



*Establishment of a FramewORk for Transforming current
EPES into a more resilient, reliable and secure system all
over its value chain*

**D4.1 Self-healing and decision support techniques
for cascading effects and grid restoration**

Document details

Deliverable no	D4.1
Deliverable name	Self-healing and decision support techniques for cascading effects and grid restoration
Version	1.0
Release date	22/07/2025
Type	R
Dissemination level	SEN
Status	Final
Authors	TU Delft – Mohamed Radwan, Steven Tan, Yigu Liu, Bahman Ahmadi, Peter Palensky, Alexandru Ștefanov LINKS – Lorenzo Bongiovanni CIRCE – Marta Bernal, Gonzalo M. Sanchez RINA – Juan Guardiola



DISCLAIMER OF WARRANTIES

This document has been prepared by eFORT project partners as an account of work carried out within the framework of the EC-GA contract no. 101075665.

Neither Project Coordinator, nor any signatory party of eFORT Project Consortium Agreement, nor any person acting on behalf of any of them:

- a) makes any warranty or representation whatsoever, expressed or implied,
 - I. with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or
 - II. that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or
 - III. that this document is suitable to any particular user's circumstance; or
- b) assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if the Project Coordinator or any representative of a signatory party of the eFORT Project Consortium Agreement has been informed of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

This work has been 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 or European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.



Document history

Version	Date of issue	Content and changes	Edited by
0.1	28/02/2025	Table of Contents	TUD
0.2	28/05/2025	First draft	TUD, LINKS, CIRCE
0.3	09/06/2025	Second draft	TUD, LINKS, CIRCE
0.4	29/06/2025	Third draft	TUD, LINKS, CIRCE
0.5	17/07/2025	Fourth draft	TUD, CIRCE, CUERVA
1.0	22/07/2025	Final draft	TUD, CIRCE



Table of contents

Executive summary	14
1 Introduction	16
2 Cyber-Physical System Modelling and Power Grid Digital Twins.....	18
2.1 Cyber-Physical System Modelling and Co-Simulation	18
2.1.1 Physical Layer Modelling	19
2.1.2 Cyber Layer Modelling	22
2.1.3 Cyber-Physical Co-Simulation	23
2.1.4 CRoF CPPS Digital Twin Testbed	24
2.2 Large-Scale Cyber-Physical Synthetic Networks for TSO Applications	26
2.2.1 Generating a Triple Interdependent Cyber-Physical System	27
2.2.2 Two-Stage Generative Model for Large-Scale Synthetic CPPS	28
2.2.3 PCN Generator: Generating the Physical Communication Network	29
2.2.4 LCN Generator: Generating the Logical Communication Network	30
2.2.5 Case Study	31
2.3 Decentralized Digital Twins for DSO Services	36
2.3.1 Introduction	36
2.3.2 Italian Pilot Grid Description	36
2.3.3 Democratic Load Scaling (DLS)	37
2.3.4 Classical DLS Algorithm	38
2.3.5 Study of Quantities Dependence on Feeder Head Power	40
2.3.6 AI-based Democratic Load Scaling Algorithm	42
2.3.7 Sensitivity to Latent Dimension	45
3 Digital Twin Impact Analysis and Cyber Attack-Induced Cascading Failures	47
3.1 Introduction	47
3.2 Cyber Attack Simulation Scenarios	47
3.2.1 Single Substation Attacks	47
3.2.2 Two Substation Attacks	48
3.3 Cyber Attack Impact Assessment Method	48
3.4 Simulation Results and Cascading Failure Analysis	50



3.4.1	Cyber Attack-Induced Cascading Failures	50
3.4.2	Cyber Attack Impact Assessment	50
4	Power Grid Operational Security and Resilience Against Cascading Failures	55
4.1	Dynamic Stability Enhancement and Oscillation Damping in Transmission Systems	55
4.1.1	First Study: Damping Control with POD-P, POD-Q, and PSS	55
4.1.2	Second Study: Coordinated Optimization of STATCOM-POD Controllers in PST16 System	68
4.2	Self-Healing and Resilience Enhancement by Preventive Islanding Against Cyber-Induced Cascading Failures	71
4.2.1	Framework and Architecture of PI-GDP Model	73
4.2.2	Graph Representation and Feature Design	74
4.2.3	Self-Supervised Graph Autoencoder Module	76
4.2.4	Graph Partitioning Module	77
4.2.5	Case Study	80
5	Decision Support for Cyber-Physical Power System Restoration and Black-Start Recovery	84
5.1	Secure Black-Start Strategies for Power Grid Restoration	84
5.1.1	Objective	85
5.1.2	Restoration and Stepwise Approach	86
5.1.3	Mathematical Formulation	87
5.1.4	Use Cases & Modelling	89
5.2	Decision Support for Cyber-Physical Power System Restoration	97
5.2.1	Introduction	97
5.2.2	Problem Formulation of Cyber-Physical Power System Restoration	100
5.2.3	Reinforcement Learning Framework for Cyber-Physical Power System Restoration	104
5.2.4	Case Study	108
6	Conclusions and Next Steps	115
6.1	Conclusions	115
6.2	Next Steps	116



References	118
-------------------------	------------



List of figures

Figure 1. Co-simulation test bed implementation	19
Figure 2. IEEE 39-bus single line diagram with substations	20
Figure 3. PST 16 single line diagram	21
Figure 4. OT network emulated using Mininet.....	22
Figure 5. Virtualized network elements for the subnetwork of Substation 1	23
Figure 6. Schematic representation of OPC UA API	24
Figure 7. Overview of CRoF CPPS digital twin for Dutch TSO Pilot.	25
Figure 8. CPPS communication networks and substation communication architecture..	27
Figure 9. The Diagram of Two-Stage Generative Model	29
Figure 10. Generated Synthetic CPPS for Continental Europe.	33
Figure 11. Generated Synthetic CPPS for France.....	33
Figure 12. Comparison with traditional generative algorithms in the literature	35
Figure 13. Topology of Sarentino valley Electrical Grid.....	37
Figure 14. Classical iterative algorithm for democratic load scaling.....	38
Figure 15. Scaling factor vs. measured power for feeders	40
Figure 16. Grid Losses vs. measured power for feeders	41
Figure 17. AI based algorithm for democratic load scaling	42
Figure 18. Boxplot of the difference of the scaling factor computed with ML and Classical approaches.....	44
Figure 19. Boxplot of time for estimating the scaling factor for ML and Classical algorithms.....	44
Figure 20. Boxplot of the difference of scaling factor and estimating time with various latent dimension sizes.....	46
Figure 21. Time Domain Simulations of cascading effect after cyber attack.....	51
Figure 22. Scatter plot of simulated cyber attacks on substation 2.....	52
Figure 23. Probabilistic analysis of cyber attacks on Substation 2.....	53
Figure 24. Cyber Attack Impact Index (CAII) for all single-substation attacks.....	53
Figure 25. Cyber Attack Impact Index (CAII) for all two-substation attacks	54
Figure 26. PSS model block diagram.....	55
Figure 27. POD model block diagram.	56
Figure 28. Modified New England IEEE-39 power system model.....	56
Figure 29. Time domain simulation: frequency (top plot) and voltage (bottom plot).....	58



Figure 30. Eigenvalue diagram.	59
Figure 31. Polar diagram of the rotor speed observability factors in Mode 1	61
Figure 32. Results of Scenario 1	62
Figure 33. Results of Scenario 2	63
Figure 34. Scenario 3. Participation Factor bar plot for Mode1 and Mode2.	64
Figure 35. Results of Scenario 2	65
Figure 36. Scenario 4. Participation Factor bar plot for Mode1 and Mode2.	66
Figure 37. Results of Scenario 4	66
Figure 38. Scenario 5. Participation Factor bar plot for Mode1 and Mode2.	67
Figure 39. Results of Scenario 5	68
Figure 40. Results after short circuit	70
Figure 41. Results after POD controller, adjusted by PSO	71
Figure 42. Results after POD controller, adjusted by NBA	71
Figure 43. Framework and Architecture of PI-DGP Model	74
Figure 44. Simulation results for attack on substation 2	81
Figure 45. Summary of simulated single substation attacks	82
Figure 46. Simulation results for attack on substations 8&9	83
Figure 47. Summary of simulated two substation attacks.....	83
Figure 48. Black-start Stepwise approach.....	87
Figure 49. Modelling microgrid, CIGRE benchmark system.	90
Figure 50. Use case 1, black-start steps.	91
Figure 51. Use case 1, power distribution.	91
Figure 52. Use case 2, black-start steps.	93
Figure 53. Use case 2, power distribution.	93
Figure 54. Use case 3, black-start steps.	95
Figure 55. Use case 3, power distribution.	95
Figure 56. Cyber-physical power system.	102
Figure 57. Restoration path dependencies embedded in the power graph.....	103
Figure 58. Distance constraint for selecting physical restoration actions.	105
Figure 59. Schematic diagram of GCN layers.	106
Figure 60. Schematic diagram of GCN-Q-Network.	107
Figure 61. Proposed GCN-DQN-based reinforcement learning framework for CPPS restoration.....	108
Figure 62. Cyber layer of the IEEE 39-bus physical system	109



Figure 63. CPPS restoration strategy: Steps 1-4.....	111
Figure 64. CPPS restoration strategy: Steps 5-8.....	112
Figure 65. Final result of the CPPS restoration strategy.....	113

List of tables

Table 1. Characteristics of the test system.....	21
Table 2. Statistics of Synthetic Communication Network.....	34
Table 3. Statistics of Generated Communication Networks.....	34
Table 4. Assigned Impact Weights for each load loss bin	49
Table 5. Cyber attack impact: recorded events and affected elements.	51
Table 6. Terminal connection of synchronous generator and wind turbine.	57
Table 7. Modes description per scenario.....	60
Table 8. Scenario 1. Results for POD-P, POD-Q, and PSS.	62
Table 9. Scenario 2. Results for POD-P, POD-Q, and PSS.	63
Table 10. Scenario 3. Results for POD-P, POD-Q, and PSS.	64
Table 11. Scenario 4. Results for POD-P, POD-Q, and PSS.	65
Table 12. Scenario 5. Results for POD-P, POD-Q, and PSS.	67
Table 13. PST16 Bus System Results.	70
Table 14. Summary of target locations and islanding cutsets.....	80
Table 15. Loads to be restored in all cases.....	89
Table 16. Use case 1, results from PowerFactory.....	92
Table 17. Use case 2, results from PowerFactory.....	94
Table 18. Use case 3, results from PowerFactory.....	96
Table 19. Load flow results after the end of the CPPS restoration strategy.....	113



Abbreviations and Acronyms

Acronym	Description
CAII	Cyber Attack Impact Index
CB	Circuit breaker
CNN	Convolutional Neural Networks
CPPS	Cyber-Physical Power Systems
CPS	Cyber-physical system
CRoF	Control Room of the Future
DER	Distributed Energy Resources
DLS	Democratic Load Scaling
DQN	Deep Q-Network
DRL	Deep Reinforcement Learning
DSS	Decision Support Systems
DSO	Distribution System Operator
DSPF	DIgSILENT PowerFactory
EV	Electric Vehicles
GAE	Graph Autoencoders
GCN	Graph Convolutional Network
HILP	High-Impact, Low-Probability
HVDC	High-Voltage Direct Current
ICT	Information and Communication Technologies
IDS	Intrusion Detection Systems
LCN	Logical Communication Network
LFO	Low-Frequency Oscillations
LV	Low Voltage
MDP	Markov Decision Process
ML	Machine Learning
MMC	Modular Multilevel Converter
MV	Medium Voltage



Acronym	Description
NBA	Novel Bat Algorithm
OPC UA	Open Platform Communications Unified Architecture
OT	Operational Technology
OV	Over Voltage
PCI	Preventive Controlled Islanding
PCN	Physical Communication Network
PI-DGP	Physics-Informed Deep Graph Partitioning
PLC	Programmable Logic Controller
POD	Power Oscillation Damping
POD-P	POD acting on active power
POD-Q	POD acting on reactive power
PPS	Physical Power System
PSR	Power System Restoration
PSS	Power System Stabilizers
PV	Photovoltaic
RES	Renewable Energy Sources
RL	Reinforcement Learning
RMS	Root Mean Square
ROCOF	Rate of Change of Frequency
SCADA	Supervisory Control and Data Acquisition
SMC	Smart Microgrid Controller
SoC	State of Charge
STATCOM	Static Synchronous Compensator
TSO	Transmission System Operator
UF/OF	Under Frequency/Over Frequency
VT/CT	Voltage Transformers/Current Transformers
WAMS	Wide-Area Monitoring Systems
WAN	Wide Area Network



Acronym	Description
WDM	Wavelength-Division Multiplexing
WP	Wind Power



Executive summary

As power systems undergo rapid digitalization, their increasing dependence on Information and Communication Technologies (ICT) has given rise to complex Cyber-Physical Power Systems (CPPS). While this digital transformation enables enhanced power system monitoring, control, and operational flexibility, it also exposes the power grid to a growing range of cyber threats. Cyber attacks targeting digital substations or power grid control systems can impact power system stability, trigger cascading failures and lead to large-scale blackouts. Addressing these risks calls for new methods for modelling cyber-physical system interdependencies, analysing the impact of cyber attacks on power system operation causing cascading failures, and developing proactive, self-healing and restorative strategies to enhance the power grid operational resilience.

This report proposes novel analytic methods and intelligent systems to assess the impact of cascading failures in interconnected power grids and enable self-healing and restorative power grid capabilities at the physical system layer. It presents a comprehensive exploration of cyber-physical system resilience in modern power grids, focusing on the development and application of advanced modelling, cascading failure analysis and mitigation tools, and restoration strategies for CPPS. It builds on the findings of deliverable D2.2 and consolidates the research activities carried out in tasks T4.1, T4.2, T4.3, and T4.4. The innovations developed through these tasks form the foundation for future demonstrations in The Netherlands in T5.3, where the digital twin testbed of interconnected power grids and the Control Room of the Future (CRoF) infrastructure at TU Delft will be employed to simulate the real-time power system operation, mitigate cascading failures and coordinate the cyber-physical system restoration.

Recognizing the critical importance of operational resilience for the interconnected power grids, this report presents a holistic framework that spans the full resilience lifecycle—from proactive mitigation to power system recovery. The scope of the report includes:

- Advanced modelling techniques for CPPS and development of high-fidelity power grid digital twins and models for the operation of both transmission and distribution power systems.
- Quantitative analysis of cyber attack-induced cascading failures and novel resilience metrics to assess the power grid operational resilience.
- Self-healing methods and tools and adaptive strategies to enhance power grid security and operational resilience against cascading effects, such as dynamic stability enhancement mechanisms and a cyber-aware Preventive Controlled Islanding (PCI) strategy.
- Design and implementation of restoration frameworks, including reinforcement learning-based cyber-physical system restoration, i.e., coordinated operational technology recovery and power system restoration, and secure black-start recovery strategies.



Together, these novel contributions support intelligent decision-making, situational awareness, and coordinated control actions to strengthen the CPPS operational resilience. The findings, methods and tools presented in this report not only contribute to the academic understanding of power system cyber resilience but also serve as a foundation for practical deployment and demonstration in real-time power system simulation environments.

