



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

D4.4 Results of CRoF training exercises



Document details

Deliverable no	D4.4
Deliverable name	Results of CRoF training exercises
Version	1.0
Release date	30/08/2026
Type	R
Dissemination level	PU
Status	Final
Author	TUD – Bahman Ahmadi, Mohmed Radwan, Alexandru Ștefanov, Ioannis Semertzis, Abhishek Saini, Peter Palensky ENCS – Anne Maria Anggraeni, Elisabetta Provvedini, Elvira Sanchez Ortiz, Biprotosh Bhattacharjee, Akram Hamdi, Salvatore Maccarrone, Maarten Hoeve SIN – Bonnie Murphy TENNET – Matija Naglic



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	23/06/2026	First draft version	TUD, ENCS, SIN
0.2	29/06/2026	Peer reviewed	TUD, ENCS, SIN, TENNET
0.3	15/07/2026	Draft revised	TUD
0.4	29/07/2026	Draft revised	TUD, ENCS
0.5	01/08/2026	Peer reviewed	ENCS
0.6	15/08/2026	Draft revised	TUD
0.7	23/08/2026	Peer reviewed	CIRCE
0.8	25/08/2026	Draft revised	TUD
1.0	30/08/2026	Final version	TUD, CIRCE



Table of Contents

Executive Summary.....	9
1 Introduction	10
1.1 Scope of the Deliverable	10
1.2 Relation with Other Work Packages	10
1.3 Methodology	11
1.4 Outline of Deliverable	11
2 Training Platform and Infrastructure	12
2.1 Introduction	12
2.2 Cyber Range Architecture	12
2.3 CRoF Integration	14
2.3.1 CRoF Infrastructure	14
2.3.2 CRoF Integration for Training	17
2.4 CRoF Training Platform	17
3 Training Scenario	18
4 Training Design	22
4.1 Rationale	22
4.2 Objectives	22
4.3 Activities	23
4.3.1 Red Team Activities	23
4.3.2 Blue Team Activities	24
4.3.3 Tools	26
4.4 Evaluation	27
4.4.1 Technical Debrief	28
4.4.2 Facilitated Group Reflection: the Me–We–Us Method	29
4.4.3 Participant Surveys	29
5 Training Execution	30
5.1 Setup and Delivery	30
5.1.1 Environment	31
5.1.2 Materials	32



5.2	Training Flow	32
	5.2.1 Day 1: Red Team Training	33
	5.2.2 Day 2: Blue Team Training	33
5.3	Evaluation Results	34
	5.3.1 Participant Overview	34
	5.3.2 Quantitative Results	35
	5.3.3 Qualitative Results	37
5.4	Lessons Learned	38
6	Conclusion.....	40
	References	41
	Annex 1: Training Feedback Survey	42
	Annex 2: Training Impact Survey	44



List of figures

Figure 1. Diagram of the Cyber Range architecture based on the Purdue levels	13
Figure 2. Power grid digital twin implementation in CRoF	14
Figure 3. Infrastructure and Architecture of CRoF servers	15
Figure 4. Architecture of the cyber layer in CRoF	16
Figure 5. Visualization of scenario attack path	18
Figure 6. Representative CRoF operator views used in the training scenario: a) impact assessment dashboard, b) preventive islanding interface, c) OT recovery and power grid restoration interface	21
Figure 7. Overview of the evaluation methodology	28
Figure 8. Red Team training day	31
Figure 9. Blue team exercise during the second day of the training	31
Figure 10. Mean scores for overall training experience (1 = Strongly disagree, 5 = Strongly agree)	35
Figure 11. Mean scores for learning outcomes (1 = Strongly disagree, 5 = Strongly agree)	36
Figure 12. Mean scores for delivery quality (1 = Strongly disagree, 5 = Strongly agree; n=6 per team)	37
Figure 13. Distribution of responses to "How likely are you to recommend this training to a colleague?"	37



Abbreviations and Acronyms

Acronym	Description
AI/ML	Artificial Intelligence / Machine Learning
APT	Advanced Persistent Threat
CINEA	European Climate, Infrastructure and Environment Executive Agency
CRoF	Control Room of the Future
CSIRTs	Computer Security Incident Response Teams
DMZ	Demilitarized Zone
ENCS	European Network for Cyber Security
EPES	Electric Power and Energy Systems
GUI	Graphical User Interface
HMI	Human-Machine Interface
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IEC	International Electrotechnical Commission
IT	Information Technology
LAN	Local Area Network
OPC UA	Open Platform Communications Unified Architecture
OT	Operational Technology
PCAP	Packet Capture
PLC	Programmable Logic Controller
ROCOF	Rate of Change of Frequency
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOC	Security Operations Centre
TSO	Transmission System Operator
TUD	TU Delft (Delft University of Technology)
WP	Work Package



Executive Summary

This deliverable reports on the design, execution, and evaluation of the eFORT training activities conducted in Task 4.7 to build human capital for Computer Security Incident Response Team (CSIRT) and power grid operators. The training was developed as a two-day Red Team/Blue Team exercise hosted at TU Delft and it combined the ENCS cyber range with the TUD Control Room of the Future (CRoF) environment. In this way, participants were exposed not only to attack and detection workflows in a segmented IT/OT setting, but also to cyber-physical system consequences of incidents through digital twin-supported operator functions.

The training complements the broader Dutch TSO demonstrator documented in Deliverable 5.1 by focusing on the human and operational use of the developed eFORT solutions. In particular, it brings together outputs from Task 3.7 on cyber detection and response, Task 4.1 on power grid digital twin, Task 4.2 on coordinated cyber-physical system restoration, and Task 4.3 on preventive controlled islanding and mitigation of cascading failures. The deliverable, therefore, documents how these results were translated into a practical learning environment for power grid operators and cyber security professionals.

The reported results show that the training was executed successfully and provided a realistic and relevant learning experience, especially in connecting cyber attacks to operational decision making for power grids. The evaluation indicates a positive perceived learning value and high relevance to participants' work, while also highlighting areas for improvement, such as clearer prerequisites, more guidance and hands-on facilitation, improved tool stability, and better tracking of participants' learning outcomes. These observations provide a basis for refining future training iterations and for further strengthening the use of eFORT solutions in operator training for cyber-physical power systems.



1 Introduction

1.1 Scope of the Deliverable

The scope of this deliverable is to document the Task 4.7 training activities that were prepared and executed to complement the eFORT demonstration work. It covers the training platform and infrastructure, the scenario and training design, the execution of the Red Team and Blue Team sessions, and the evaluation results and lessons learned from the conducted exercise. The deliverable focuses on how the selected eFORT tools and demonstrator components were used in a training context. Detailed technical descriptions of the underlying methods and demonstrator implementations are referenced to the related technical and demonstration deliverables.

1.2 Relation with Other Work Packages

This deliverable is positioned at the interface between the training activities in Task 4.7 and the technical developments delivered in other eFORT Tasks. The training exercise uses outputs from several Tasks as operational content, training infrastructure, and demonstration material, so that participants can interact with project results in realistic scenarios rather than only through stand-alone descriptions.

Task 3.7 provides the cyber detection, situational awareness, and orchestration layer used in the training. Its outputs underpin the cyber range exercise materials on monitoring, incident detection, alert handling, and automated or semi-automated response, using tools such as Wazuh, Suricata, OpenVAS, and SOARCA.

Task 4.1 provides the digital twin foundation used in the TUD environment. The CRoF-based power system models, together with the supporting communication interfaces and snapshots of system state, allow the training to connect cyber incidents to physical grid impact assessment and operator awareness.

Task 4.2 contributes to the coordinated restoration concept demonstrated in the training. Its results demonstrate that power system recovery must jointly consider OT communication recovery and power system restoration, and that operator decisions can be supported through cyber-physical restoration views and staged execution paths.

Task 4.3 contributes with the preventive islanding and cascading effects mitigation functions used in the TUD demonstration part of the training. These results allow participants to see how cyber alerts can be translated into preventive operational actions aimed at reducing the severity of disturbances and avoiding large scale blackout conditions.

In addition, the training is closely related to the demonstration-oriented work in WP5. The defined use cases, scenario logic, and site integration work provide the practical context in which the training is executed. While Deliverable 5.1 documents the Dutch demonstrator from the technical demonstration perspective, Deliverable 4.4 complements that work by focusing on training design, participant interaction, evaluation, and lessons learned.



1.3 Methodology

The methodology followed in this deliverable is based on a joint design-and-execution approach across the involved partners. TUD coordinated the overall Task 4.7 activity and the integration of the CRoF environment, ENCS led the cyber range-based training scenario and hands-on exercise design, and SIN defined the evaluation approach and feedback collection logic. This collaboration ensured that the learning objectives, technical setup, and evaluation criteria remained aligned throughout preparation and delivery.

The training content was structured as a two-day sequence with complementary perspectives. Day 1 focused on the Red Team view of attacker logic, reconnaissance, exploitation, and post exploitation steps in a segmented grid operator environment. Day 2 focused on the Blue Team view of monitoring, evidence-based incident detection, mitigating measures, and coordinated response across the cyber range and the TUD cyber-physical environment.

Methodologically, the exercise combined theory, guided hands-on practice, and scenario execution. Prior to delivery, the partners prepared handouts, credentials, and exercise infrastructure, and performed dry runs to verify that the cyber range, CRoF services, operator interfaces, and supporting assets behaved consistently. This preparation was necessary because the training depends on synchronized interaction between cyber monitoring, scenario progression, and cyber-physical decision support functions.

The evaluation methodology combined direct observation during the exercise with structured technical debriefing, facilitated reflection, immediate participant surveys, and a delayed impact survey. This layered approach was selected to capture not only immediate satisfaction and perceived learning, but also how participants reflected on their performance and whether the training influenced later practice.

1.4 Outline of Deliverable

Following the executive summary and introduction, Section 2 describes the training platform and infrastructure, including the cyber range, the CRoF integration, and the eFORT training platform. Section 3 presents the training scenario, while Section 4 explains the training design in terms of rationale, objectives, activities, tools, and evaluation approach. Section 5 reports the training execution, the environment and materials used, the step-by-step training flow, the evaluation results, and the lessons learned. Section 6 concludes the deliverable, after which the annex material is provided.



2 Training Platform and Infrastructure

2.1 Introduction

This section introduces the technical environment used for the CRoF training exercises and explains how the main eFORT components are combined to create a realistic cyber-physical training setting. Its purpose is not only to describe the cyber range and the CRoF separately, but also to show how they are connected so that participants can move from cyber events and monitoring activities to their operational implications for grid operation.

Accordingly, the section first presents the cyber range architecture used to emulate the segmented IT/OT environment of a grid operator and then discusses the integration with the CRoF digital twin infrastructure at TU Delft. Through this connection, alerts, attack steps, and response actions can be linked to the power system model and the operator facing services, allowing the training to evaluate both cyber security performance and cyber-physical consequences within a single coherent environment.

2.2 Cyber Range Architecture

The cyber range (Figure 1) simulates a segmented grid operator architecture comprising the enterprise IT, OT control centre, and substation levels that are separated through layered principles commonly used in the energy sector. The purpose of the cyber range design is to show a realistic environment to execute threat scenarios and detection engineering on the energy infrastructure. Segmentation in the simulated architecture follows the Purdue reference model (Williams, 1994) and IEC 62443 controls (ISA / IEC, 2019) for separation of zones, where each layer represents a different Purdue level.



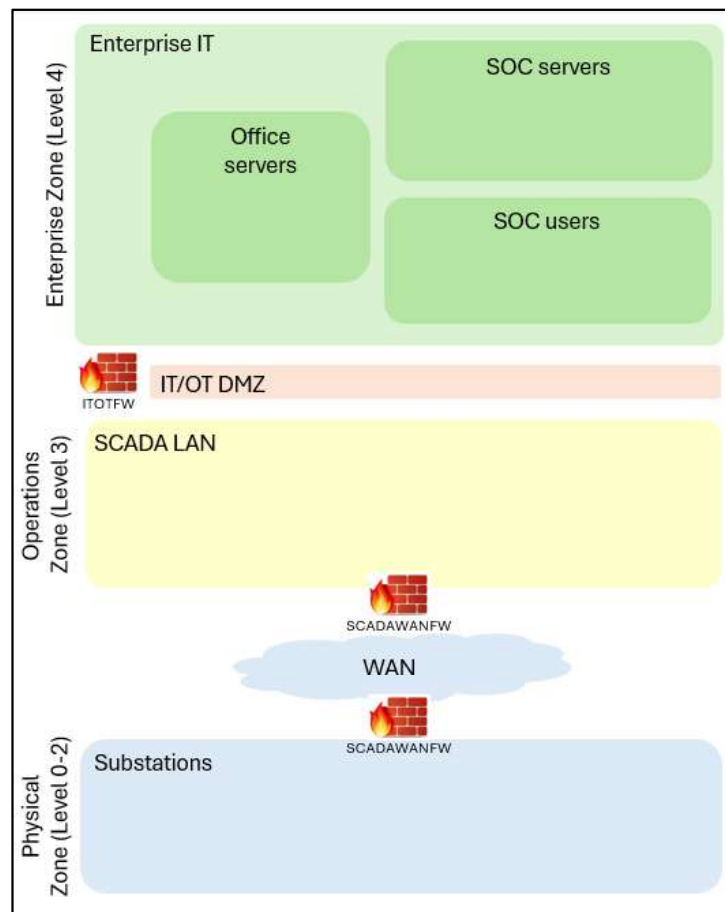


Figure 1. Diagram of the Cyber Range architecture based on the Purdue levels

The topmost architectural layer, Level 4, contains the corporate IT network, including its workstations. For the purpose of this training, the security operations centre (SOC) has a dedicated network segment located in this layer for its servers and workstations. Within the SOC servers, the Wazuh SIEM is used to collect and visualize incoming information from network sensors and hosts logs. Other tools include OpenVAS for vulnerability detection, flow monitoring sensors, and the signature-based sensors for the OT/IT and SCADA LAN network. Both sensors have a Suricata instance installed.

The second layer represents the demilitarized zone (DMZ). This layer, often referred to as Level 3.5, sits between the enterprise IT and operations zones and acts as a buffer between them. It is a dedicated network that separates the IT and OT zones. Communication between these zones is mediated through a database server in the DMZ.

The third layer is the operations or OT zone, where the SCADA system is hosted (Level 3). Grid operators make use of the workstations and HMIs in this zone to read device measurements and send commands to the substations.

The lower level represents the substations (Levels 0-2). This is where the RTU and circuit breaker are located.

2.3 CRoF Integration

2.3.1 CRoF Infrastructure

The Control Room of the Future (CRoF) at TU Delft provides a cyber-physical digital twin environment that connects the training activities to the wider eFORT demonstrator platform. It combines monitoring, analysis, and control capabilities in a setting that replicates relevant control room functions and enables cyber incidents to be studied alongside their operational implications for the grid.

Figure 2 illustrates the CRoF infrastructure, which creates a cyber-physical digital twin environment for monitoring, analyzing, and controlling the power grid. This setup closely mimics real control room operations. In addition to the fundamental monitoring and control features, the platform incorporates advanced resilience and cyber security tools developed through the eFORT project.

At the infrastructure level, the CRoF brings together the physical power system simulation, the OT communication network emulation, and the interfaces required to exchange data between them. The physical grid behavior is simulated in DlgSILENT PowerFactory, while the cyber layer is emulated on distributed CRoF Linux servers using Mininet-based substation and control center models. The OPC UA interface synchronizes measurements, alarms, status values, and control variables across the cyber and physical layers, enabling the digital twin to operate as a single coherent co-simulation environment. The complete setup description for CRoF is provided in the deliverable for Task 5.3 of the eFORT project.

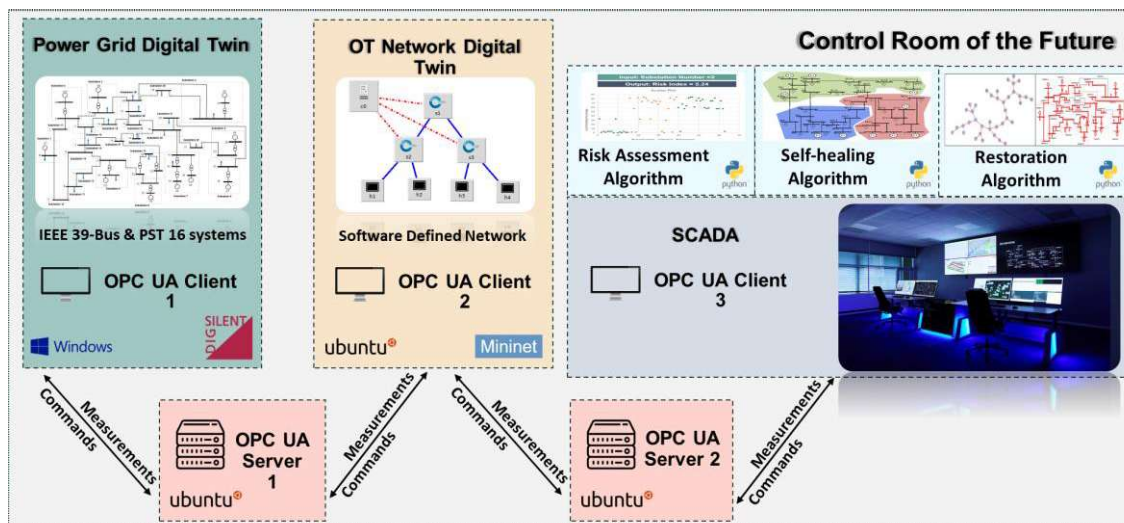


Figure 2. Power grid digital twin implementation in CRoF

Additional information regarding the CRoF infrastructure is shown in Figure 3, where the OT cyber layer is implemented as a distributed set of coordinated network models rather than as one monolithic emulation. A supervisory orchestration layer maintains the lifecycle, health status, and assignment of the active cyber models and aligns their availability with the services used by the digital twin and the control room environment.

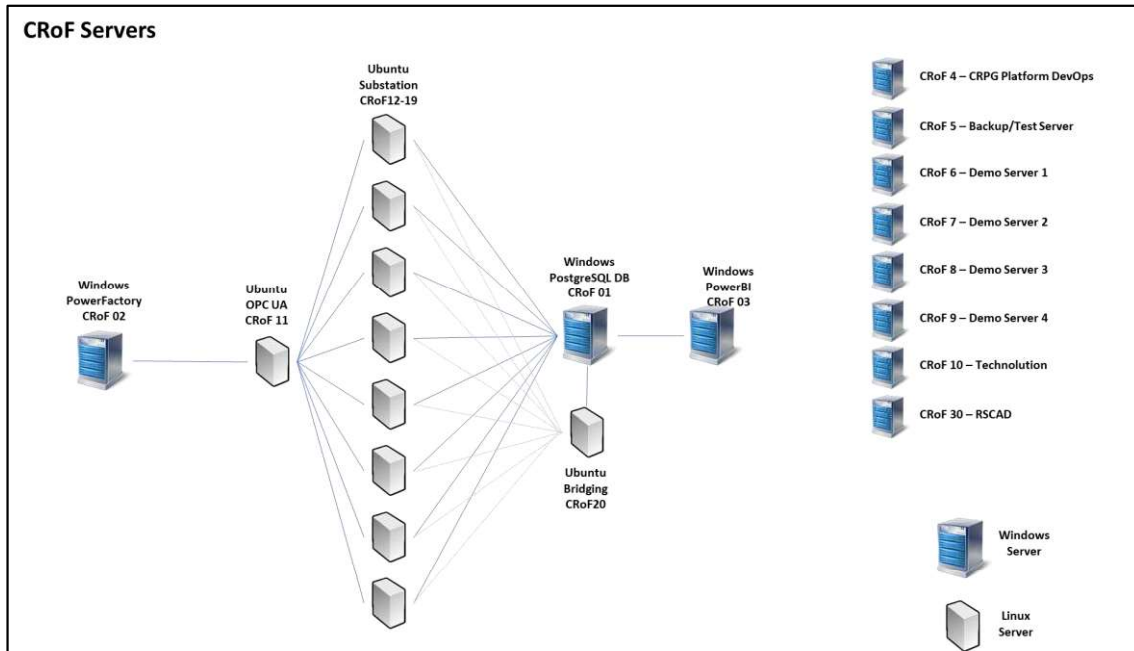


Figure 3. Infrastructure and Architecture of CRoF servers

Each CRoF Linux machine can run multiple Mininet instances simultaneously, where each instance simulates the communication environment of a different substation or OT segment. Within a substation model, the emulated topology may include switching components, gateway hosts, and device hosts representing measurement, supervision, and control functions. Spreading these Mininet instances across multiple Linux systems enables scalability while maintaining substation isolation, which is crucial for analyzing localized failures and staged recovery processes.

The interplay among various Mininet-based cyber models is crucial for achieving realism. These models are not considered isolated toy networks; instead, they exchange traffic via realistic, mediated paths such as control room applications, shared data services, gateways, and interzone links. This setup allows for an accurate representation of scenarios in which, for example, one substation remains accessible while another is isolated, or in which a shared cyber service acts as a bottleneck affecting multiple substations simultaneously.

From the control room perspective, the data flow reflects the real OT operational chain. Measurements, alarms, and status updates from substation side hosts are sent upward via substation gateways and shared services to control room applications. Meanwhile, commands from operators or automated systems travel back through the cyber layer to

the specific substation assets, which then update the power system in the co-simulation.

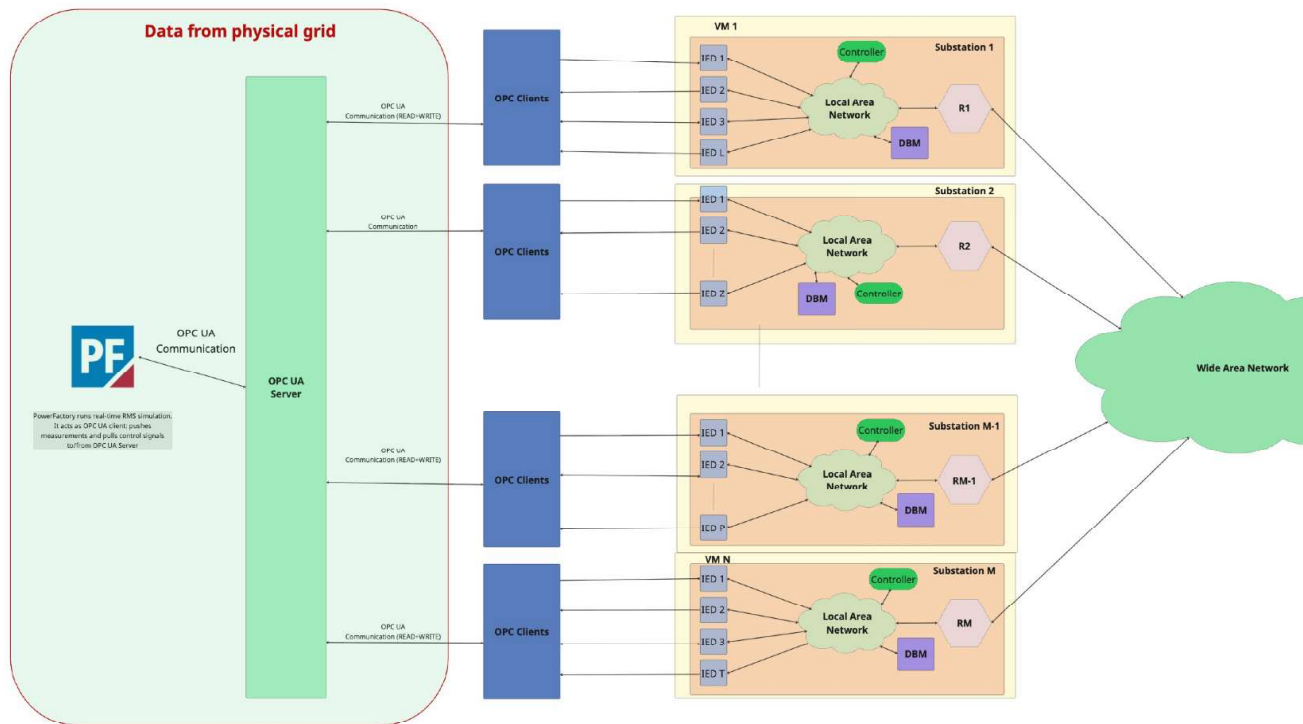


Figure 4 illustrates the cyber layer's architecture, built on the CRoF infrastructure shown in Figure 3.

Additional CRoF machines host supporting services such as databases, visualization, orchestration, and testing functions. This distributed setup allows multiple substation communication models to run in parallel, preserves substation-level isolation, and supports broader studies related to resilience, cascading effects, restoration, and training under realistic operational conditions.

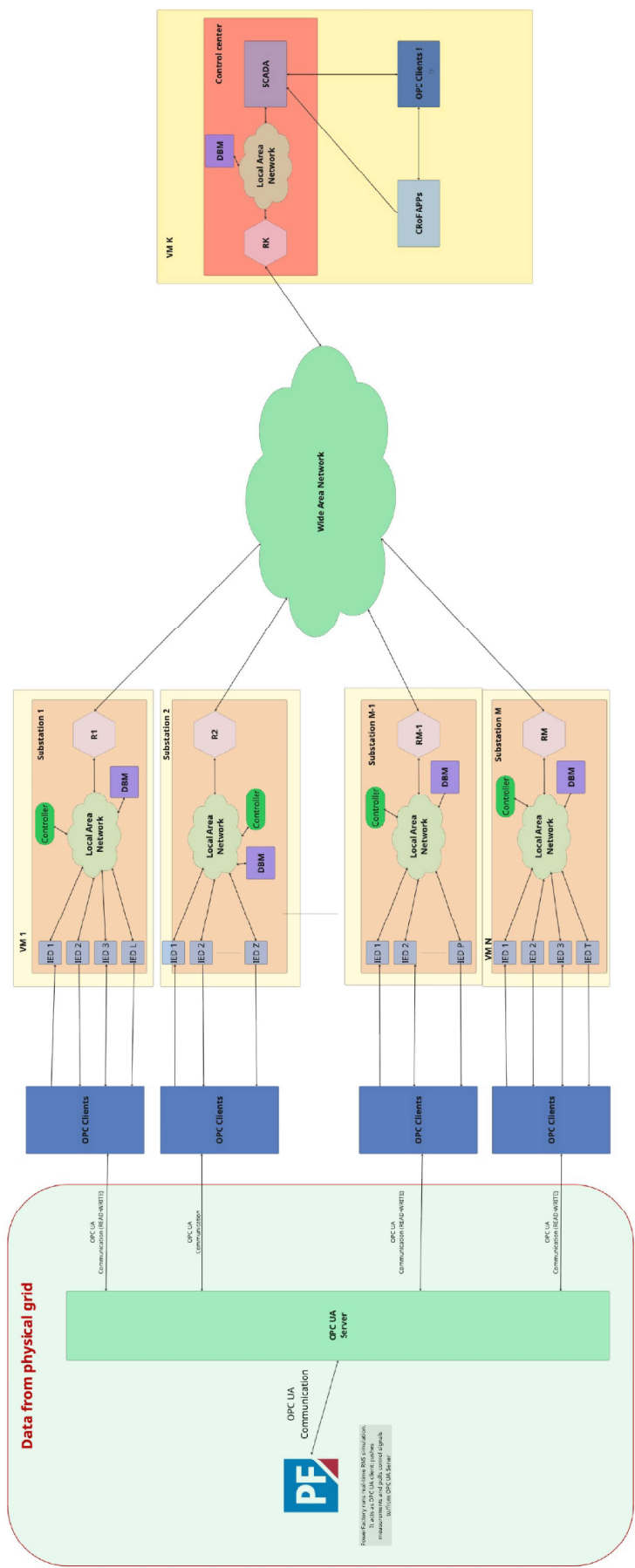


Figure 4. Architecture of the cyber layer in CRoF.



2.3.2 CRoF Integration for Training

For training exercises, the CRoF serves as the operational counterpart to the cyber range. It receives the cyber side context from the segmented training environment and links it to the digital twin, enabling participants to relate observed attack steps to their potential consequences for grid monitoring, control, and coordinated response.

This allows the exercise to be followed from both the security and the operational perspectives. Participants can observe how degraded communication paths, compromise of field assets, or disruption of control center services influence visibility and controllability in the simulated grid, while the CRoF services provide a controlled environment for discussing response priorities, cross-domain coordination, and the practical meaning of cyber-physical dependencies.

In this way, the CRoF does not function as a stand-alone demonstrator alongside the cyber range, but it extends the training by adding a cyber-physical layer in which alerts, attack progression, and operator actions can be interpreted in relation to the grid. This strengthens the training objective of building human capital by exposing participants to the interplay between cyber security events and power system operations within a single coherent workflow.

2.4 CRoF Training Platform

The training platform combines the cyber range environment and the CRoF-based digital twin into a single cyber-physical training environment. From the participant's perspective, the platform resembles the architecture of a representative electricity grid operator, with a public facing zone, an enterprise IT zone, a demilitarized zone, an operations or control center zone, and lower level substation segments. Across these layers, the environment hosts business workstations, SOC services, SCADA applications, operator HMIs, and field facing OT assets under realistic segmentation and access constraints.

This layered structure is important because it allows trainees to follow an incident across the same boundaries that exist in real grid operator environments. Attack paths, monitoring data, containment actions, and operator decisions are therefore not presented in an abstract laboratory setup. Instead, they unfold across segmented IT and OT zones with constrained communications, mediated data exchange, and distinct responsibilities for cyber analysts and grid operators.

The cyber range complements the CRoF as it simulates substation SCADA functions and servers. It provides a controlled, cyber side environment in which adversary activity, detection engineering, SOC playbooks, and response workflows can be executed, while the CRoF provides the operational digital twin in which the consequences of those cyber events can be interpreted for grid monitoring and control. Together, they connect alerts and attack progression to operational effects, enabling trainees to understand both how an incident develops technically and why it matters for power system operation, restoration, and coordinated decision making.



3 Training Scenario

The scenario simulates a multistage attack on the SCADA system of a hypothetical TSO. The overall goal of the threat actor is to switch the circuit breakers by accessing and tampering with an OPC server. A visualization of the attack path is shown in Figure 5.

The scenario begins with a phishing attack successfully gaining initial access to an IT workstation. From the compromised workstation, the threat actor discovers and scans the IT/OT DMZ to identify vulnerable systems and gain lateral access to the OT network. The vulnerabilities in the machines are then exploited to locate the SCADA LAN network and the OPC server that sits within it. A network scan is then executed using the OPC server to discover the HMI and RTUs.

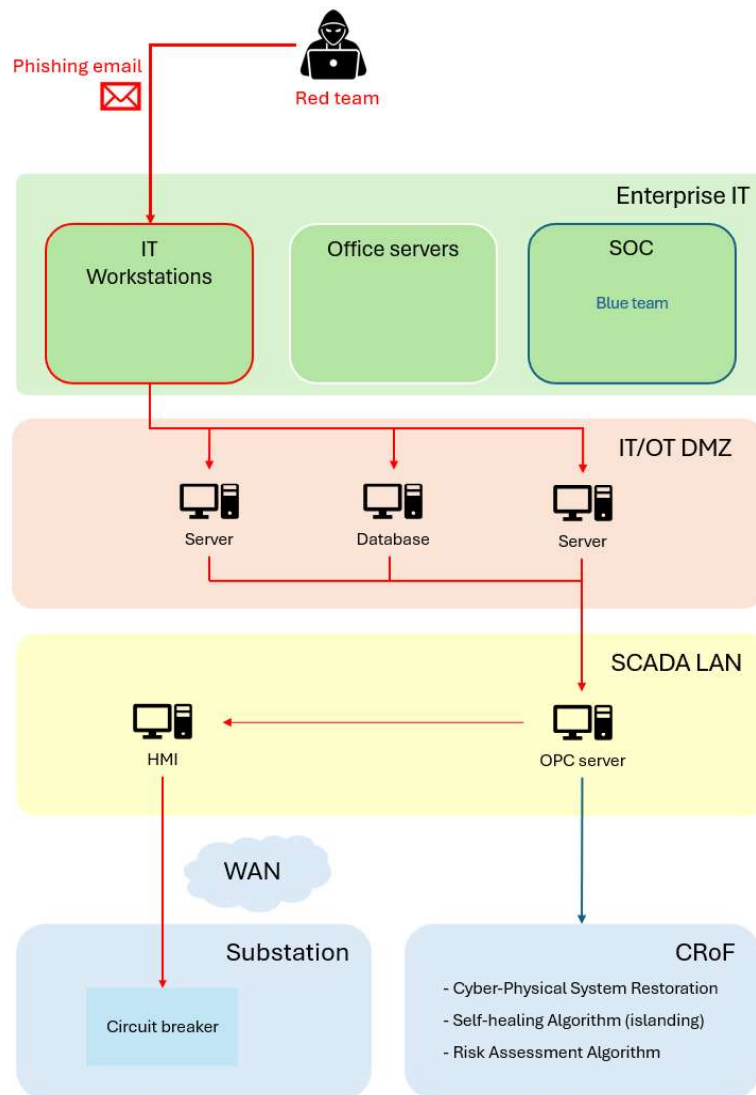


Figure 5. Visualization of scenario attack path

The final step of the attack path is to use port forwarding on the HMI. In a real scenario, a circuit breaker would be switched off, but in the case of this training, an intelligent electronic device is targeted as it is present on the same network and can be compromised using the same methodology.

As the threat actor commences their attack path, the security operations team must defend the network from the threat actor, utilizing the detection techniques below:

- Network monitoring, using sensors to analyze the network for malicious traffic,
- IT techniques, scanning and analyzing vulnerabilities using OpenVAS, and monitoring the network using signature-based sensors,
- Host monitoring, identifying malicious activities using syslogs gathered from monitored hosts.

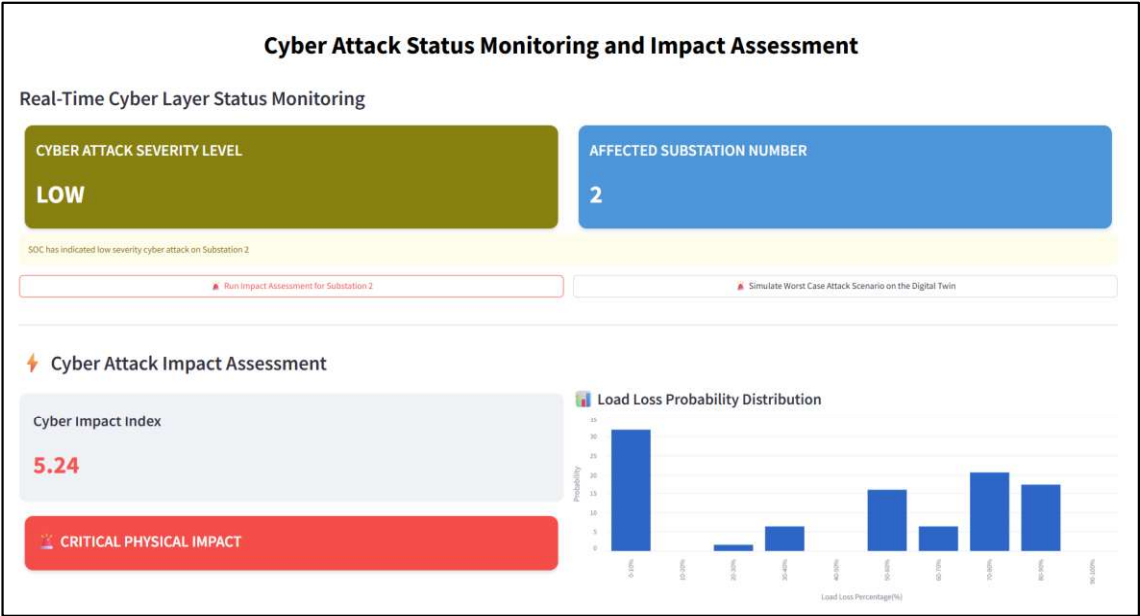
The TUD CRoF integration is used in the training scenario to extend the cyber range exercise with operator focused cyber-physical decision making. In practical terms, this means that the Blue Team activities do not stop at detection and incident handling inside the IT and OT cyber environment; they continue into the CRoF digital twin environment, where participants train on impact assessment of cascading effects, preventative islanding to mitigate cascading effects, and OT recovery and power grid restoration after a major disturbance.

For the cascading effects scenarios, operators first work with the CRoF cyber status and impact assessment dashboard. This interface receives incident notifications from the SOARCA side and presents the current cyber threat state, the affected substation, and an impact index, together with a probability distribution of possible physical consequences. From the same interface, trainees can launch worst case digital twin simulations and discuss how a reported cyber incident could propagate into line outages, instability, or a broader blackout. In this way, the TUD impact assessment capability is used to train operators to interpret cyber alarms in terms of power system risk rather than as isolated SOC events only.

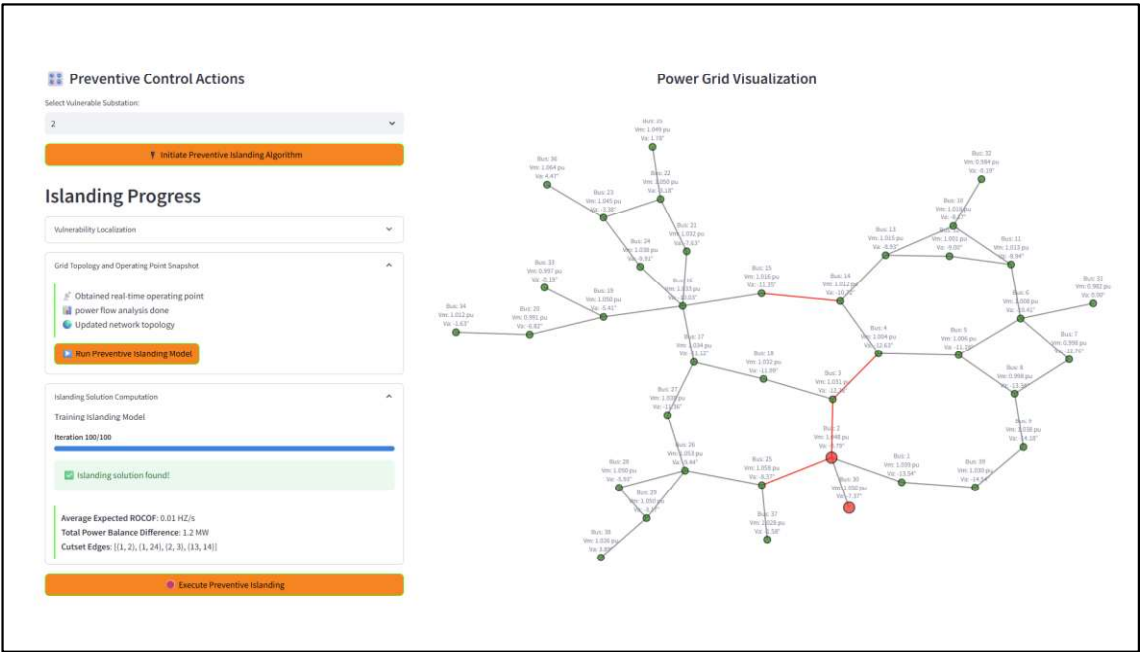
When the assessed risk justifies preventive action, operators continue with the preventive islanding interface. This view combines topology and power flow information from the CRoF digital twin with the machine learning-based islanding tool, presenting candidate cut sets for islanding configuration, expected ROCOF, and estimated power imbalance for the proposed islands. The training objective here is to enable participants to evaluate the trade-off between accepting limited short term operational degradation and preventing a much larger cascading event, and then to execute the selected islanding action through the integrated FastAPI Mininet-OPC UA control path.

For OT recovery and power grid restoration training, the CRoF environment provides a restoration interface in which the physical grid view and the communication network view are presented together, alongside mapped command identifiers and operator action choices such as manual recovery or OPC-based recovery. Supporting restoration views exposes the cyber layer recovery state and the AI assisted restoration logic, enabling operators to understand why a step is proposed. The reasoning of the AI model can be discussed for the training, whether the relevant asset is already cyber reachable, and how the next recovery action should be validated before execution. This allows the CRoF scenarios to train operators in coordinated restoration workflows that integrate observability, controllability, and communication path recovery into a single coherent exercise. Representative operator views used in these activities are shown in Figure 6.



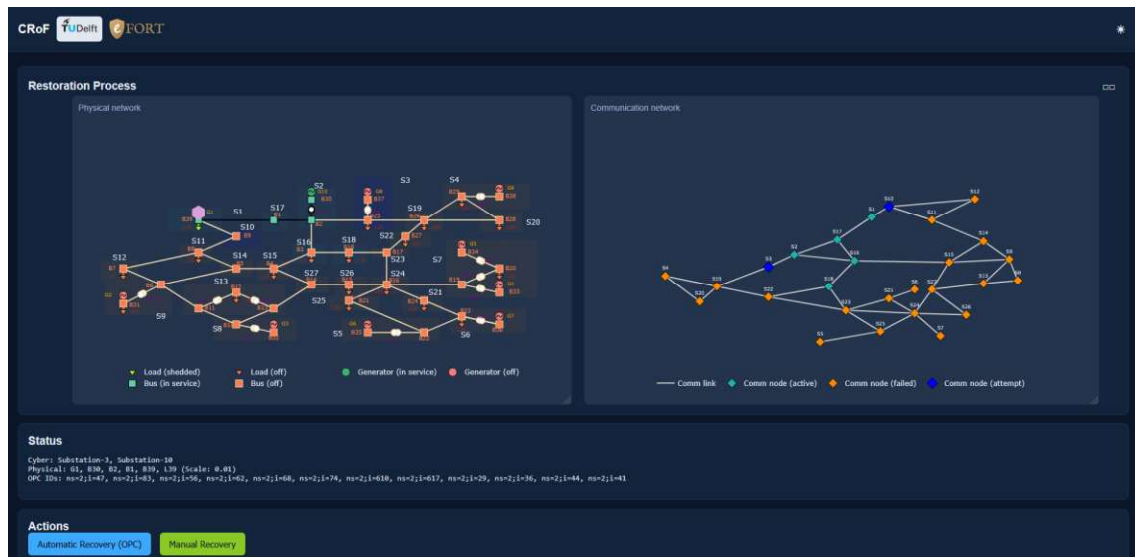


a)



b)





c)

Figure 6. Representative CRoF operator views used in the training scenario: a) impact assessment dashboard, b) preventive islanding interface, c) OT recovery and power grid restoration interface



4 Training Design

The training design is based on the model presented in “Telling ain’t training” (Stolovitch & Keeps, 2011). The model emphasises active participation and practical skill development through four key elements:

- **Rationale:** Describes why the training is relevant and provides an understanding on the practical value of the session to the participants’ work.
- **Objectives:** A clear statement of learning points and expectations upon completion of the training. The objectives should be measurable and observable.
- **Activities:** Learning activities that enable participants to achieve the defined objectives. The main focus is on active participation and practical application of the targeted skills.
- **Evaluation:** Performance of participants is measured and assessed on whether the objectives have been achieved.

4.1 Rationale

Following the described model, training begins by explaining its importance and relevance to participants’ daily responsibilities. The training tackles realistic challenges that participants may face in their roles, such as identifying risks and vulnerabilities, logging and incident detection in network traffic, selecting appropriate mitigations, and coordinating response measures.

The exercise falls within the scope of the eFORT project to make European power grids more resilient and reliable against cyber attacks by developing technologies to identify, prevent, and mitigate risks and vulnerabilities.

Hence, the training is a hands-on exercise that simulates real attack scenarios, where participants learn and apply offensive and defensive cyber security knowledge in a controlled environment. By participating in this structured exercise, knowledge on vulnerabilities, coordination, and communication is reinforced through practical application, enhancing readiness in the event of a real world incident.

4.2 Objectives

The training exercise is developed under Task 4.7, both to test the innovations developed under the eFORT project and train grid operators in tackling cyber security challenges. As the training tackles both the offensive and defensive perspectives of cyber security, the training is divided into two sessions, with each having a different set of objectives.

From the offensive perspective, the participants are expected to be able to:

- Understand the building blocks of cyber attacks and how they are used in the real world;
- Identify and assess the risks of cyber attacks on OT systems;



- Demonstrate understanding of threat actor behavior by simulating a cyber attack in operational, realistic conditions;
- Reflect on the effect of cyber attacks on the grid.

From the defensive perspective, the participants are expected to be able to:

- Understand effective countermeasures against cyber attacks on the grid;
- Assess cyber security events and determine appropriate prevention and response measures ;
- Apply prevention and response measures in operational, realistic conditions;
- Demonstrate clear communication between sub-teams during incident handling;
- Reflect on the effect of cyber attacks on the grid and the effectiveness of countermeasures.

4.3 Activities

The training is designed to simulate a realistic scenario involving the perspectives of the attacker and the security team. Each training day focuses on one of these perspectives, enabling participants to apply offensive cyber security techniques and practise risk-driven responses for cyber-physical defence. The training follows a two-day Red Team, Blue Team format that combines theoretical instruction with hands-on sessions. The learning objectives are tailored to the exercises conducted on each day. The attack path described in the Training Scenario section is used for both days. By participating as both red and Blue Team, the participants can strengthen both awareness of potential attack vectors and defence capabilities.

4.3.1 Red Team Activities

On the first day, participants act as the Red Team (attackers) and perform a series of attacks to understand how vulnerabilities and payloads can be exploited in a real world setting. No defensive mechanisms are introduced yet.

Before delving into offensive knowledge sessions, participants are presented with an overview of the importance of considering cyber attacks against OT. It is also important for the Red Team to understand the different types of vulnerabilities that attackers can exploit in the real world.

The knowledge sessions are supplemented by hands-on training in network scanning and post exploitation tactics. During the Red Team exercise, participants use Nmap through the Command-Line Interface (CLI) to identify hosts and services. They then select appropriate exploit modules in Armitage and execute them against the identified services.

The final exercise ties together what the participants have learned throughout the theory and hands-on sessions by applying them in the scenario attack path. The baseline exercise replicates the full multistage attack path outlined in Section 3 where starting from the compromised enterprise IT workstation, participants conduct reconnaissance and lateral movement through the IT/OT DMZ, access the SCADA LAN and OPC server,



identify the HMI and field devices, and utilize port forwarding to target the training PLC as a secure proxy for circuit-breaker operations.

4.3.2 Blue Team Activities

On the second day, participants act as the Blue Team (security operations team, defenders), while the training team acts as the Red Team (attackers). The Blue Team is responsible for detecting and applying appropriate mitigations in response to the attack sequence.

As with the Red Team activities, participants receive a brief overview of the impact of OT cyber attacks and the role of a Security Operations Center (SOC). From a SOC perspective, participants explore ways to counter cyber attacks through prevention and response measures.

The exercise is divided into two phases. In the preparation phase, the participants analyse the system, identify possible vulnerabilities that the Red Team could exploit, and propose corresponding countermeasures. These countermeasures are not implemented during the exercise but serve as a basis for reflection during the detection phase. During the detection phase, participants use monitoring tools to detect the steps executed by the Red Team. They should also note whether their proposed mitigation measures would have prevented each step in the attack.

For the exercise, participants are divided into three teams based on monitoring techniques:

- **Flow monitoring.** This team monitors alerts coming from different network sensors and analyses packets using Wireshark. In the preparation phase, the team should understand what normal traffic looks like and filter alerts to be able to better detect an attack in the detection phase.
- **IT-Techniques.** This team identifies system vulnerabilities using a vulnerability scanner during the preparation phase and monitors alerts from signature-based IDS sensors during the detection phase.
- **Host monitoring.** This team monitors logs coming from hosts in the network. In the preparation phase, the team should understand what normal activity on the hosts looks like and filter alerts to better detect attacks during the detection phase.

In the Blue Team exercise, the digital twin is used to extend cyber detection into operator oriented cyber-physical training. Rather than limiting the participants to SOC monitoring alone, the TUD integration allows them to examine how the reported cyber incident can affect observability, controllability, cascading failures, and restoration of the power grid. In this way, the Blue Team is trained not only to identify malicious activity in the segmented cyber range but also to interpret why that activity matters for grid operation and what coordinated response actions should follow in the control room environment.

The first TUD capability introduced for this purpose is the impact assessment workflow for cascading effects. As described in Deliverable 5.1, the CRoF receives cyber security notifications and incident information and exposes them through an operator dashboard that provides real time situational awareness of the cyber layer. Through this interface, operators can see the affected substation, the current cyber threat state, an impact index



expressing the likely physical severity of the event, and a probability distribution of possible consequences. The same interface enables the launch of worst case digital twin simulations, allowing trainees to discuss how a cyber attack may propagate into line outages, instability, or a complete blackout. This capability is used to train operators to translate cyber alarms into power system risk assessments rather than treating the incident as an isolated IT or SOC event. Representative operator views for this part of the training are shown earlier in Figure 6a. This impact-assessment activity is based on the work conducted in Task 4.1 concerning the power-grid digital twin and is integrated within the WP5 Dutch TSO demonstration initiatives, as documented in D5.1.

A second training capability is the preventative islanding workflow developed for defending against cascading effects. Here, the digital twin interacts with the machine learning-based islanding tool through the CRoF services. The islanding tool consumes grid models, real time topology information, vulnerable zones, and simulation-based impact metrics from the digital twin to compute adaptive islanding partitions before the disturbance escalates. The resulting solutions are visualized in the operator interface, along with key indicators such as the expected Rate of Change of Frequency (ROCOF) and the estimated power imbalance within the proposed islands. During the training, participants review the suggested cut set, assess the expected operational trade-offs, and discuss whether accepting limited short term degradation is justified to prevent a much wider cascading event. This provides the Blue Team with a concrete cyber-physical decision support exercise in which detection results are linked to preventive control actions. The corresponding GUI is represented in Figure 6b. It thus builds upon the results of Task 4.3 on preventive controlled islanding and cascading failure mitigation, including their implementation in the WP5 Dutch TSO demonstrator documented in D5.1.

The TUD contribution also includes cyber-physical system restoration training inside the digital twin environment. In this part of the exercise, operators work with a restoration interface that combines the physical grid view and the communication network view, along with mapped command identifiers and operator action choices, such as manual or OPC-based recovery. The restoration workflow is intentionally human supervised: trainees inspect whether the relevant asset is already cyber reachable, verify the next proposed recovery step, compare physical and communication recovery status, and only then approve execution. In the underlying demonstrator described in Deliverable 5.1, additional support views expose the cyber layer recovery state, and the AI assisted reasoning behind the suggested action frontier, which helps operators understand why a specific restoration step is preferred and how the next action should be validated before proceeding. This trains participants in coordinated restoration after a severe disturbance, not as a purely electrical procedure but as a joint cyber-physical recovery process. The restoration interface shown in Figure 6c reflects this training perspective. This capability reutilizes the coordinated cyber-physical restoration outcomes from Task 4.2 and the associated WP5 Dutch TSO demonstration documented in D5.1.

Taken together, these TUD digital twin functions allow the Blue Team to train on three linked operator tasks: impact assessment of cascading effects, preventative islanding to mitigate them, and restoration from a blackout. The practical value of the training is that participants can move from cyber monitoring to consequence analysis, from consequence analysis to preventive action, and from preventive action to supervised



restoration within one coherent workflow. This makes the Blue Team exercise substantially richer because the trainees must reason across the interface between cyber security operations and power system operations while using the CRoF-based tools developed in eFORT.

4.3.3 Tools

The main tool used during the Red Team exercise is Armitage, a graphical cyber attack management interface built on the Metasploit framework. It has a Graphical User Interface (GUI) with networking capabilities, such as host discovery, service and port scans, and route creation. Using these capabilities, participants can create a route from the initially compromised host to the IT/OT DMZ subnet, then to the OPC server in the SCADA LAN, and eventually to the HMI. It is also utilized for the port forwarding described in the attack scenario. Armitage also provides access to exploit modules that can be executed against vulnerable machines. Participants can choose modules from this list to exploit the identified hosts and services.

The Blue Team is equipped with different tools for their activities.

A tool common to all teams is the Wazuh SIEM, used for monitoring activities. Wazuh is an open-source security monitoring platform that collects and analyses security relevant data from systems, applications, and infrastructure. Through Wazuh, users can detect suspicious activity and investigate security events.

Wazuh allows creating different users and user-specific dashboards. This made it possible to create a separate user for each team, allowing each team to see only the data relevant to their tasks. The host monitoring team analysed syslog data from different monitored hosts, while the flow monitoring and IT techniques teams received alerts from network sensors.

The network alerts are generated by Suricata, an open source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) that analyses network traffic and flags potential threats. In this environment, Suricata is configured to operate in IDS mode only. This is done to avoid blocking the activity of the Red Team, since the scope of the exercise is to detect and analyse the steps of the attack rather than to prevent or interrupt them. To detect malicious activity, Suricata uses predefined rules or "signatures", which allows it to identify known attack patterns.

The rules are configured differently for the two teams. The IT techniques team uses Suricata with a predefined set of rules. By contrast, the flow monitoring team receives alerts for all network traffic. The flow monitoring team also has access to PCAP files containing captured network traffic, enabling more detailed inspection of potentially malicious traffic. These packets can be examined using Wireshark, an open-source network packet analyser. Wireshark allows users to inspect individual packets, follow communication between hosts, and analyse protocols, ports, payloads, and other details of network traffic. This makes it useful for understanding what happens on the network and for validating whether specific traffic is benign or suspicious.

The IT-Techniques group also has access to an OpenVAS web interface, where they can analyse the results of a vulnerability scan previously executed on the network. OpenVAS is an open source vulnerability scanning tool that identifies known



vulnerabilities, misconfigurations, and weaknesses in systems and services. This allows the team to investigate possible entry points or vulnerable machines in the environment.

The main tool set for the cyber-physical part of the exercise is built around the CRoF cyber-physical co-simulation environment. The OT communication network is emulated using distributed Mininet instances running on several CRoF Linux servers, with each instance representing a substation LAN or another bounded OT segment. This makes it possible to realistically reproduce communication reachability, latency, service dependencies, and staged cyber recovery.

The cyber layer is coupled through an OPC UA server/interface to the DlgSILENT PowerFactory power system models running on the CRoF Windows server. PowerFactory serves as the electrical digital twin, providing the real time grid topology, operating point, and dynamic response needed for the demo. A FastAPI-based central interface is used to exchange data between the cyber range, the CRoF services, and the operator applications, and to trigger the corresponding monitoring, islanding, and restoration functions.

On top of this infrastructure, TUD provides the analytics and trained AI/ML-based operator support tools used in the training activity. These include the impact assessment functionality for cascading effects, the ML-based preventative islanding tool, and the AI assisted cyber-physical system restoration support. Through the dedicated GUIs, operators can inspect cyber alarms, physical grid status, candidate islanding cut sets, restoration frontiers, communication reachability, mapped commands, and the reasoning behind recommended actions.

4.4 Evaluation

The last element of the training model is the evaluation. The purpose of the evaluation is to assess whether the objectives outlined above are achieved. Immediately after the exercise, participants take part in a structured debriefing session in which they reflect on their performance and identify areas for improvement. The discussion is guided by standard evaluation questions and technical debriefing points aligned with the learning objectives, ensuring that the focus remains on practical performance rather than theoretical knowledge.

The debriefing is supplemented by the collection of quantitative feedback, and a delayed impact assessment conducted four weeks after the training. This multi-layered approach combines immediate qualitative reflection, quantitative evaluation, and an assessment of the longer-term impact of the training. An overview of the evaluation approach is presented in Figure 7.



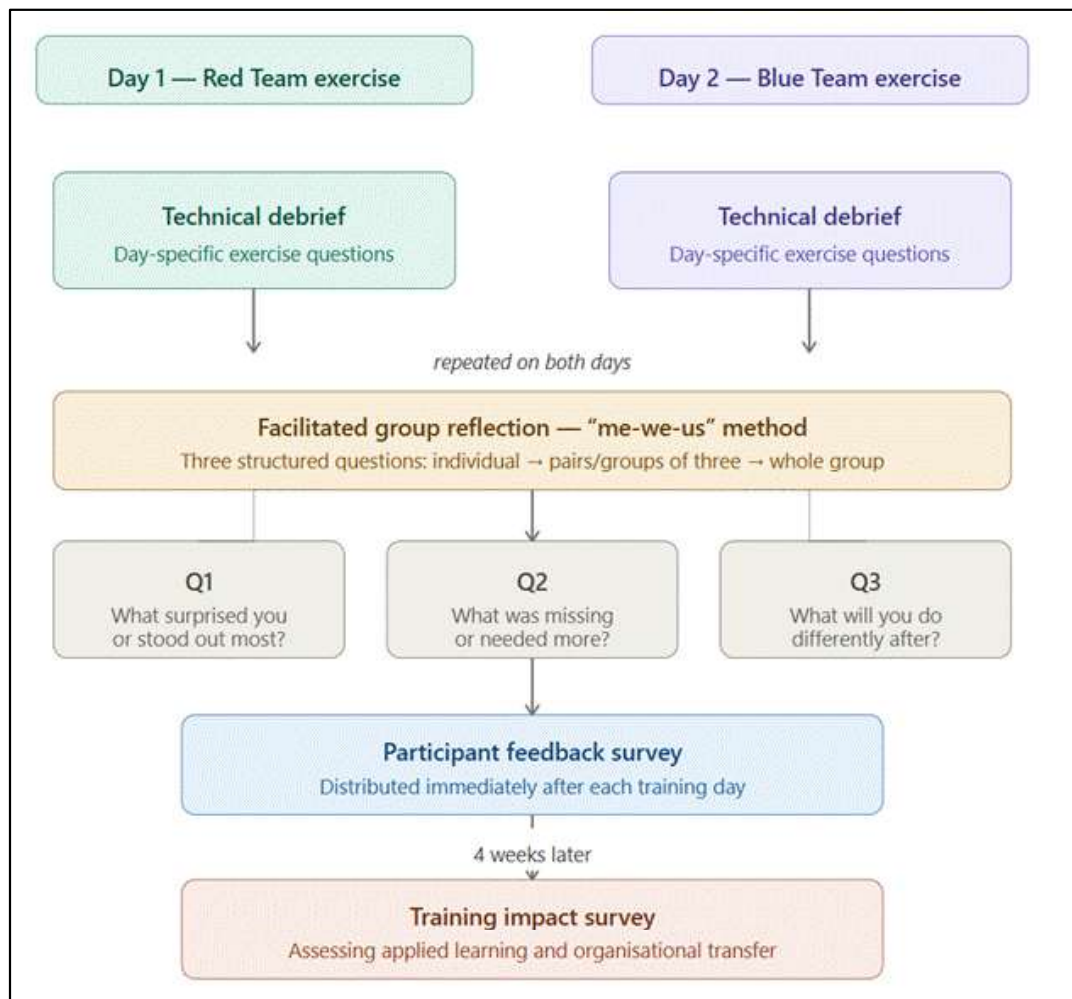


Figure 7. Overview of the evaluation methodology

4.4.1 Technical Debrief

The technical debrief provides a structured review of how participants approached and executed the exercise. The discussion is tailored to the respective training perspectives. Red Team participants review the sequence of actions they performed, the techniques and decision-making processes they applied, and the extent to which their approach achieved the intended objectives. Blue Team participants reflect on the methods used to identify and assess malicious activity, their coordination during the response, and the contribution of the digital twin to situational awareness and incident handling.

The debriefing also addresses the technical and operational difficulties encountered during the exercise, including points at which participants lacked information, experienced uncertainty, or needed to adapt their approach. Facilitators support participants in identifying effective practices, understanding the consequences of key decisions, and considering alternative approaches. The session concludes by translating these observations into practical lessons and areas for further development, while maintaining a clear focus on performance within the exercise rather than on theoretical knowledge.

4.4.2 Facilitated Group Reflection: the Me–We–Us Method

Additionally, a facilitated reflection of the exercise is conducted to evaluate the overall activity. This exercise employs the *me–we–us* methodology, a structured facilitation approach in which participants first answer three guiding questions individually, then discuss in pairs or groups of three, and finally share key insights with the whole group.

The three guiding questions are:

- *What surprised you or stood out to you the most today?*
- *Was there something you would have liked more of, or anything important that felt missing?*
- *What will you do differently, pay more attention to, or try out after today's training?*

4.4.3 Participant Surveys

A participant feedback survey is distributed immediately after each training day, covering satisfaction with the training structure, delivery, and practical organization, as well as perceived learning gains and likelihood of recommending the training to colleagues. Responses are collected on a five-point Likert scale, supplemented by open text fields. The survey is included in Annex 1.

Additionally, a post training survey will be sent to the participants four to six weeks after the training. This impact survey captures the degree to which participants have applied learning outcomes in practice, whether the training has influenced processes or team practices within their organizations, and any barriers encountered in knowledge transfer. The training impact survey instrument is provided in Annex 2.



5 Training Execution

This chapter describes how the training was prepared, delivered, and evaluated. It first outlines the practical setup of the training, including the technical environment and the materials used to support the sessions. It then presents the overall training flow, and the activities carried out on each day. Finally, the chapter reports the evaluation results and discusses the extent to which the training objectives are achieved, as well as the feedback provided by the participants.

5.1 Setup and Delivery

The training itself took place in the CRoF at TUD (see Figure 8). The morning sessions were dedicated to introductions, theory sessions, and hands-on sessions, followed by the exercise and debriefing in the afternoon. Representatives from ENCS presented and assisted participants for the morning sessions. In the afternoon, trainers took a secondary role, providing the minimum information needed and guiding participants if they encountered any difficulties.

Handouts were provided to the participants for the hands-on and exercise. The handouts included generic instructions for the participants to follow. The Blue Team exercise setting used during delivery is shown in Figure 9.

All participants attending on the first day were part of the Red Team. Participants returned to the session on the second day as the Blue Team. During the Blue Team exercise, representatives from ENCS took on the role of the Red Team to execute the scenario attack path.

TUD representatives were also present as technical facilitators for the CRoF-based cyber-physical part of the exercise. They supported the operation of the digital twin environment, coordinated the interaction between the cyber range and the TUD services, and guided participants whenever the scenario required the use of the TUD operator tools for impact assessment, islanding, or restoration.



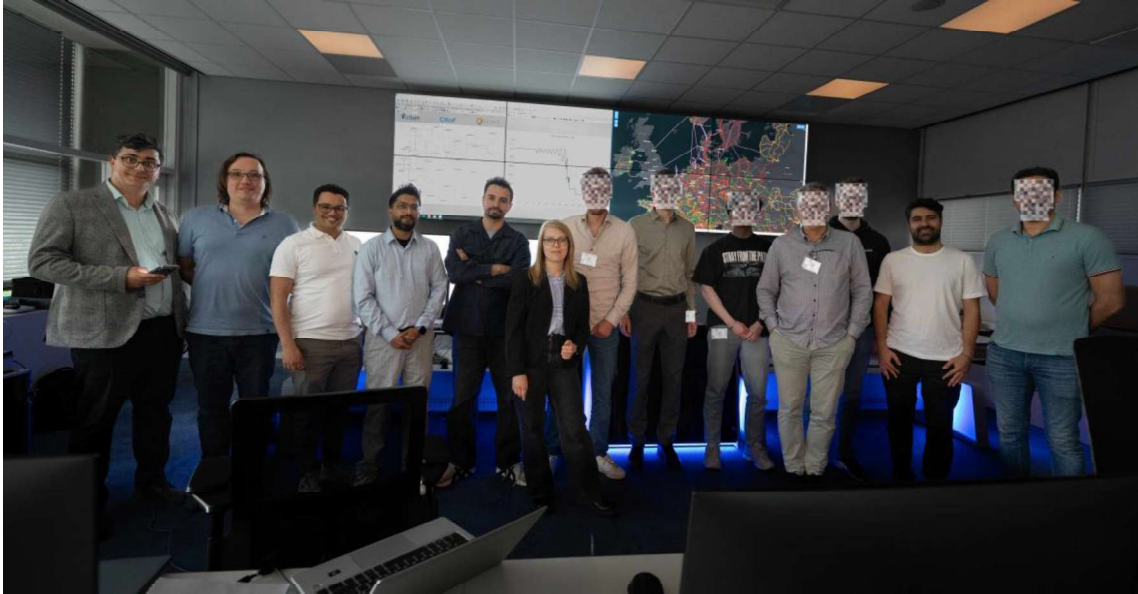


Figure 8. Red Team training day

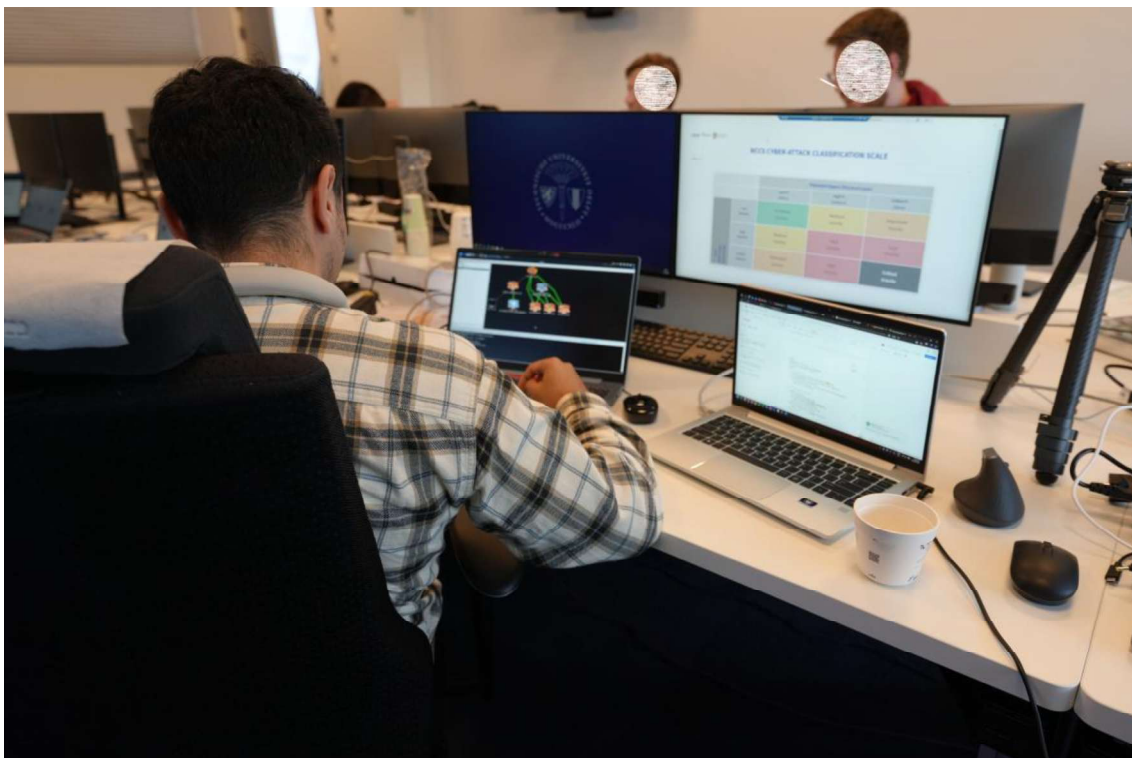


Figure 9. Blue team exercise during the second day of the training

5.1.1 Environment

The CRoF environment serves as the CRoF-based operational layer for the exercise. It hosts the power system digital twin in DigSILENT PowerFactory, the Mininet-based OT communication emulation, the OPC UA bridge, and the operator facing GUIs. During the Blue Team exercise, this environment complements the cyber range by allowing participants to follow how a cyber incident can affect the physical grid, assess cascading



effects, and explore mitigation and restoration actions in a supervised cyber-physical setting.

The environment is intended for training and demonstration rather than unrestricted free experimentation. It runs prepared models and orchestrated scenarios, so the available actions are bounded by the configured topology, the number of active workstations, and the need to keep the cyber range, CROF services, and digital twin snapshots synchronized. Some actions are therefore trainer guided and time sequenced to preserve scenario consistency, ensure stable execution of the Mininet, OPC UA, and PowerFactory chain, and keep the focus on the planned learning objectives. The prepared models represent the relevant operating and communication conditions of a transmission system operator: the PowerFactory model contains multiple substations and operating states suitable for cascading-effects assessment, preventive islanding, and blackout-restoration studies, while the distributed Mininet models reproduce bounded substation and control-centre OT segments with gateway hosts, field-device hosts, service dependencies, and constrained communication paths. Their coupling through OPC UA allows the training scenario to reproduce both physical-grid behavior and the loss or recovery of cyber reachability.

5.1.2 Materials

During the training, the participants were provided with the following list of materials:

- Handouts for:
 - Blue team network monitoring hands-on
 - Blue team vulnerability scanning and signature-based detection hands-on
 - Blue team host monitoring hands-on
 - Red Team hands-on session
- Credentials for laptops used during the exercise
- Network map of cyber range architecture

5.2 Training Flow

The training is carried out over two days, with one day dedicated to the Red Team and one to the Blue Team. Although the specific content and activities differ between the teams, the overall structure remains the same:

- **Introduction:** The session begins with an introduction outlining the purpose of the training and what participants can expect. Participants also receive a classroom-based session covering the knowledge and skills required to take part in the exercise. For the Red Team, this focuses on offensive security with emphasis on network scanning and post exploitation techniques, while the Blue Team's theory session focuses on vulnerabilities and preventive/responsive measures.
- **Exercise:** The introduction is followed by a practical exercise based on a realistic work-related scenario. Participants apply the knowledge and skills introduced during the classroom session in a simulated operational environment. The exercise



requires them to work through a sequence of activities, make decisions, and collaborate with other participants where relevant.

- **Debriefing:** Each training day concludes with a facilitated debriefing in which participants revisit the exercise and reflect on their performance. The debriefing enables trainers to assess whether the objectives have been achieved and provides feedback that can be used to improve the content, structure, and delivery of future training sessions.

5.2.1 Day 1: Red Team Training

The practical Red Team training, delivered by ENCS, consists of two components: guided hands-on sessions and a scenario-based exercise.

The guided hands-on sessions cover the following activities:

1. Participants first learn to analyse the segmented grid operator environment from an attacker perspective, with particular attention to potential pathways from the enterprise IT toward the OT/SCADA environment and the objective of progressively gaining access to deeper parts of the target network.
2. Participants then practice reconnaissance and network discovery by scanning the relevant network ranges, identifying reachable hosts, determining their roles, and analysing exposed services and open ports that may reveal potential attack paths.
3. They subsequently learn how to prepare and carry out exploitation activities using Armitage, including adding targets, running Nmap scans, matching identified services with suitable exploit modules, and obtaining an initial shell on a vulnerable host.
4. The training continues with post exploitation activities, including the use of elevated privileges, credential or hash extraction, session migration, remote access, and the application of pivoting techniques to move through intermediate systems and overcome network segmentation controls.

After completing the guided sessions, participants apply the acquired techniques in a realistic exercise involving a fictional grid operator network. This exercise is based on the scenario described in Section 3. Starting from the enterprise IT environment, they conduct a multi-stage attack and attempt to move through the segmented network towards the OT environment. The objective is to compromise the OPC server and use the obtained access to operate a circuit breaker. Participants are expected to identify and exploit suitable attack paths independently, combining reconnaissance, exploitation, post-exploitation, and pivoting techniques introduced during the guided sessions.

Figure 8 shows the Red Team training day.

5.2.2 Day 2: Blue Team Training

The Blue Team training combines ENCS cyber detection tasks with the TUD cyber-physical demonstration path:



1. Participants are first introduced to the Blue Team's mission, the division of responsibilities across the IT techniques, host monitoring, and network monitoring teams, and the two phases of the exercise: preparation and detection.
2. During the preparation phase, participants familiarize themselves with the cyber range architecture, analyse vulnerability scan results, examine logs, packet capture data, and syslog information, and propose mitigating measures that could disrupt or prevent the anticipated attack path.
3. During the detection phase, participants apply these methods to identify individual attack steps using supporting evidence, distinguish genuine security incidents from false positives, and report their findings so that detected activity and proposed mitigating actions can be documented on the exercise timeline.
4. Participants then observe how the attack progresses across the IT, DMZ, and OT layers, tracing the sequence of actions and understanding how activity in one part of the network enables further movement towards the operational environment.
5. Once the attack reaches substation level, the TUD component of the training demonstrates how the control room receives the cyber alert in the CRoF and uses the digital twin-based impact assessment function to estimate the physical consequences of the incident.
6. Participants are then introduced to preventive islanding as a form of operator decision support. They review the affected network zone, the current grid state, and the available islanding cut sets before a potential containment action is considered.
7. Finally, if the disturbance escalates, participants follow a cyber-physical system restoration demonstration in which communication path recovery, black start admissibility, manual versus OPC execution, and AI supported reasoning are used to coordinate cyber and physical recovery in one workflow.

5.3 Evaluation Results

A post exercise survey was distributed to all participants at the conclusion of both training days. From 8 participants, six respondents completed the survey on each day, representing the Red Team (Day 1, attacker perspective) and the Blue Team (Day 2, security operations perspective). Quantitative responses used a five-point Likert scale (1 = Strongly disagree, 5 = Strongly agree). Results are presented below by thematic cluster, followed by a summary of qualitative feedback.

5.3.1 Participant Overview

A total of 8 participants completed the post exercise survey across both training days, out of 8 participants, four attended on both days. There were six people present for the Red Team (Day 1) and six present for the Blue Team (Day 2).

The attendees represented a wide spectrum of the functions found in Electric Power and Energy Systems (EPES) operations, ranging from energy distribution operations and control centre, network and system admins, risk management, and OT security



operations. This also results in varying degrees of cyber security experience; some having more experience than others.

5.3.2 Quantitative Results

5.3.2.1 Overall Experience

Both teams reported broadly positive levels of overall satisfaction and felt the training met their expectations. The Blue Team recorded a higher mean satisfaction score (4.50 vs. 3.83), partly reflecting a single Red Team respondent who rated satisfaction at 2, noting the content was better suited to less experienced practitioners. Expectations were equally met across both groups, with a mean score of 4.17. These results are summarised in Figure 10.

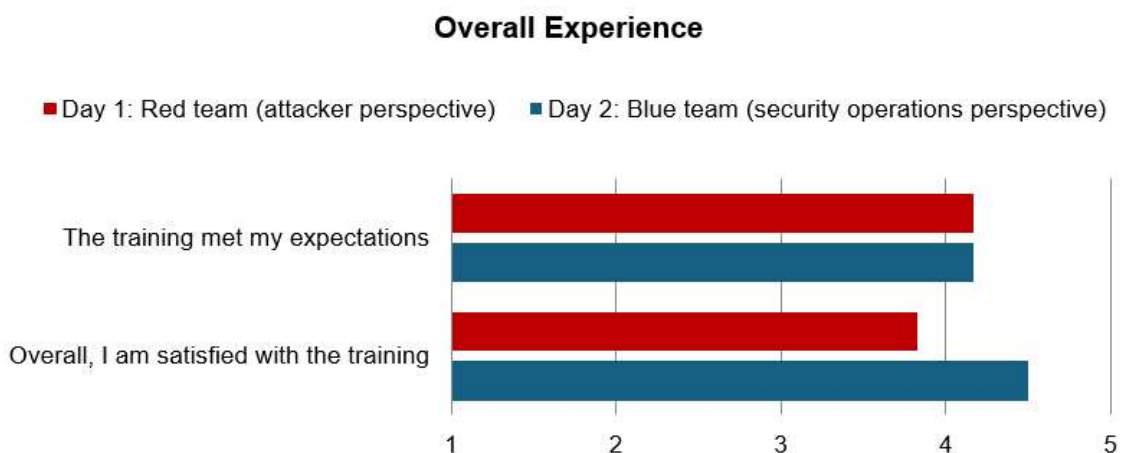


Figure 10. Mean scores for overall training experience (1 = Strongly disagree, 5 = Strongly agree)

5.3.2.2 Learning Outcomes

Content relevance was rated highly by both cohorts, with all 12 respondents providing a positive rating (4 or 5). Perceived understanding of cyber threats also scored well across both groups (Red Team 4.00, Blue Team 4.33). The largest divergence within this cluster appeared on the question of confidence in applying skills learned in practice: the Red Team returned a mean of 3.00 — the lowest score across the entire survey — compared to 3.83 for the Blue Team. This likely reflects the steeper technical prerequisites of offensive tooling compared to the detection and monitoring tasks conducted during the Blue Team session. The comparison is shown in Figure 11.



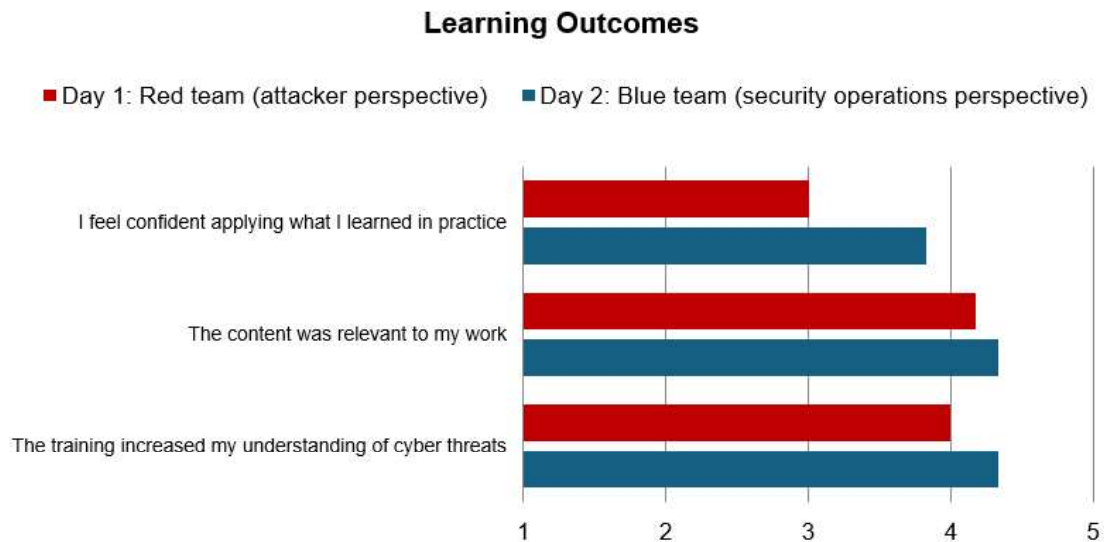


Figure 11. Mean scores for learning outcomes (1 = Strongly disagree, 5 = Strongly agree)

5.3.2.3 Delivery Quality

Training delivery was rated more favorably by the Blue Team across almost all questions in this cluster. Facilitator clarity received near unanimous positive ratings from both groups, with a mean of 4.67 (Blue Team) and 4.17 (Red Team). The combination of theory and hands-on sessions was also well received, particularly by the Blue Team (4.50 vs. 4.17). The most notable gap appeared in perceived structure: the Blue Team rated this at 4.33, while the Red Team averaged 3.33, the largest single difference across the whole survey. Qualitative responses suggest this reflects varying levels of prior Linux and networking experience among Red Team participants. Practical organization scored similarly across both groups (red 4.00, blue 3.83), with Blue Team comments pointing to minor logistical issues around navigation to the training venue. The delivery quality comparison is shown in Figure 12.

5.3.2.4 Likelihood to Recommend

Both teams recorded an identical mean score of 2.33 on Question 11, which asked how likely participants were to recommend the training. This item used the reverse-oriented scale presented in Annex 1 (1 = Very likely, 5 = Very unlikely); therefore, lower scores indicate stronger recommendation intent. The mean of 2.33 consequently indicates a generally positive intention to recommend the training. The distributions nevertheless differed: three of six Blue Team respondents selected "very likely", while Red Team responses were spread more evenly across the scale. Qualitative comments suggest that recommendation intent is strongly conditional on audience, as participants consistently noted that the training is most appropriate for those with a baseline in networking or security operations. The response distribution is shown in Figure 13.



Delivery Quality

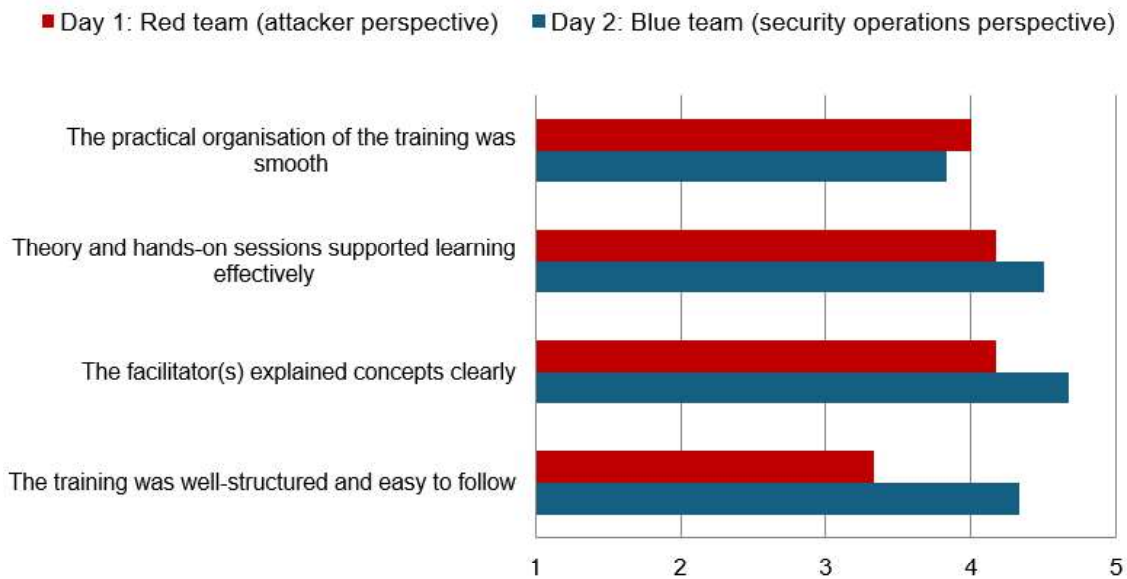


Figure 12. Mean scores for delivery quality (1 = Strongly disagree, 5 = Strongly agree; n=6 per team)

Likelihood to Recommend

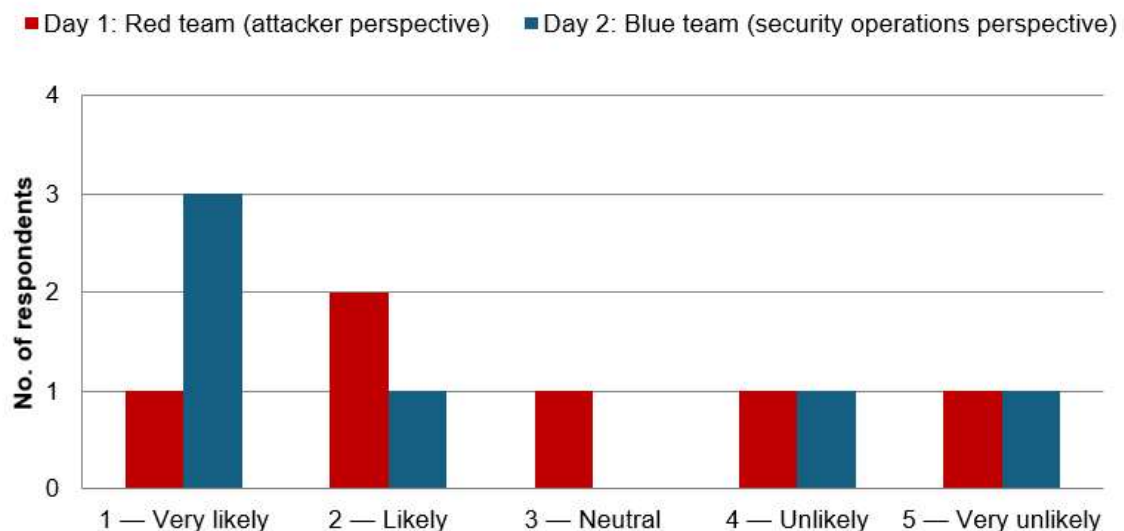


Figure 13. Distribution of responses to “How likely are you to recommend this training to a colleague?”

5.3.3 Qualitative Results

In addition to the quantitative Likert survey questions, participants were also asked three open-ended questions: key takeaways from the training, reasons for their recommendation rating, and suggestions for improvement. A summary of responses is provided below.



5.3.3.1 Key Takeaways

Red Team participants emphasized gaining insight into the attacker's perspective, particularly the step-by-step logic of a real attack, including reconnaissance, pivoting, and exploitation. Blue team respondents focused on systemic themes: the importance of early vulnerability identification, the ease with which an attacker can move laterally once inside a network, and the value of clear communication between security and operations teams during an incident.

5.3.3.2 Recommendation Rating Rationale

Across both groups, the training was considered most valuable for participants with limited prior cyber security exposure. Several respondents noted it provides a strong conceptual foundation but may fall short for more senior practitioners seeking advanced or realistic attack scenarios. Blue team participants were more emphatic in their intent to recommend, particularly citing the close link to real SOC operations and the clarity of the causal chain from attack to impact.

5.3.3.3 Suggestions for Improvement

The most consistent theme across both groups was the need to better communicate prerequisites in advance, ensuring participants have the foundational knowledge required to engage fully with the hands-on components. Red Team respondents raised technical issues including server stability, the complexity of the network setup, and tool reliability (Armitage). Blue team respondents highlighted logistical improvements around directions to the training venue and called for more advanced attack scenarios and better tooling support for network monitoring tasks.

5.4 Lessons Learned

Through the training, valuable insights can be gained into participant performance, training design, and execution. While the participants were overall satisfied with the training, several improvements can be derived from the feedback received.

Key concerns raised surrounding logistical improvements, training difficulty, and tool stability. A minor consideration for future training is clarity on directions to the precise training venue. To prevent confusion, mitigating steps can be taken, such as the use of signs and coordination with the front desk at the venue.

From the practical execution of the training, some participants have noted challenges in following the hands-on session, thus hindering an effective learning process. To bridge the gap in participant understanding, the training could be more facilitative by providing explanations in each step of the hands-on sessions. Providing the rationale for actions during the hands-on can provide the necessary contextual information, thereby improving participants' understanding and engagement throughout the sessions and exercises.

To further alleviate these issues, defining prerequisites for the technical knowledge base will allow trainers to target the appropriate audience and ensure effective knowledge transfer during training.



As participants' experience in cyber security varies, the perceived difficulty of the training also varies. Senior security practitioners indicated that the exercise falls short of providing in-depth security knowledge and of incorporating complex real world threats. From a training design perspective, the attack path can reference real advanced persistent threat (APT) tactics and tools to add complexity to the exercise for SOC and security advanced participants. If time is not constrained, conducting the exercise with multiple advanced scenarios will allow participants to repeatedly apply practical skills.

From a trainer's perspective, the training currently lacks an integrated system to track the learning outcomes of each participant; the visibility of participant performance and skills learned could be improved. Future iterations of the training can incorporate a scoring-based system into the cyber range platform to digitally track user actions and provide correct assessments on the steps taken throughout the exercise.

The exercise identified several technological gaps and needs for future training iterations. The most immediate needs are greater stability and repeatability across the cyber range-CRoF integration chain, more reliable scenario reset and synchronization between Mininet, OPC UA, PowerFactory, and the operator applications, stronger network-monitoring support, and an integrated mechanism for recording participant actions and learning outcomes. The feedback also showed a need for clearer technical prerequisites and for additional advanced scenarios that can challenge experienced security practitioners.

Besides, the exercise provided operational evidence that the eFORT innovations can work together under the prepared training conditions. The cyber range, CRoF digital twin, cyber-monitoring tools, impact-assessment dashboard, machine-learning-based islanding support, and AI-assisted cyber-physical restoration workflow were combined in one end-to-end sequence. Participants could follow an attack from reconnaissance and exploitation through detection and cyber-physical consequence assessment to mitigation and restoration decisions. This does not replace the detailed technical validation reported in D5.1, but it confirms that the developments can be integrated into a coherent operator-facing workflow and used for training.

The lessons learned led mainly to operational adjustments, not an immediate redesign of algorithms. Trainer guidance and timing maintained synchronization and supported participants during interventions. Remaining findings are now concrete recommendations, including better handouts, clearer communication, more facilitative explanations, tool-stability improvements, advanced scenarios, and digital performance tracking.



6 Conclusion

This deliverable shows that the eFORT Task 4.7 training successfully translated project developments into a practical learning environment for grid operators and cyber defenders. By combining the ENCS cyber range with the TUD CRoF environment, the training exposed participants to the full chain from attacker behavior and evidence-based detection to cyber-physical impact assessment, preventive mitigation, and OT recovery and power grid restoration support. In this respect, the training did not treat cyber security and power system operation as separate domains, but as linked operational responsibilities.

The evaluation results indicate that the training was perceived as relevant and useful, particularly in helping participants understand how cyber incidents can propagate toward operational consequences and how eFORT tools can support response and resilience. At the same time, the exercise highlighted concrete improvement points for future iterations, including clearer prerequisite communication, more facilitative hands-on guidance, improved tool stability, and better mechanisms for tracking participant learning progression.

Overall, the work reported here confirms the value of using integrated cyber-physical demonstrator environments not only for technical validation, but also for human capital development. Future training iterations can build on this basis by refining the exercise flow, extending advanced scenarios, and further strengthening the operational integration between cyber range activities and CRoF-based decision support demonstrations.



References

- ISA / IEC. (2019). ISA 62443-4-2 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components.
- Stolovitch, H. D., & Keeps, E. J. (2011). Telling ain't training. Association for Talent Development.
- Williams, T. J. (1994). The Purdue Enterprise Reference Architecture. *Computers in Industry*, 24, 141-158.
- Chow Editor, J. H. (n.d.). Power Electronics and Power Systems Power System Coherency and Model Reduction. <http://www.springer.com/series/6403>
- ENTSO-E Transmission System Map. (2019). <https://www.entsoe.eu/data/map/>
- Kipf, T. N., & Welling, M. (2016). Variational Graph Auto-Encoders 1 A latent variable model for graph-structured data.
- Mininet: An Instant Virtual Network on Your Laptop. (n.d.). Retrieved 23 April 2025, from <https://mininet.org/>
- Presekal, A., Stefanov, A., Rajkumar, V. S., & Palensky, P. (2023). Attack Graph Model for Cyber-Physical Power Systems Using Hybrid Deep Learning. *IEEE Transactions on Smart Grid*, 14(5), 4007–4020. <https://doi.org/10.1109/TSG.2023.3237011>



Annex 1: Training Feedback Survey



eFort RedTeam-BlueTeam Training Participant Feedback Survey

Thank you for joining the RedTeam-BlueTeam training. We would appreciate your feedback. This short survey asks about your overall experience, including how useful and relevant you found the training for your work. We are also interested in your main takeaways and whether there is anything you may do differently as a result of the training.

Your feedback will help us improve future OT cybersecurity trainings and better understand what supports learning, preparedness, and practical application.

The questionnaire is anonymous and the results will be analysed in aggregate form.

Please answer the following questions:

1. Overall, I am satisfied with the training

Strongly disagree	Slightly disagree	Neutral	Slightly agree	Strongly agree
☐	☐	☐	☐	☐
2. The training met my expectations

Strongly disagree	Slightly disagree	Neutral	Slightly agree	Strongly agree
☐	☐	☐	☐	☐
3. The training increased my understanding of cyber threats and response measures

Strongly disagree	Slightly disagree	Neutral	Slightly agree	Strongly agree
☐	☐	☐	☐	☐
4. The content was relevant to my work

Strongly disagree	Slightly disagree	Neutral	Slightly agree	Strongly agree
☐	☐	☐	☐	☐
5. I feel confident applying in practice what I learned

Strongly disagree	Slightly disagree	Neutral	Slightly agree	Strongly agree
☐	☐	☐	☐	☐
6. The training was well-structured and easy to follow

Strongly disagree	Slightly disagree	Neutral	Slightly agree	Strongly agree
☐	☐	☐	☐	☐
7. The facilitator(s) explained concepts clearly

Strongly disagree	Slightly disagree	Neutral	Slightly agree	Strongly agree
☐	☐	☐	☐	☐



This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.



This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.



8. The combination of theory and hands-on practical sessions supported learning effectively

Strongly disagree	Slightly disagree	Neutral	Slightly agree	Strongly agree
☐	☐	☐	☐	☐

9. The practical organization of the training was smooth

Strongly disagree	Slightly disagree	Neutral	Slightly agree	Strongly agree
☐	☐	☐	☒	☐

10. What are the two most important things you are taking away from this training?

11. How likely are you to recommend this training to a colleague?

Very likely	Somewhat likely	Neutral	Slightly unlikely	Very unlikely
☐	☐	☐	☐	☐

12. What was the reason for your answer above?

13. What could be improved in future training?

14. Do you have any additional comments or suggestions? Please mention here:



This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.



Annex 2: Training Impact Survey



eFort RedTeam-BlueTeam Training Training Impact Survey

Thank you again for taking part in the RedTeam-BlueTeam training. We would appreciate your feedback on how the training has supported your work since then. This short survey asks about the relevance and value of the training for your work in practice. We are interested in which elements have been most useful, and whether the training has influenced your work, your team, or your organisation in any way.

Your feedback will help us improve future OT cybersecurity trainings and better understand what supports learning, preparedness, and practical application over time.

The questionnaire is anonymous and the results will be analysed in aggregate form.

Please answer the following questions:

1. How relevant has the training been to your work since attending it?

Not at all relevant	Slightly relevant	Neutral	Very relevant	Extremely relevant
☐	☐	☐	☐	☐

2. Looking back, how would you rate the overall value of the training?

Not valuable at all	Slightly valuable	Moderately valuable	Very valuable	Extremely valuable
☐	☐	☐	☐	☐

3. How much of what you learned during the training have you been able to apply in practice?

Not at all	A little	Somewhat	Quite a lot	A great deal
☐	☐	☐	☐	☐

4. Which elements of the training have been most useful in practice?

5. What have been main obstacles, if any, to applying what you have learned?



This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.





6. Have you shared any knowledge, tools, or approaches from the training with colleagues who did not attend?

Yes	Partly	No	Does not apply to me
☐	☐	☐	☐

7. Has the training influenced any decisions, projects, processes or ways of working in your team or organisation?

Yes	No	Unsure	Does not apply to me
☐	☐	☐	☐

8. In case you answered “yes” to the previous question, what has changed?

9. Do you have any additional comments or suggestions for us? Please mention here:



This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

