, the power flow is transferred to the third transformer, creating an overload constraint. The trainee must analyze the situation using the SCADA interface and identify an appropriate remedial action to remove the overload.

The first remedial action demonstrated is a topological action. The trainee opens the busbar coupler at the relevant voltage level. This action changes the substation topology and redistributes the flows. After the action is applied, the flow on the overloaded transformer is reduced and the overload constraint disappears. This demonstrates how the training platform can be used to reproduce a realistic operator decision-making process, where the operator observes the system state, identifies the constraint, applies a corrective action, and verifies the system response.

The scenario also demonstrates the difference between the trainer's view and the trainee's view. The trainer has access to the full simulated system state, including all variables and constraints. The trainee, however, receives a SCADA-like operational view based on measurements, events, and estimated values. This separation is essential for realistic training, because operators in real control rooms do not have direct access to the complete internal state of the simulated system.

In the trainee SCADA view, the operator can observe active and reactive power values, measured values updated at regular intervals. The demo shows that measured values are refreshed periodically, while estimated values are also available to support situational awareness. For example, measurements on transformer flows are displayed on curves, with markers indicating newly received measurements. The trainee must interpret these signals to understand the operational situation.

The scenario then introduces a cyber-physical event: loss of observability on the telecommunication grid. This event is injected from the trainer side using a DSL-based command. The loss of observability affects the trainee view but not the trainer view. The trainer can still observe the complete system state, while the trainee no longer receives updated information for the affected substation. This demonstrates the ability of the platform to simulate communication disturbances and assess their impact on operator awareness and decision-making.

The loss-of-observability case is particularly important because it reproduces situations where the physical grid continues to evolve, but the operator's view becomes incomplete or outdated. In the demo, changes made to breakers or topology are not immediately reflected in the trainee SCADA view while observability is lost. This creates a realistic training condition where the trainee must operate under degraded information.

After observability is restored, the scenario returns to the overload condition and demonstrates a second type of remedial action: generation reduction. In this case, the Game Master mimics the role of a producer or generation operator by reducing the output of nearby generation units. The demonstrated example refers to several generation units located close to the congestion area. A DSL function is used to reduce production with a ramp over a defined period. The first generation reduction is not sufficient to remove the constraint, so additional generation reduction actions are applied until the overload is relieved.

The demonstrated scenario therefore covers several important training dimensions:

- physical grid contingencies, including transformer outages and overloads;
- topology-based remedial action through busbar-coupler operation;
- cyber-physical disturbance through loss of observability;
- degraded operator awareness due to missing or outdated SCADA information;
- generation redispatch or production reduction as a remedial strategy;
- comparison between trainer state view and trainee SCADA view;
- use of DSL commands for scenario execution and event injection.

This scenario provides a representative proof of concept for training operators on realistic operational conditions where physical events, cyber events, and human decisions interact.

7.2 Description of the training activities

The training activity is organized around two main roles: the trainer and the trainee. The trainer prepares and supervises the training session through the Game Master environment. The trainee participates as the system operator and interacts with the simulated grid through a SCADA-like interface. The two views operate in parallel, but they do not provide the same level of information.

Before the exercise starts, the trainer logs into the training lobby and creates a session. A session corresponds to a set of files and configuration elements required to run the exercise, including the power-grid case, dynamic data, cyber configuration, and the scenario to be played. Once the session is created, the trainer can enter the active session as Game Master and start the simulation.

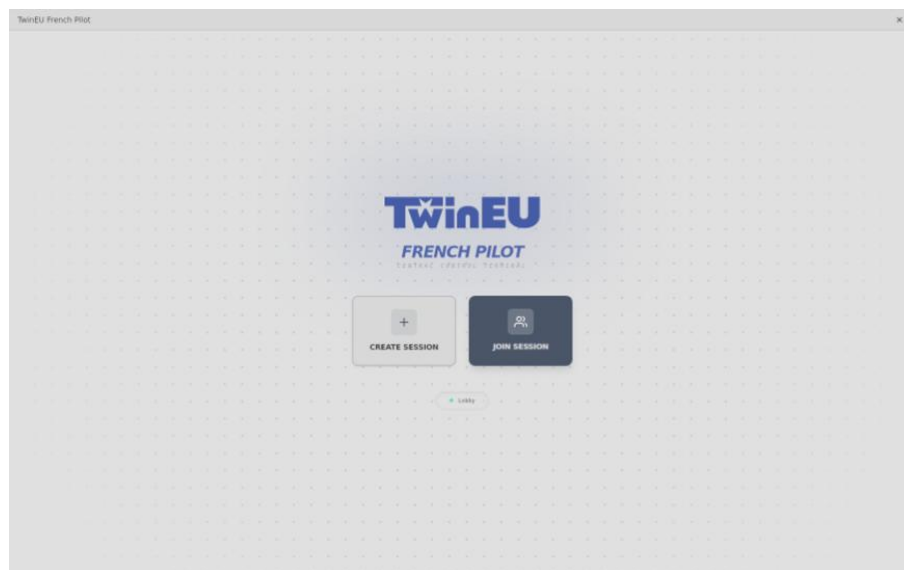


Figure 30: Training Session Lobby

The image shows a "Create Session" modal form within the "TwinEU French Pilot" application. The form has a title bar with a plus icon and a "Back" button. It contains several input fields: "Session name" with the value "scenario_MQIS_NB", "Configuration" section with "Context name" and "DSL name" both set to "scenario_MQIS_NB", and "Config path" with the placeholder text "Enter optional config path". At the bottom of the form is a dark blue button labeled "Create session".

Figure 31: Session Creation Interface

When the simulation starts, the platform initializes the different components of the training environment. These include the Game Master, Orchestrator, Grid Simulator, Asset Simulator, Information Flow Model, SCADA Emulator, logging system, and KPI-related components. The Orchestrator is responsible for coordinating these components and managing the execution timeline.

The Game Master interface provides the trainer with access to the full state of the simulated system. This includes complete grid information, simulated values, active constraints, and relevant curves showing the evolution of selected variables. In the demonstrated case, the trainer displays the substation of interest and monitors the status of transformer flows, voltage constraints, and other system variables.

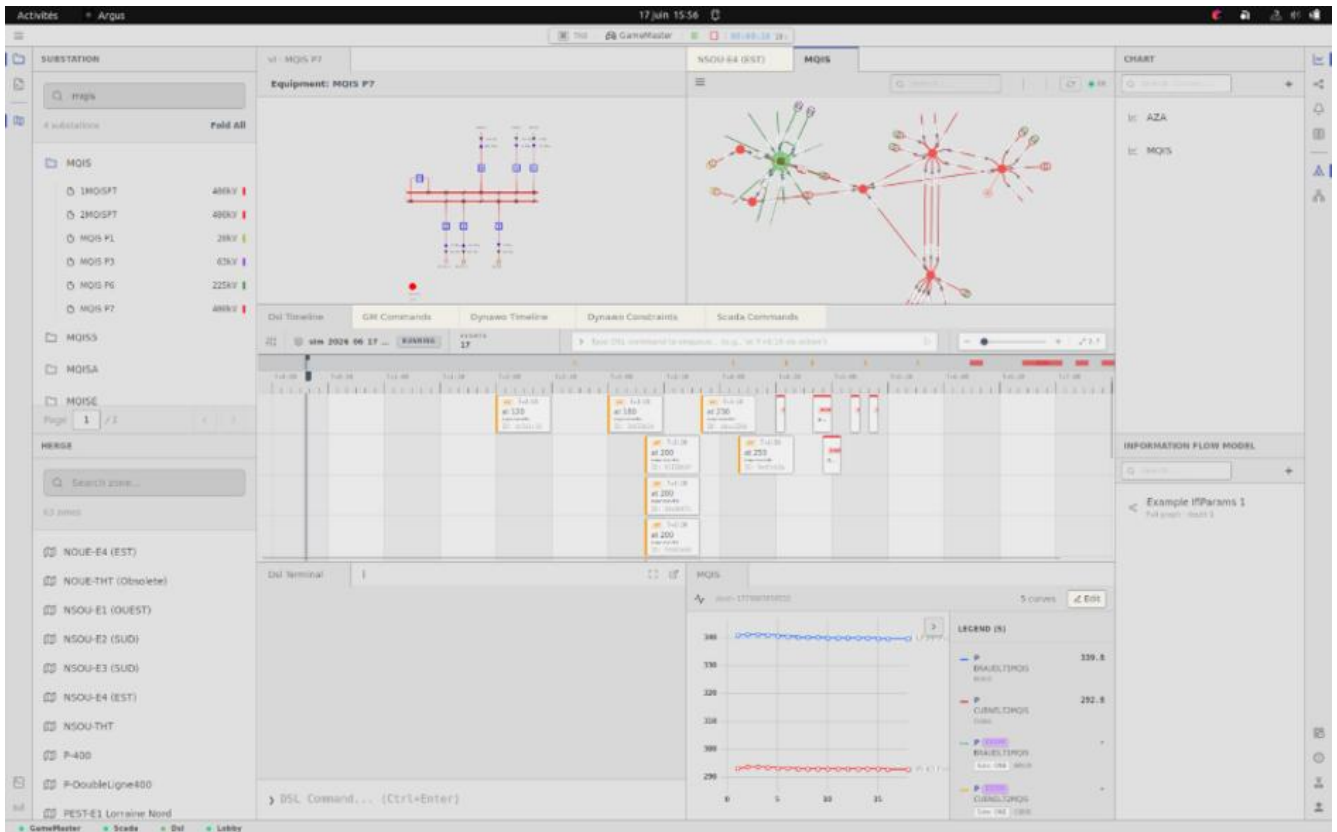


Figure 32: Game Master View of the Simulated Substation

The trainer can then introduce events into the scenario. In the overload scenario, the trainer opens the breakers of two transformers. These actions are processed by the Orchestrator and propagated to the relevant simulation components. The resulting physical response is calculated by the Dynawo Grid Simulator and reflected in the system variables. The trainer can observe the resulting changes directly in the full state view.

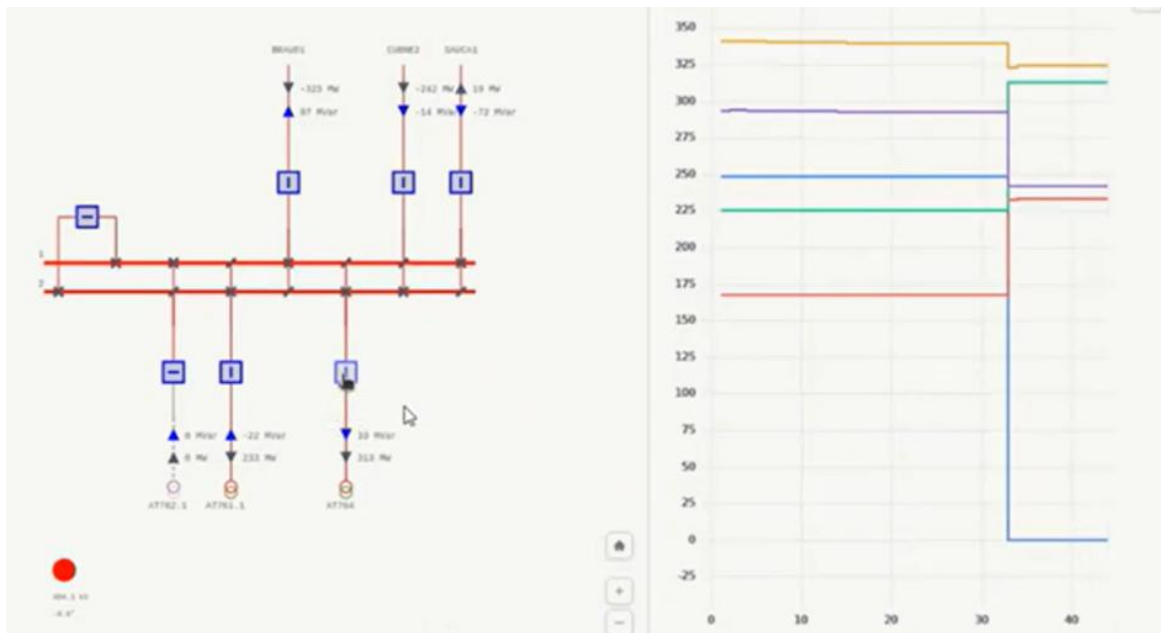


Figure 33: Trainer opens the breaker of two transformers

The trainee interacts with the system through the SCADA Emulator. This view is designed to reproduce the type of operational information available to a dispatcher in a control room. The trainee receives measurements, events, alarms, estimated values, and available controls. The trainee can also send commands and setpoints to the system.

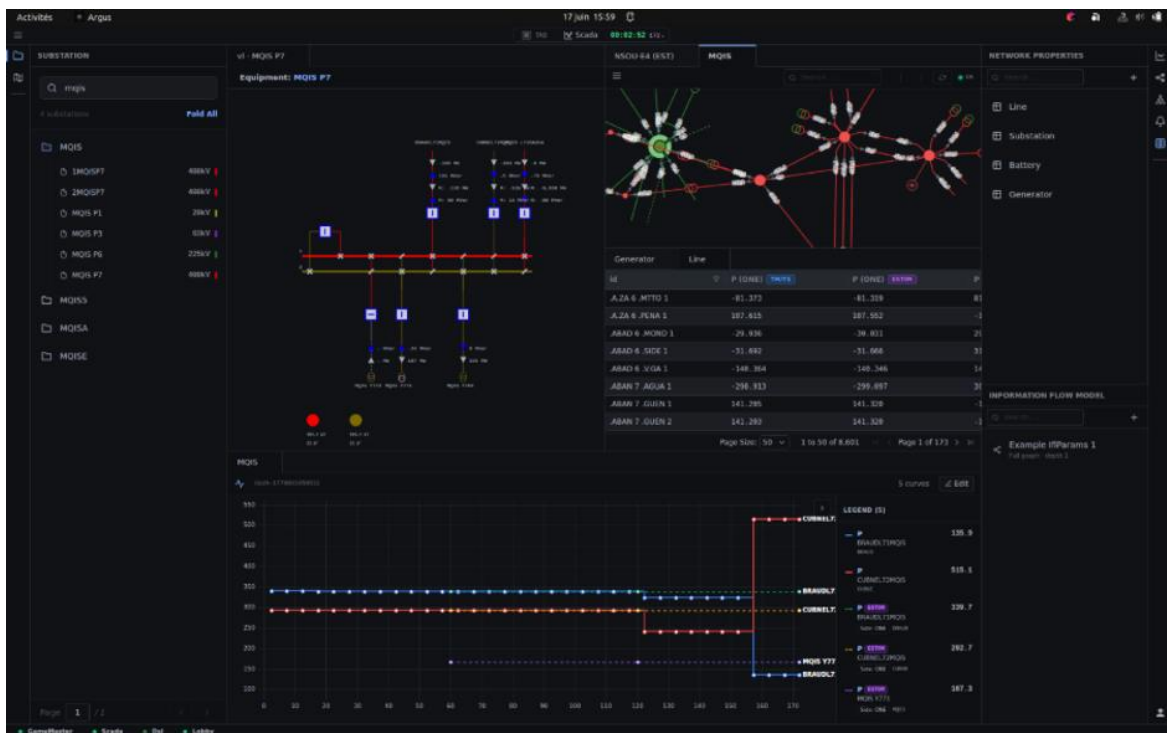


Figure 34: Trainee View

In the demonstrated scenario, the trainee observes that two transformer flows become zero after the trainer opens the corresponding breakers. The flow on the remaining transformer increases, leading to an overload constraint. The trainee must identify the constraint and decide how to act. The

SCADA interface supports this decision-making process by displaying measurements, curves, alarms, logbook entries, and active constraints.

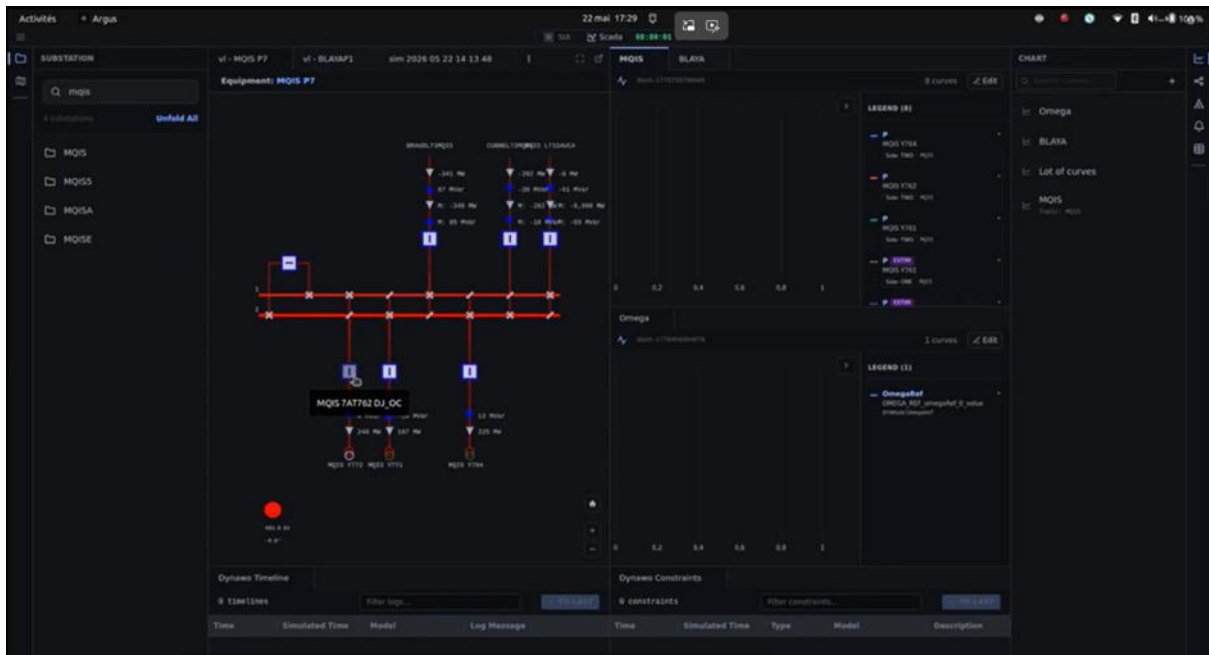


Figure 35: Trainee SCADA view during the overload scenario

The trainee then performs a topological remedial action by opening the busbar coupler. This action is sent through the SCADA interface and processed by the Orchestrator. The Orchestrator updates the relevant simulation components, and the new network state is computed. After the action, the flow on the overloaded transformer decreases and the overload constraint disappears. This confirms that the trainee action successfully relieved the constraint.

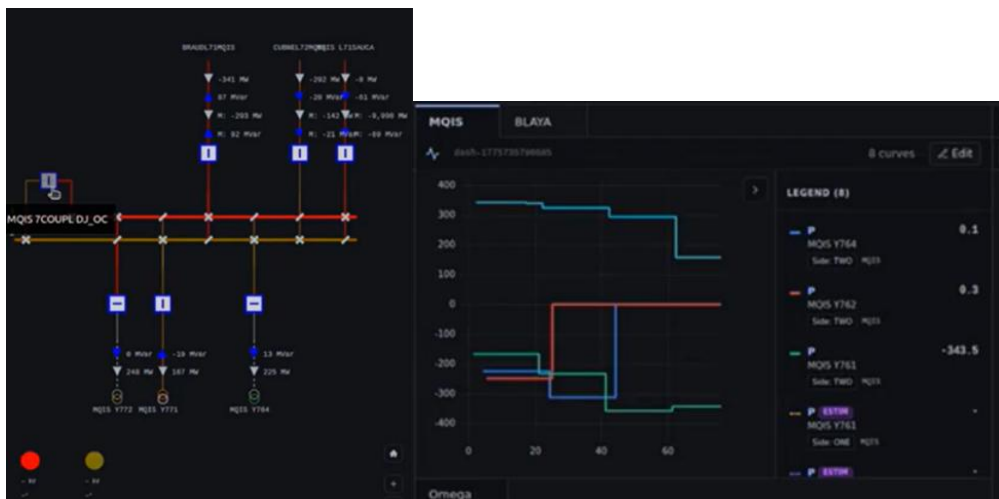


Figure 36: Topological remedial action through busbar-coupler opening

The training activity also includes cyber-event handling. In the demonstrated loss-of-observability case, the trainer injects a telecommunication event using DSL commands.

```

1 // Example DSL file for power system simulation
2 // Compatible with French THT-HT network
3
4 // Set simulation parameters
5 set simulation duration to 30000 seconds;
6 set time step to 1 seconds;
7
8 // Time-based events
9
10 // Outage of AT 762 in voltage level MQIS P7
11 open switch "MQIS P7_MQIS 7AT762 DJ_OC";
12
13 // Fault (simulated by breaker opening on an AT)
14 open switch "MQIS P7_MQIS 7AT764 DJ_OC";
15
16 // RA#1
17 open switch "MQIS P7_MQIS 7COUPL DJ_OC";
18
19 // Undo RA#1
20 close switch "MQIS P7_MQIS 7COUPL DJ_OC";
21
22 // Redo RA#1 - but with communication link out of order
23
24 // Lose communication with MQIS RTU
25 change network characteristics link from "RTU_ICCP_MQIS" to "FLOIR", drop fixed true;
26 change network characteristics link from "FLOIR" to "RTU_ICCP_MQIS", drop fixed true;
27
28 open switch "MQIS P7_MQIS 7COUPL DJ_OC";
29
30 // Recover MQIS RTU
31 change network characteristics link from "RTU_ICCP_MQIS" to "FLOIR", drop fixed false;
32 change network characteristics link from "FLOIR" to "RTU_ICCP_MQIS", drop fixed false;
33
34 // Undo RA#1
35 close switch "MQIS P7_MQIS 7COUPL DJ_OC";
36
37 // Lower generator production

```

Figure 37: DSL Commands

The event affects the information received by the trainee but does not affect the trainer's full state view. This allows the trainer to supervise the real system state while the trainee experiences degraded observability. Such exercises are valuable for training operators to manage situations where measurements or switch statuses are unavailable, delayed, or inconsistent.

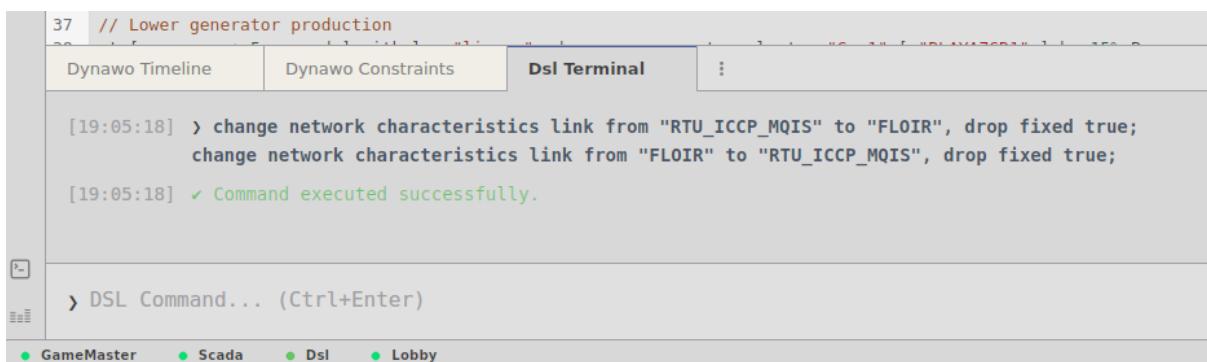
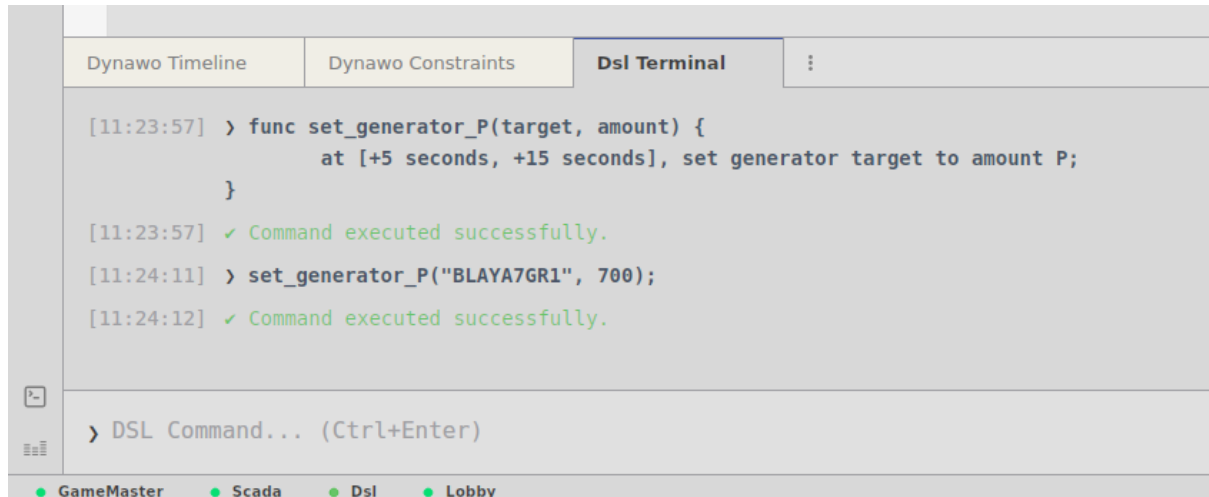


Figure 38: Loss of observability event injected through DSL

The scenario also demonstrates the effect of degraded observability on operator decision-making. The trainer injects a loss-of-observability event on the telecommunication side using DSL commands. This event does not affect the trainer's view, which continues to display the complete simulated system state, but it affects the trainee's SCADA view. As a result, the trainee may no longer receive updated measurements or switch states for the affected substation. Although state estimation can

still provide partial information based on the remaining available measurements, the actual state of the affected substation is not fully visible to the trainee until observability is restored.

After restoring observability, the scenario is brought back to the overload condition to demonstrate an alternative remedial action. Instead of modifying the topology, the Game Master mimics the role of a producer or generation operator and reduces the output of nearby generation units. This action is executed through a DSL function that applies a ramped generation reduction over a defined time period.



```

Dynawo Timeline | Dynawo Constraints | Dsl Terminal | ⋮
[11:23:57] > func set_generator_P(target, amount) {
                at [+5 seconds, +15 seconds], set generator target to amount P;
            }
[11:23:57] ✓ Command executed successfully.
[11:24:11] > set_generator_P("BLAYA7GR1", 700);
[11:24:12] ✓ Command executed successfully.

DSL Command... (Ctrl+Enter)

● GameMaster ● Scada ● Dsl ● Lobby

```

Figure 39: Use of DSL function to reduce generation output with a ramp

The first reduction may not be sufficient to remove the overload, requiring additional generation reductions on other units. This demonstrates how the training platform can compare different types of remedial strategies, including topology-based actions and generation-based actions, under the same simulated operational condition.

This allows the same training session to combine multiple phases: normal operation, physical contingency, corrective operator action, cyber disturbance, recovery of observability, and alternative remedial action. The trainer can therefore adapt the scenario dynamically according to the trainee's response.

The training activity can also involve decision-support assistants or external automation modules. The architecture allows these modules to be connected through SCADA-like interfaces and to receive measurements, signals, commands, or setpoints. This makes it possible to compare the behavior of human operators, automata, and assistant modules under the same scenario conditions.

The logging system records the evolution of the session, including events, operator actions, simulated values, alarms, and constraints. This information supports post-session analysis and debriefing. The trainer can review what happened during the exercise, assess whether the trainee correctly identified the operational issue, evaluate the selected remedial action, and compare the outcome with alternative strategies.

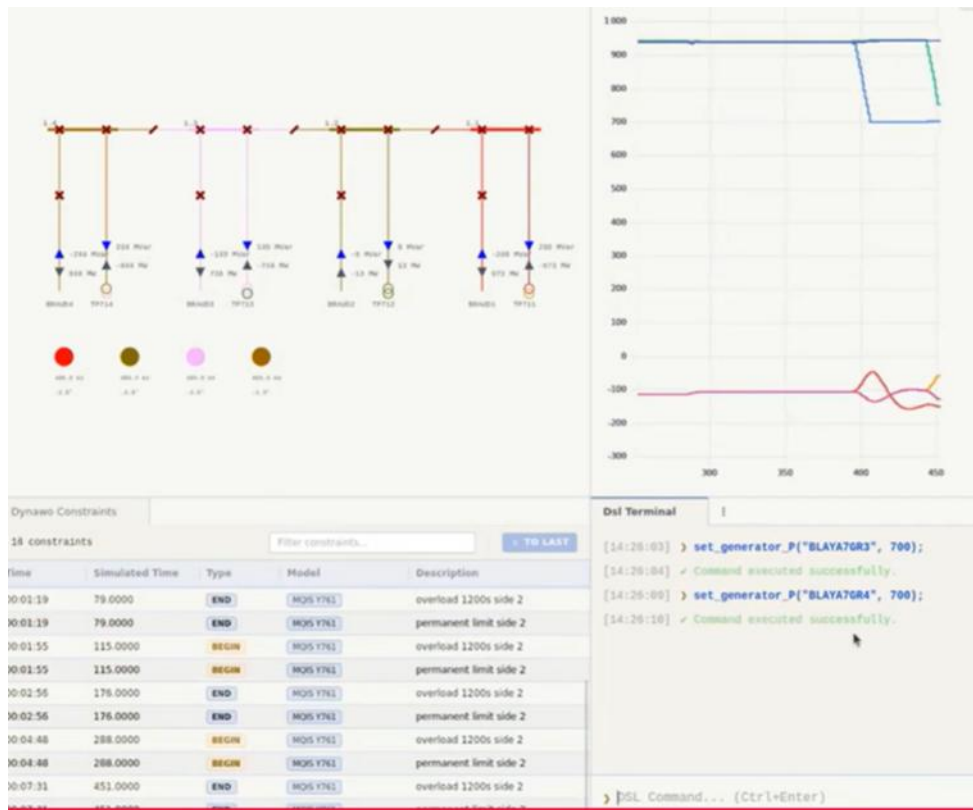


Figure 40: Generation reduction as an alternative remedial action

Overall, the training activity follows a complete operational workflow:

1. The trainer creates and configures a training session.
2. The simulation environment is initialized.
3. The trainer starts the scenario and injects events.
4. The trainee observes the SCADA view through measurements refresh rate and state estimation (every 10 seconds in France) and analyses the system state.
5. The trainee performs corrective actions.
6. The system response is simulated in real time.
7. Cyber events such as loss of observability can be introduced.
8. The trainer monitors the complete state and supervises the exercise.
9. Logs, alarms, constraints, and system states are recorded.
10. The session can be replayed or analysed for debriefing and KPI computation.

This workflow demonstrates how the French Digital Twin supports operator training, scenario-based learning, cyber-physical resilience assessment, and validation of future decision-support functions.

7.3 Lessons learned and recommendations

7.3.1 Lessons Learned

The development and demonstration of the French Digital Twin for operator training provided several useful lessons:

- First, the demonstration showed that realistic operator training should include both the electrical grid and the communication layer. Operators need to be trained not only on physical events such as outages and overloads, but also on communication problems such as loss of observability, missing measurements, or delayed information.
- Second, the separation between the trainer view and the trainee view is important. The trainer needs access to the complete system state in order to supervise the exercise, while the trainee should only see the information normally available in a control room. This makes the training more realistic.
- Third, the loss-of-observability scenario showed the value of cyber-physical training. In this case, the physical grid continues to change, but the trainee does not immediately see all updates in the SCADA view. This helps operators practice decision-making when information is incomplete or outdated.
- Fourth, the demonstration confirmed that different remedial actions can be tested in the same training environment. In the overload scenario, the trainee first used a topological action by opening a busbar coupler. The scenario also showed another option, where generation was reduced using DSL commands. This makes it possible to compare different operational responses.
- Fifth, the use of DSL commands is useful for the trainer. It allows the trainer to launch events, modify the scenario, simulate cyber effects, and test different corrective actions during the session.
- Finally, logging and replay are essential for effective debriefing. Recording events, operator actions, constraints, and system states allows the trainer to review the session afterwards and assess the trainee's response.

The overload scenario presented in this deliverable is used as a baseline scenario to demonstrate the end-to-end training workflow, including event injection, physical grid response, SCADA- based trainee interaction, degraded observability, remedial actions.

The advanced scenario reported in Deliverable 5.1 [2], includes the testing of the NAZA, Nouvel Automate de Zone Adaptatif (New Adaptive Zone Automation) automaton, which is a cyber-physical congestion management automaton. Full experimentation of more complex scenarios with operators is planned during the exploitation phase.

7.3.2 Recommendations

The main recommendation is to evolve the French Digital Twin from a proof-of-concept demonstration into a repeatable training environment. Priority should be given to scenario management, DSL extension, trainer and trainee interfaces, logging, KPI computation, configuration services, and integration of decision support tools.

8 Conclusion

This deliverable demonstrates that digital twins can fundamentally improve the way power systems are analysed, operated, and prepared for disruptions by enabling integrated cyber-physical assessment within a dynamic and controlled environment. Across transmission, distribution, and operator-training applications, the developed digital twins successfully captured complex interactions between physical infrastructure, communication networks, control systems, and human operators. The results show that cyber and physical phenomena are tightly interconnected and that disturbances originating in either domain can rapidly propagate across system layers, producing consequences that are often difficult to identify through conventional analysis approaches.

A key finding of this work is that modern power systems are increasingly exposed to cyber-physical risks whose impacts can range from local operational disturbances to large-scale system-wide failures. The work performed in Task 5.2 demonstrated how successful cyberattacks can initiate cascading events leading to transmission-line overloads, uncontrolled islanding, generation loss, and extensive service interruptions. Depending on the attack scenario, load losses ranging from approximately 36% to 80% were observed, highlighting the potentially severe consequences of cyber-induced cascading failures. An important observation was the identification of a “point of no return”, beyond which conventional protection schemes and corrective actions are unable to prevent system collapse. These findings underline the importance of preventive cybersecurity measures and predictive resilience assessment capabilities capable of identifying emerging threats before cascading failures become irreversible.

At the same time, the activities carried out in Task 5.3 demonstrated that coordinated flexibility activation from battery energy storage systems can effectively mitigate congestion and maintain acceptable voltage profiles in distribution networks with high renewable-energy penetration. The proposed digital twin framework successfully combined real-time simulation, hardware-in-the-loop integration, and optimisation-based control to improve operational performance under stressed operating conditions. However, the cybersecurity assessment revealed the strong dependence of optimisation-driven control schemes on the integrity of measurements and control signals. False-data injection and command-manipulation attacks resulted in physical constraint violations, inefficient resource utilisation, and degraded controller performance despite relatively small modifications of the underlying data. These findings reveal a fundamental trade-off between operational efficiency and cyber resilience and emphasise the need for robust data validation, anomaly detection, and resilient control architectures.

Beyond technological solutions, the digital twin developed within Task 5.5 highlighted the critical role of human operators in maintaining system resilience. The demonstrated training scenarios showed that communication failures and loss-of-observability events can significantly affect situational awareness and decision-making, even when the physical network remains stable. The results confirm that resilience assessment should not be limited to physical infrastructure and automation systems but must also consider the impact of cyber events on operator performance. Furthermore, the platform demonstrated the value of digital twins as environments for training system operators and validating advanced decision-support assistants and automation solutions prior to deployment in real operational settings.

Taken together, the results of Tasks 5.2, 5.3, and 5.5 confirm that digital twins provide a unique environment for understanding vulnerabilities, evaluating resilience-enhancement measures,

validating advanced control strategies, and preparing operators for complex cyber-physical situations. The ability to safely reproduce severe operational conditions that cannot be practically tested on real infrastructure constitutes one of the most important advantages of digital twin technology. Furthermore, the results consistently demonstrate that cyber resilience, physical resilience, and human preparedness should be treated as complementary dimensions of a common resilience framework rather than as separate challenges.

Based on the findings of this work, several recommendations emerge. First, resilience assessment frameworks should explicitly integrate cybersecurity considerations into both system planning and operation rather than treating cyber and physical domains separately. Second, future control and optimisation platforms should incorporate mechanisms for anomaly detection, data validation, and secure communication in order to improve tolerance against malicious interference and data uncertainty. Third, monitoring and protection systems should evolve towards predictive and adaptive approaches capable of identifying emerging cascading failures before critical thresholds are exceeded. Finally, continuous operator training and validation through realistic digital twin environments should become an integral part of future grid-resilience strategies, ensuring that both human operators and automated systems can respond effectively to increasingly complex cyber-physical threats.

Digital twins are expected to play a central role in the evolution of future power systems as grids become increasingly decentralised, digitalised, and interconnected. Their ability to combine real-time monitoring, simulation, cybersecurity assessment, operator training, and decision-support validation within a unified framework makes them a key enabling technology for resilient grid operation. The work presented in this deliverable demonstrates that digital twins are far more than simulation tools. They provide a comprehensive cyber-physical environment for analysing vulnerabilities, validating mitigation strategies, training operators, and supporting the transition towards more resilient and secure energy systems. Their continued development and integration into power-system planning and operation will be a key enabler for addressing the challenges associated with the future energy transition.

References

- [1] TwinEU project, Deliverable 2.2, “TwinEU Use Cases, pan-European scenarios and KPIs”, June. 2025, [online] Available: https://twineu.net/wp-content/uploads/2025/07/TwinEU_D2.2_v1.0-3.pdf.
- [2] TwinEU project, Deliverable 5.1, “From conceptual use cases to real demonstration – Digital Twin for cyber-physical grid resilience”, June. 2026, [online] Available: <https://twineu.net/deliverables/>
- [3] M. Venkatasubramanian and K. Tomsovic, Power System Operation and Control, no. April. 2004. doi: 10.1016/B978-012170960-0/50057-8.
- [4] M. Panteli, D. N. Trakas, P. Mancarella, and N. D. Hatziargyriou, “Power Systems Resilience Assessment: Hardening and Smart Operational Enhancement Strategies,” *Proc. IEEE*, vol. 105, no. 7, pp. 1202–1213, 2017, doi: 10.1109/JPROC.2017.2691357.
- [5] M. Panteli and P. Mancarella, “The grid: Stronger, bigger, smarter?: Presenting a conceptual framework of power system resilience,” *IEEE Power Energy Mag.*, vol. 13, no. 3, pp. 58–66, 2015, doi: 10.1109/MPE.2015.2397334.
- [6] EASAC, “Extreme weather events in Europe,” no. March, pp. 1–8, 2018, [Online]. Available: www.easac.eu
- [7] S. Peyghami, P. Palensky, and F. Blaabjerg, “An overview on the reliability of modern power electronic based power systems,” *IEEE Open J. Power Electron.*, vol. 1, no. March, pp. 34–50, 2020, doi: 10.1109/OJPEL.2020.2973926.
- [8] S. B. Aruna, D. Suchitra, R. Rajarajeswari, and S. G. Fernandez, “A Comprehensive Review on the Modern Power System Reliability Assessment,” *Int. J. Renew. Energy Res.*, vol. 11, no. 4, pp. 1734–1747, 2021, doi: 10.20508/IJRER.V11I4.12480.G8326.
- [9] M. M. Islam *et al.*, “Improving Reliability and Stability of the Power Systems: A Comprehensive Review on the Role of Energy Storage Systems to Enhance Flexibility,” *IEEE Access*, vol. 12, no. October, pp. 152738–152765, 2024, doi: 10.1109/ACCESS.2024.3476959.
- [10] C. Ye, L. Guo, Y. Ding, M. Ding, P. Wang, and L. Wang, “Reliability Assessment of Interconnected Power Systems with HVDC Links Considering Frequency Regulation Process,” *J. Mod. Power Syst. Clean Energy*, vol. 11, no. 2, pp. 662–673, 2023, doi: 10.35833/MPCE.2021.000491.
- [11] A. Salvi, P. Spagnoletti, and N. S. Noori, “Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem,” *Comput. Secur.*, vol. 112, p. 102507, 2022, doi: 10.1016/j.cose.2021.102507.
- [12] B. Somda and C. C. Liu, “Digital Twin for Resilient Power Distribution Systems,” *2024 22nd Int. Conf. Intell. Syst. Appl. to Power Syst. ISAP 2024*, pp. 1–6, 2024, doi: 10.1109/ISAP63260.2024.10744374.
- [13] W. Chai and Q. Ma, “Application of Digital Twin and Hologram Technology to Achieve Distribution Network Reliability Forecast,” *Proc. - 2022 7th Asia Conf. Power Electr. Eng. ACPEE 2022*, pp. 783–787, 2022, doi: 10.1109/ACPEE53904.2022.9784043.
- [14] ENTSO-E, *Rate of Change of Frequency (RoCoF) Withstand Capability: ENTSO-E Guidance Document for National Implementation for Network Codes on Grid Connection*, Brussels, Belgium, Mar. 29, 2017. [Online]. Available: https://eepublicdownloads.entsoe.eu/clean-documents/Network%20codes%20documents/NC%20RfG/IGD_RoCoF_withstand_capability_final.pdf

- [15] Northeast Power Coordinating Council (NPCC), *Automatic Underfrequency Load Shedding, PRC-006-NPCC-2*, NPCC Regional Reliability Standard, Apr. 25, 2024. [Online]. Available: <https://www.npcc.org/>