eFORT

This project has received funding from the European Union’s **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

eFORT Incident Response and Resilience Actions

29-08-2023

eFORT

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

ARES Conference – EPESec Workshop

Swarna Kumarswamy-Das, TNO The Netherlands

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Outline

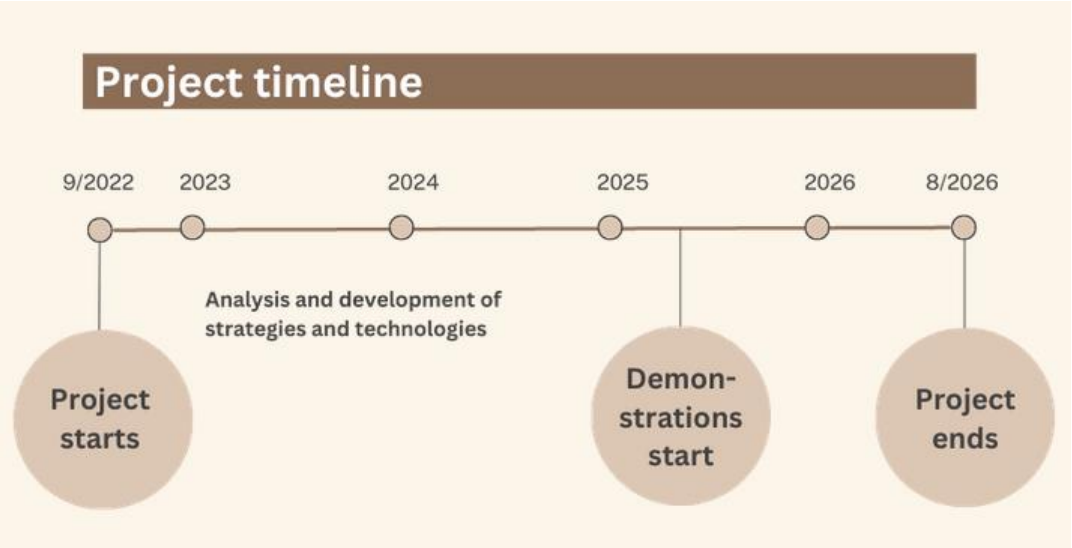
1. Introduction - eFORT
2. Incident response
3. Resilience actions

This project has received funding from the European Union’s **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Introduction - eFORT

Coordinator: CIRCE (ES)

9 million € Budget	**23** Partners	**9** European countries



Project timeline

9/2022 — 2023 — 2024 — 2025 — 2026 — 8/2026

Project starts

Analysis and development of strategies and technologies

Demon-strations start

Project ends

4 Demonstrators:

Escúzar, Spain
DSO-micro grid

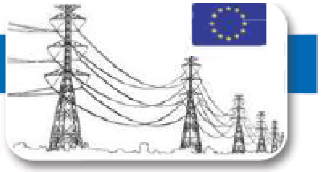
Delft, The Netherlands
TSO

Sarentino Valley, Italy
DSO

Iltsi, Ukraine
Substation

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

eFORT



4 Innovation Pillars

1 ENHANCED TOOLS FOR ANALYSING EPES' RISKS AND THREATS

2 MEASURES AND TECHNOLOGIES TO STRENGTHEN EPES' ROBUSTNESS

3 MORE SECURE AND PRIVATE GRID DATA MANAGEMENT

4 OPERATIONAL TECHNOLOGIES AND STRATEGIES FOR UPGRADING GRID RESILIENCY

Set of solutions

Intelligent Platform (software)

- Vulnerabilities database
- Interactive visualization tool
- Dynamic risk assessment tools (cyber and physical)
- Self-healing algorithm

Asset management

- Cascading effects and inter-area oscillations impact on TSO stability
- Secure TSO-DSO data sharing procedures
- IoT security advances
- Real-time islanding operation and decision support for grid restoration
- Digital Substations (process bus, RTU, BIM, advanced LAN)
- Securebox (IDS/IPS execution, secure DER operation, tamper proof, encryption techniques)
- Control Room of Future (training, CSIRT)

Digital technologies

- Intrusion detection and prevision systems - Security Information and event management
- Digital twins of the whole interconnected power grid
- Blockchain for grid resiliency and verification
- AI-based control algorithms
- Edge computing and IoT

4 Demonstrators

TSO level: Cascading effects and restoration of interconnected power grids

DSO level: Flexibility and islanding on mountainous and remote areas

Substation: Digitalisation and secure design of a substation

DSO-micro grid: IoT, blockchain and cybersecurity in a prosumer-grid

- Techno-Economic analysis
- Replication potential evaluation
- Assessment of business models
- Recommendations for standards and regulations
- Exploitation of synergies with BRIDGE initiatives

↑ Reliability, ↑ Resiliency, ↑ Security

vs.

Failures, Cyberattacks, Physical disturbances, Data privacy issues

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Demonstration 2 – The Netherlands

Preventing cascading failures and restoring interconnected power grids

Key partners

Lead: TenneT

TNO

European Network for Cyber Security

DNV

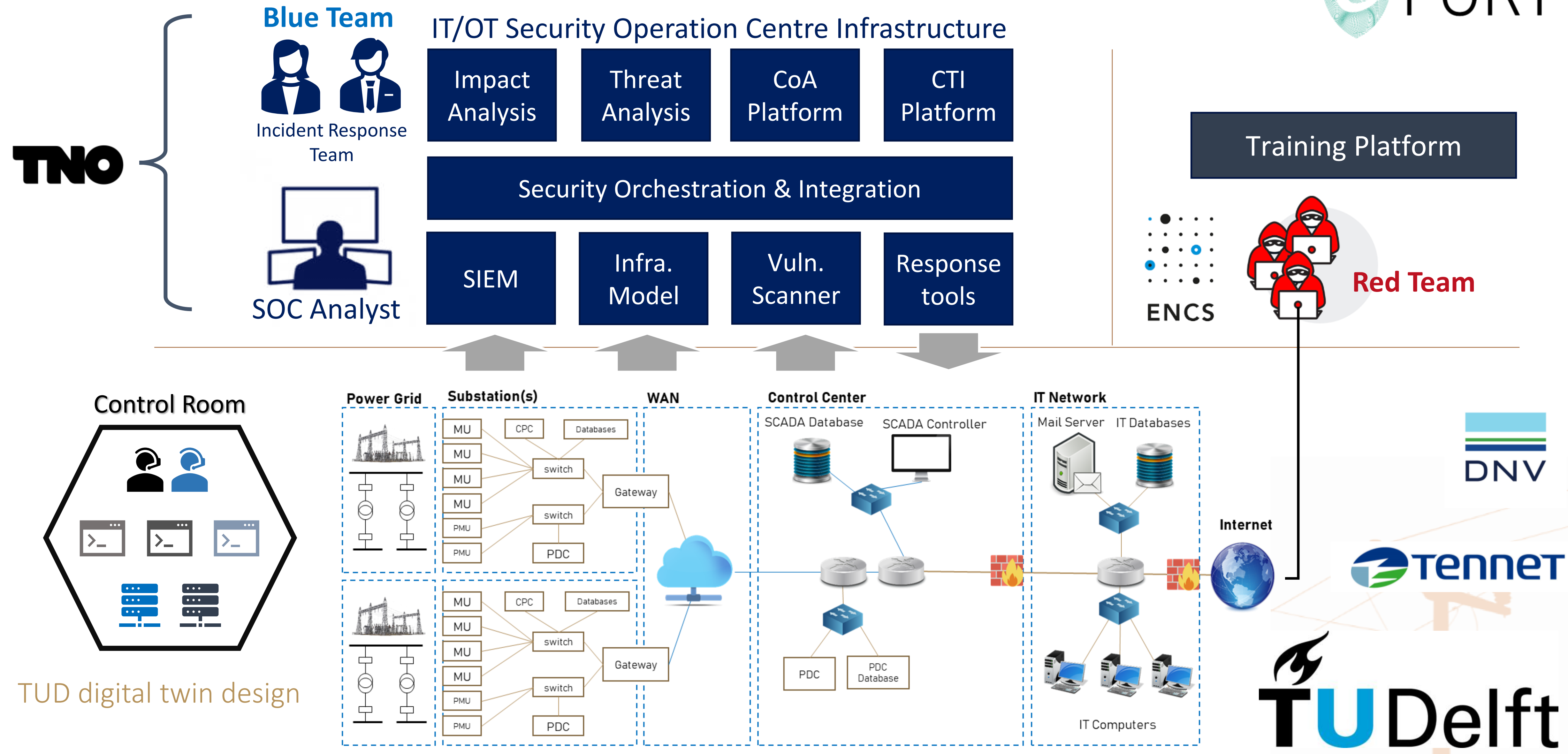
Delft University of Technology

CIRCE

- Digital Twin of Power grid & cyber range for IT/OT equipment & network
- Control Room station
- Security Operation Centre

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Dutch sub-consortium in eFORT



Blue Team

Incident Response Team

SOC Analyst

IT/OT Security Operation Centre Infrastructure

Impact Analysis

Threat Analysis

CoA Platform

CTI Platform

Security Orchestration & Integration

SIEM

Infra. Model

Vuln. Scanner

Response tools

Training Platform

Red Team

Control Room

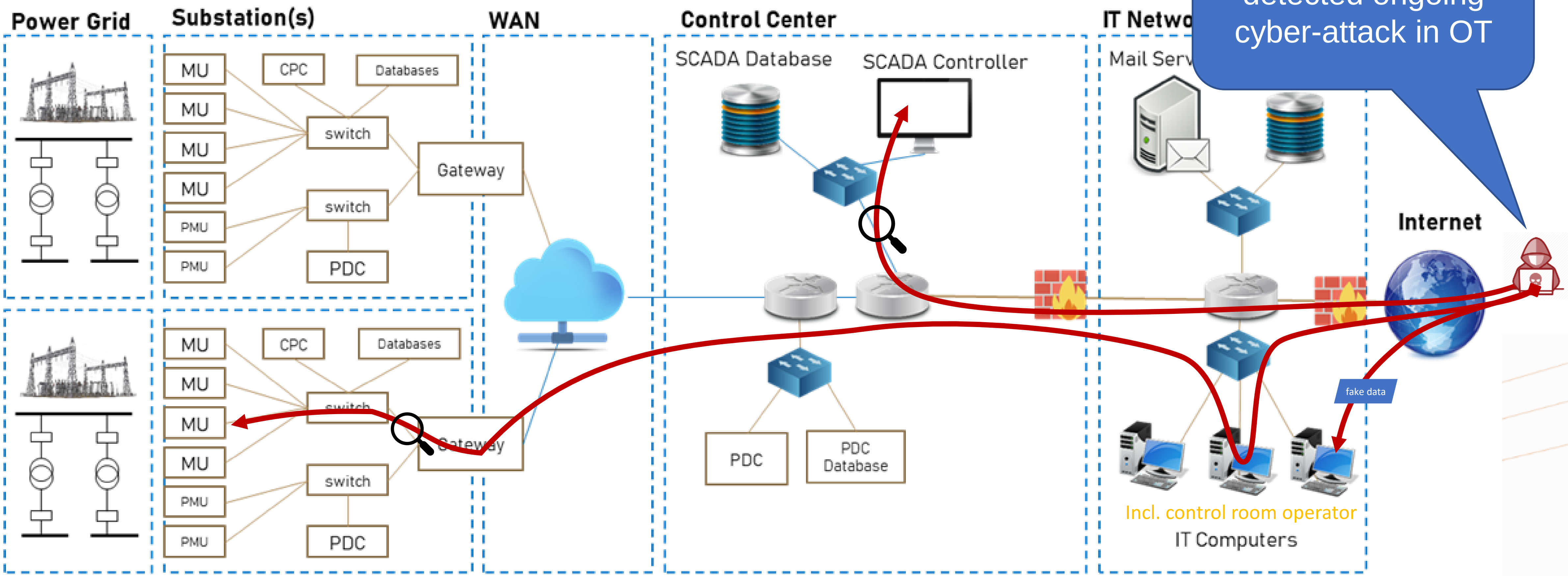
TUD digital twin design

MU: Merging Unit – PMU: Phasor Measurement Unit – CPC: Centralized Protection and Control – PDC: Phasor Data Concentrator

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Use cases

UC1. Responding to detected ongoing cyber-attack in OT

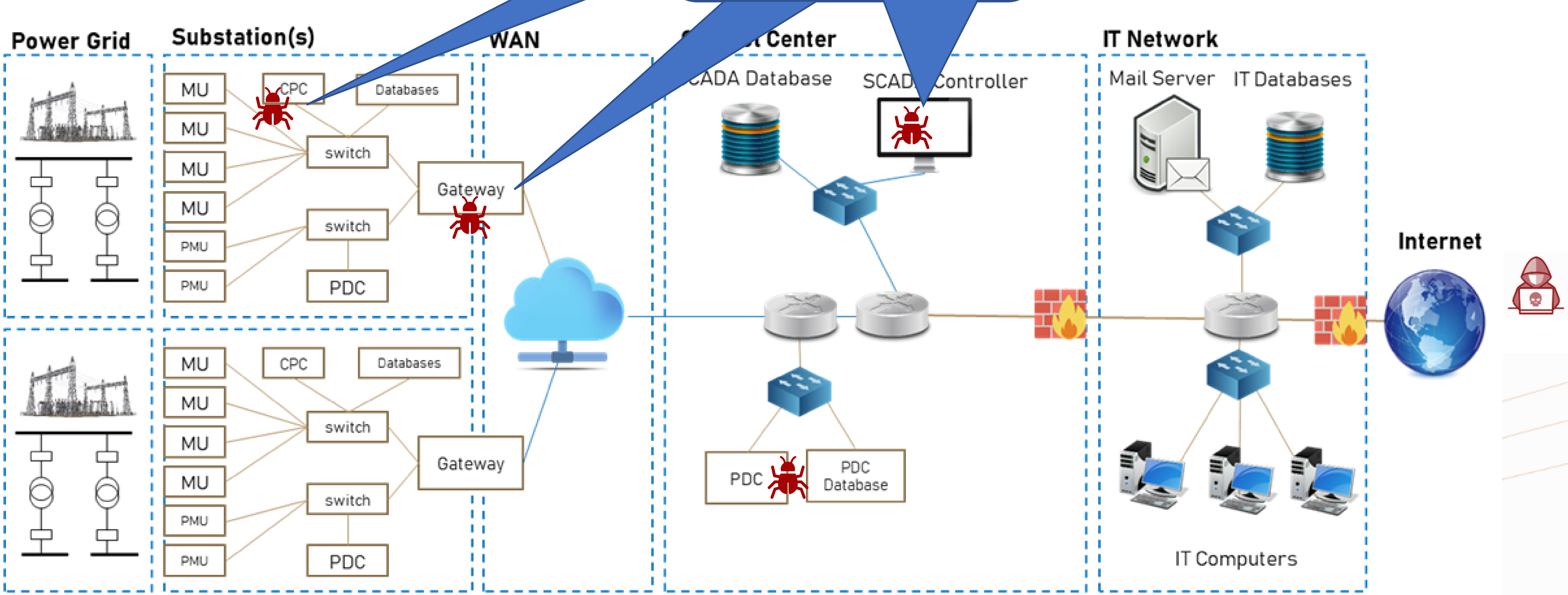


MU: Merging Unit – PMU: Phasor Measurement Unit – CPC: Centralized Protection and Control – PDC: Phasor Data Concentrator

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Use cases

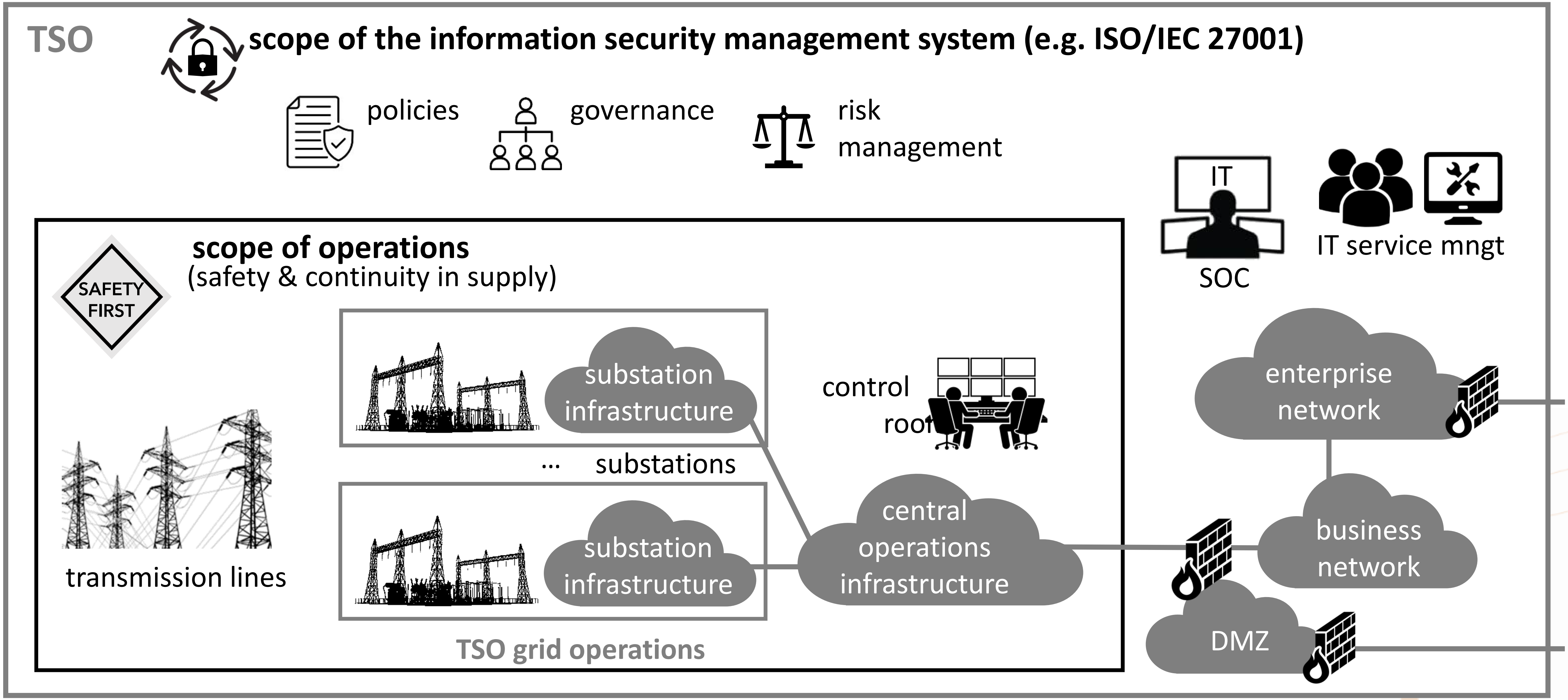
UC2. Responding to new vulnerability in OT systems



MU: Merging Unit – PMU: Phasor Measurement Unit – CPC: Centralized Protection and Control – PDC: Phasor Data Concentrator

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

eFORT – TNO focus (as is)



TSO

scope of the information security management system (e.g. ISO/IEC 27001)

policies

governance

risk management

IT

SOC

IT service mngt

scope of operations

(safety & continuity in supply)

SAFETY FIRST

substation infrastructure

… substations

substation infrastructure

control room

transmission lines

central operations infrastructure

TSO grid operations

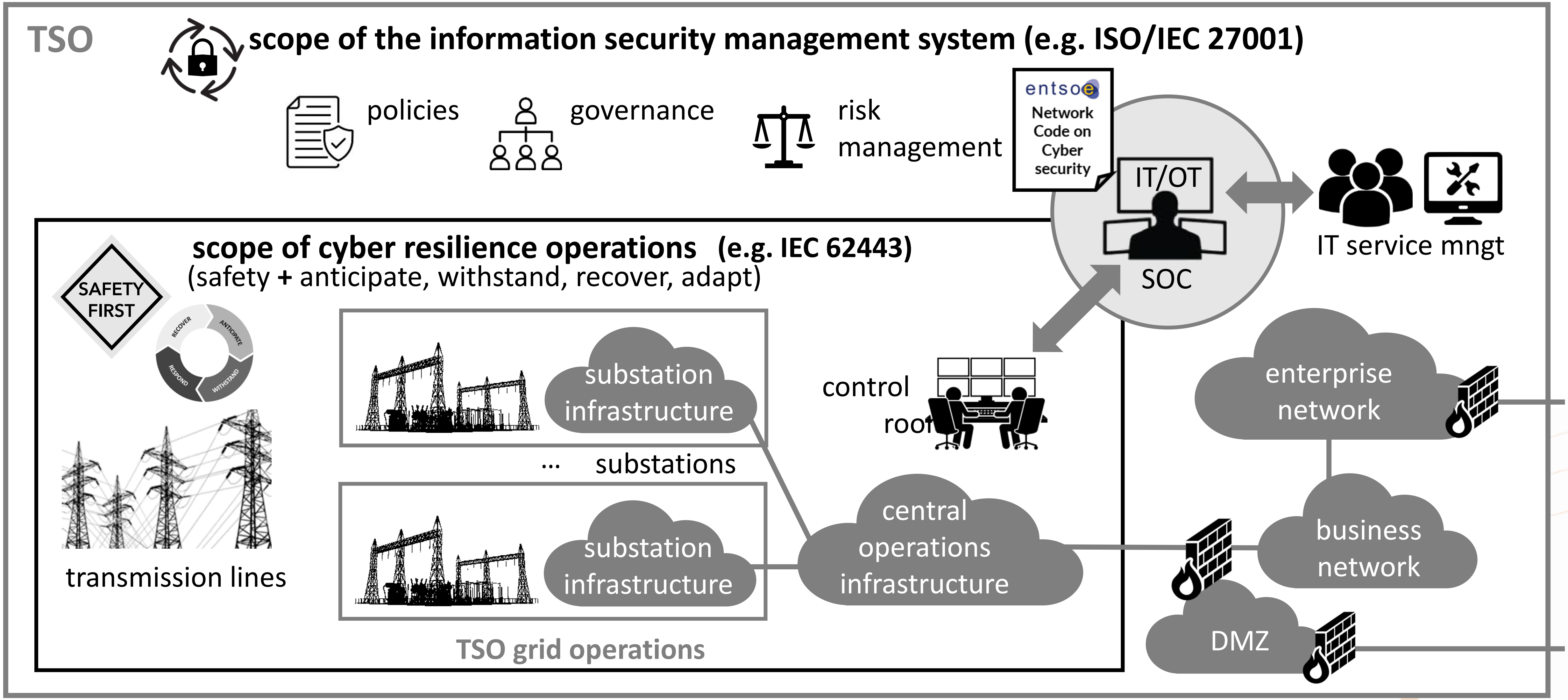
enterprise network

business network

DMZ

This project has received funding from the European Union’s **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

eFORT – TNO focus (to be)



TSO

scope of the information security management system (e.g. ISO/IEC 27001)

policies

governance

risk management

entsoe Network Code on Cyber security

IT/OT

SOC

IT service mngt

scope of cyber resilience operations (e.g. IEC 62443)

(safety **+** anticipate, withstand, recover, adapt)

SAFETY FIRST

substation infrastructure

… substations

substation infrastructure

control room

central operations infrastructure

transmission lines

TSO grid operations

enterprise network

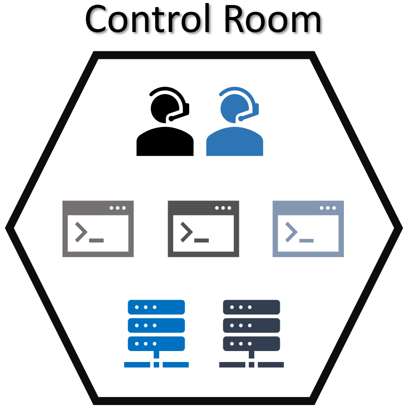
business network

DMZ

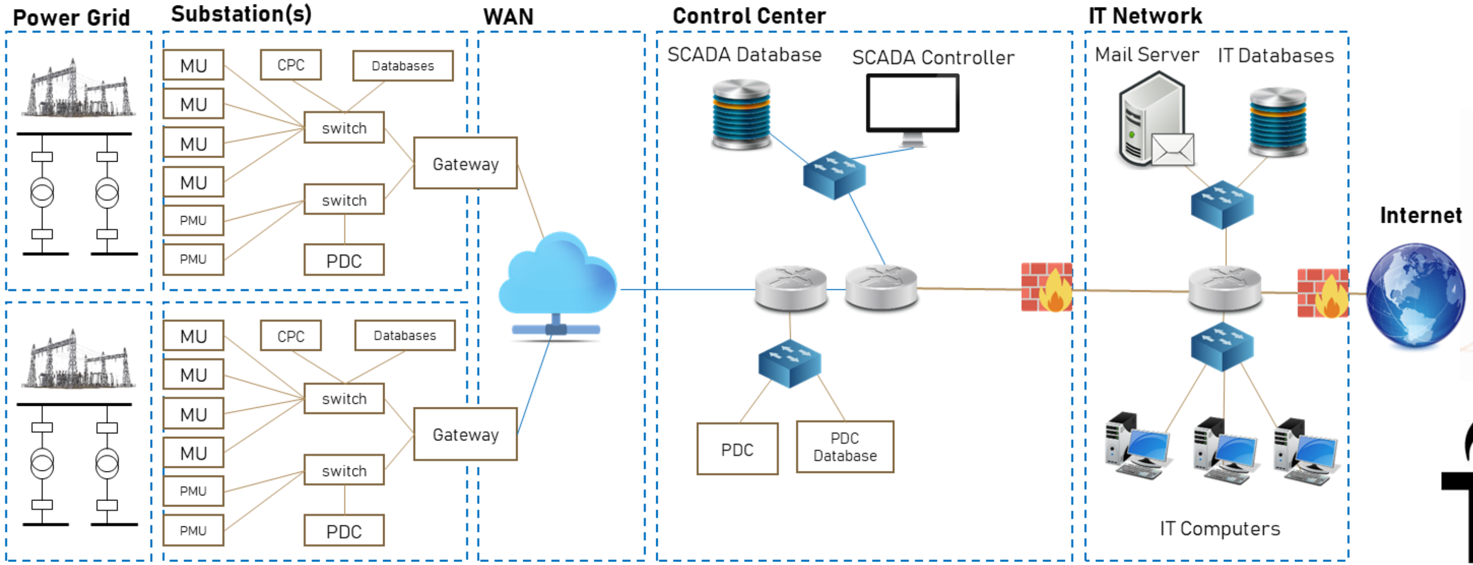
This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Demonstrator in NL

Control Room of the Future (CRoF)



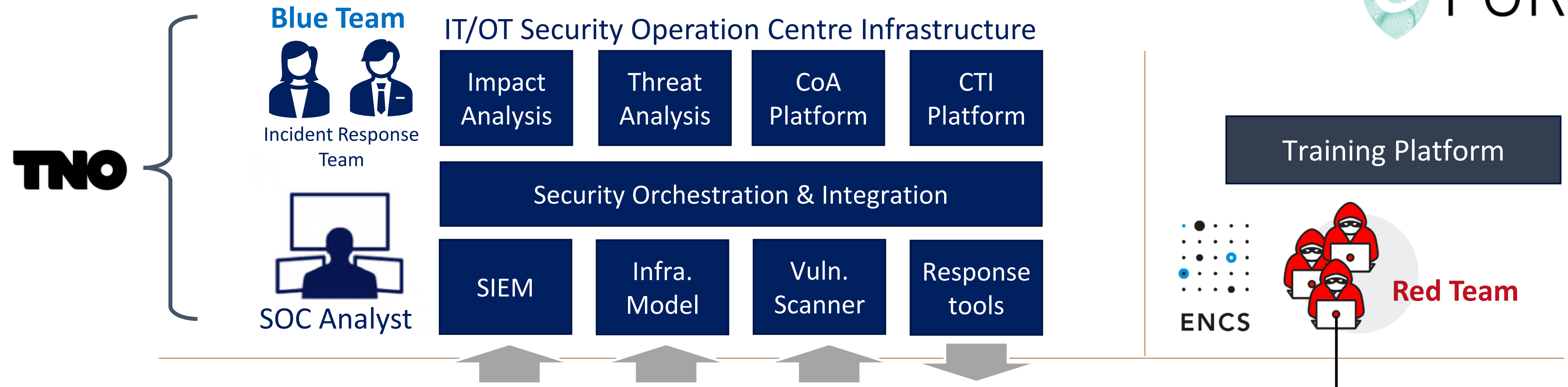
digital twin design



MU: Merging Unit – PMU: Phasor Measurement Unit – CPC: Centralized Protection and Control – PDC: Phasor Data Concentrator

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Dutch sub-consortium in eFORT



TNO

Blue Team

Incident Response Team

SOC Analyst

IT/OT Security Operation Centre Infrastructure

Impact Analysis

Threat Analysis

CoA Platform

CTI Platform

Security Orchestration & Integration

SIEM

Infra. Model

Vuln. Scanner

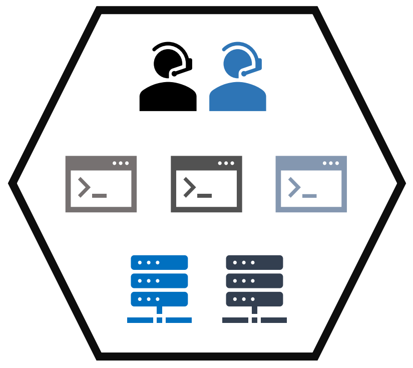
Response tools

Training Platform

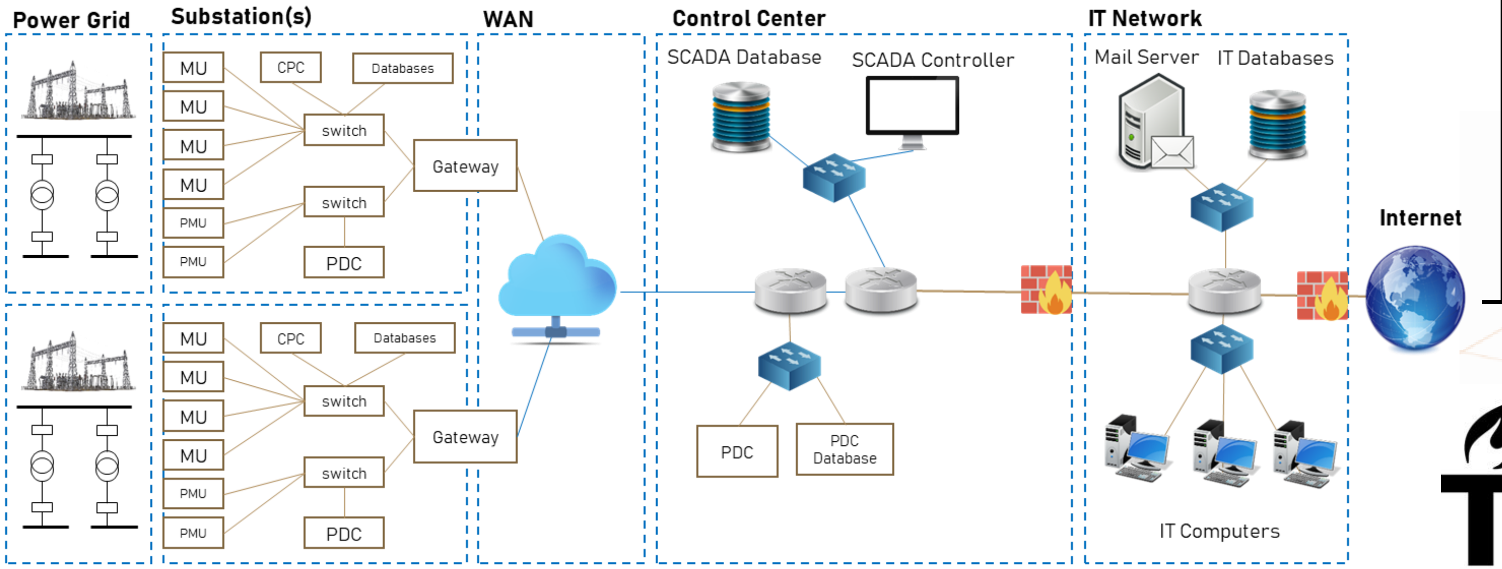
ENCS

Red Team

Control Room



TUD digital twin design



MU: Merging Unit – PMU: Phasor Measurement Unit – CPC: Centralized Protection and Control – PDC: Phasor Data Concentrator

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

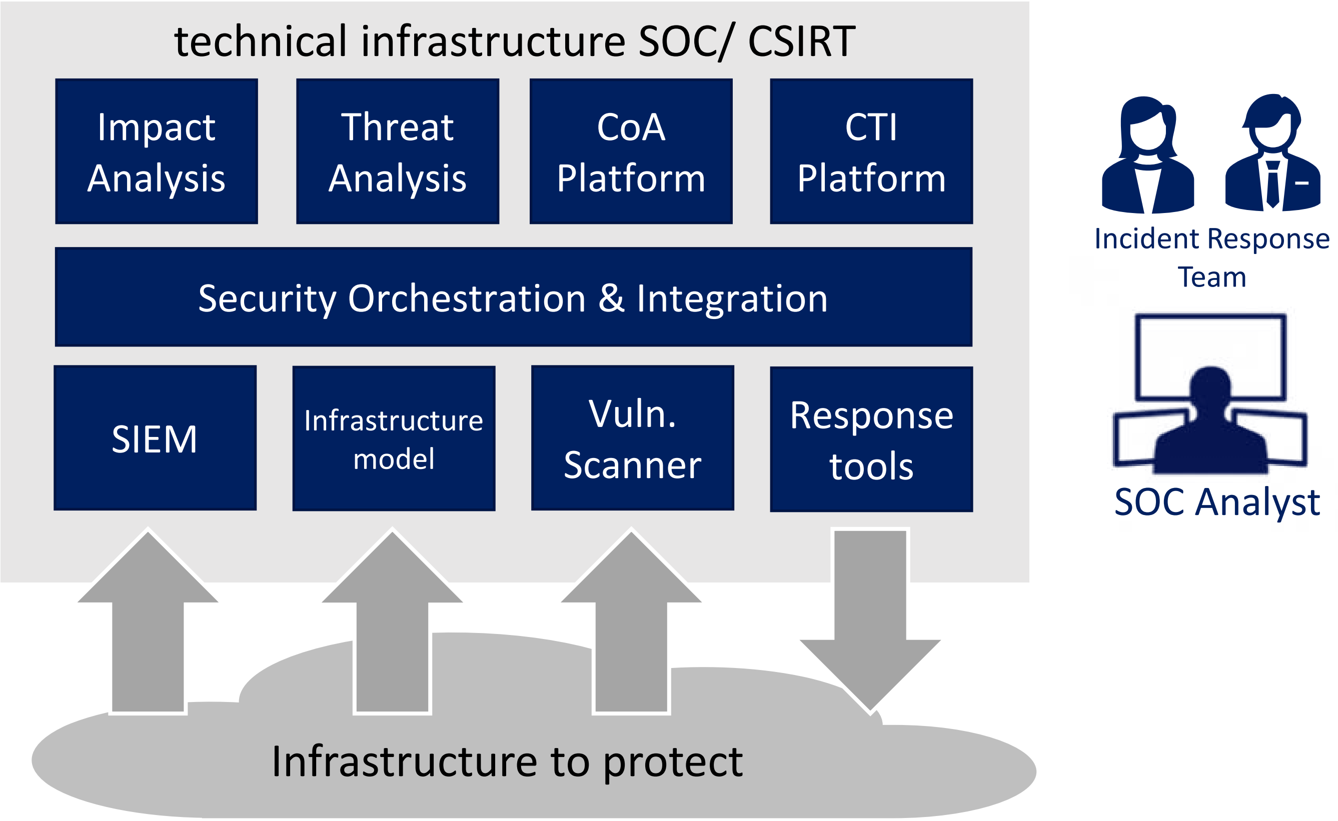
Outline

1. Introduction - eFORT
2. Incident response
3. Resilience actions

This project has received funding from the European Union’s **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

SOC / CSIRT for EPES

IT/OT Security Operation Centre Infrastructure



IEC 62443-2-1

- SPE4 COMP 3 – Patch management
- SPE 7 – Event and incident management

FIRST Services Framework

Service Areas

- (Information) Security Event Management
- (Information) Security Incident Management
- Vulnerability Management

11 Strategies of a World-Class SOC

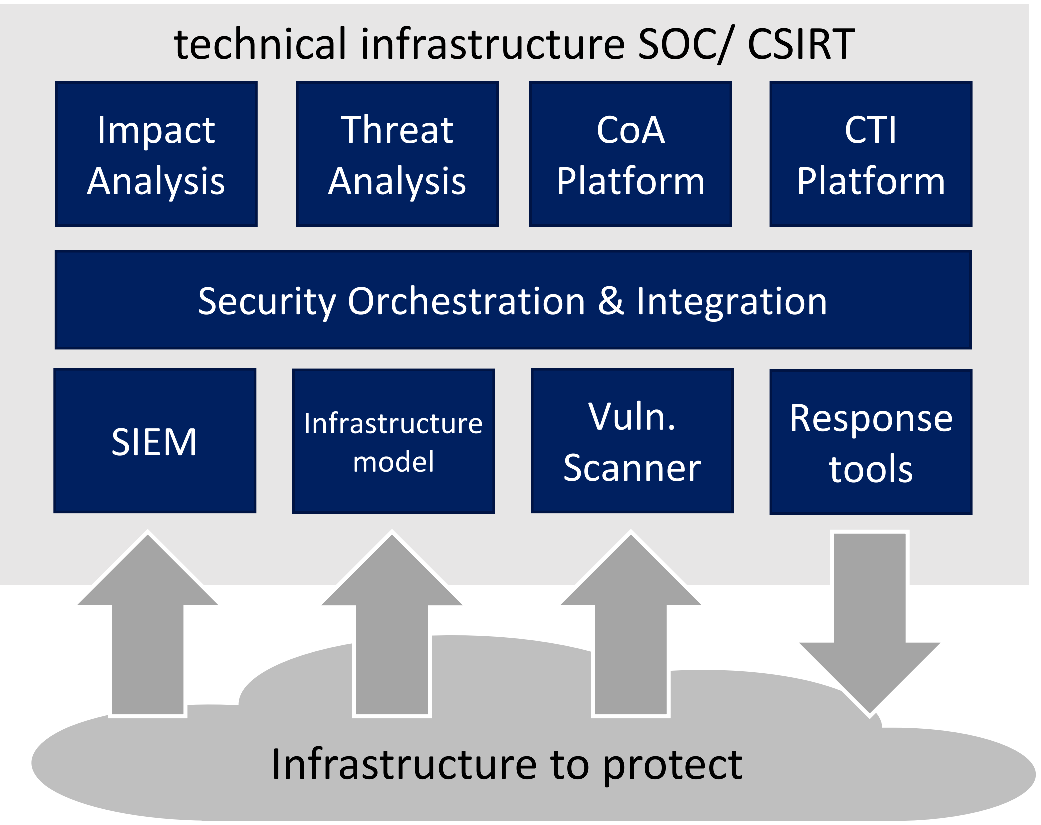
Functional Categories

- Incident Triage, Analysis, and Response
- Cyber Threat Intelligence, Hunting, and Analytics
- Vulnerability Management (if performed by the SOC)
- Expanded SOC Operations
- SOC Tools, Architecture, and Engineering
- Situational Awareness, Communications, and Training
- Leadership and Management

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

SOC / CSIRT for EPES

IT/OT Security Operation Centre Infrastructure



Incident Response Team

SOC Analyst

Cybersecurity Incident & Vulnerability Response

- Processes (workflows / roles & responsibilities
- / checklists)
- Response Actions (e.g. containment, temporary mitigate vuln.)

SOC / CSIRT process

Playbooks

Patch

Contain

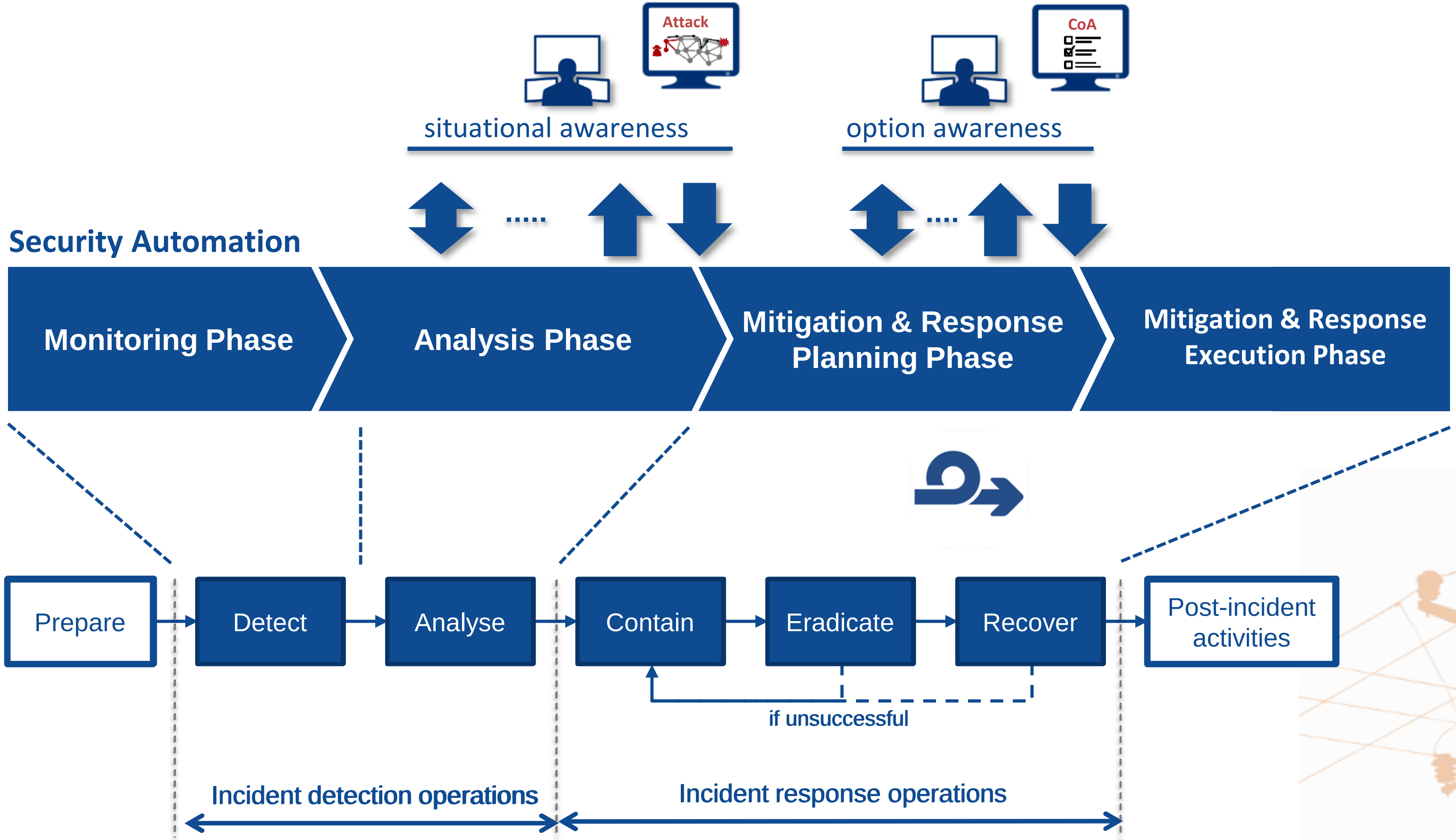
Lock account

Decoy

Disable service

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Support Incident Response with Automation



situational awareness

option awareness

Security Automation

Monitoring Phase

Analysis Phase

Mitigation & Response Planning Phase

Mitigation & Response Execution Phase

Prepare

Detect

Analyse

Contain

Eradicate

Recover

Post-incident activities

if unsuccessful

Incident detection operations

Incident response operations

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Outline

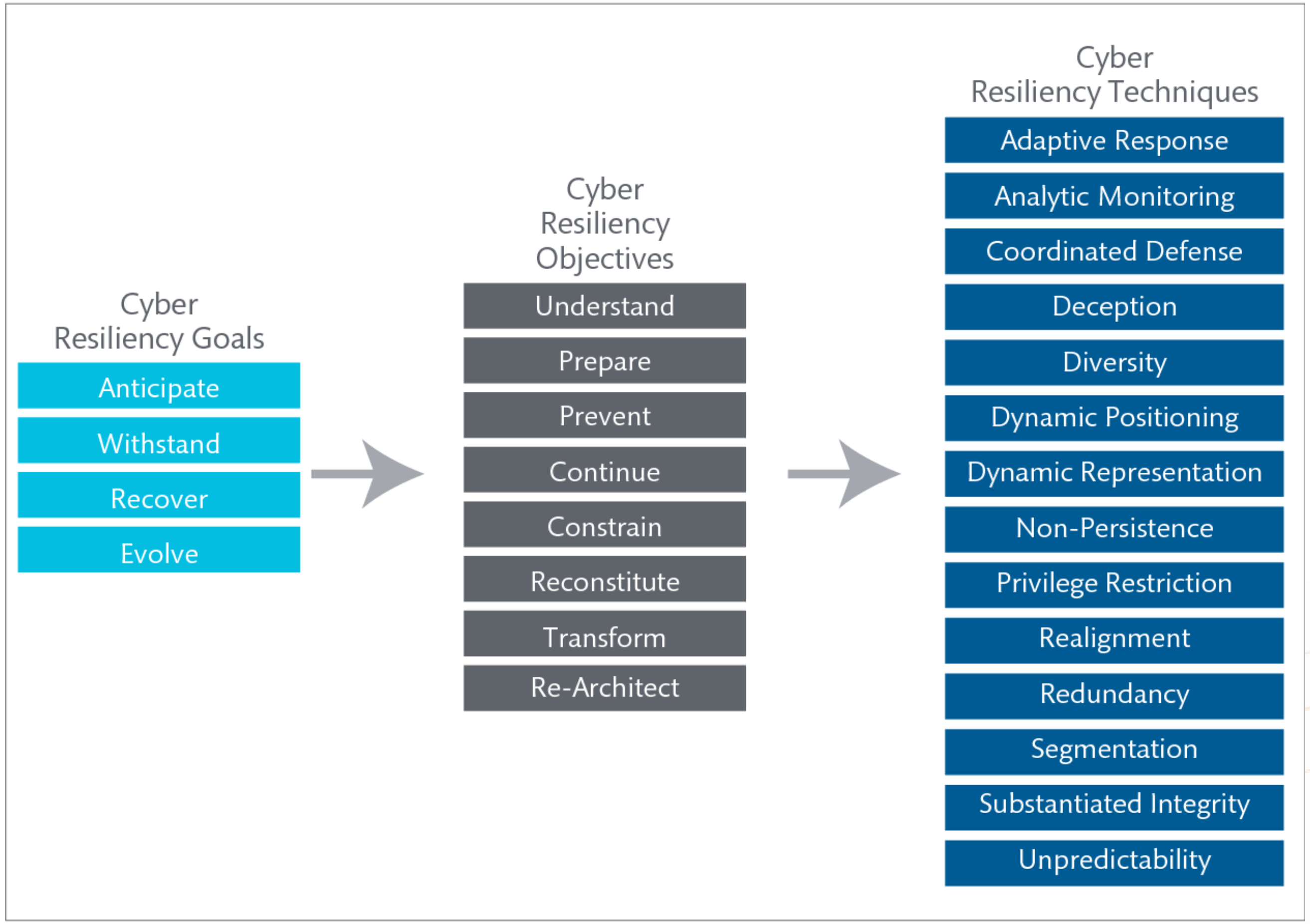
1. Introduction - eFORT
2. Incident response
3. Resilience actions

This project has received funding from the European Union’s **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

EPES Resilience / cyber resilience

the resilience of the EPES
(***main goal***:
- anticipate
- absorb
- recover
- adapt

from shocks)



Cyber Resiliency Goals

- Anticipate
- Withstand
- Recover
- Evolve

Cyber Resiliency Objectives

- Understand
- Prepare
- Prevent
- Continue
- Constrain
- Reconstitute
- Transform
- Re-Architect

Cyber Resiliency Techniques

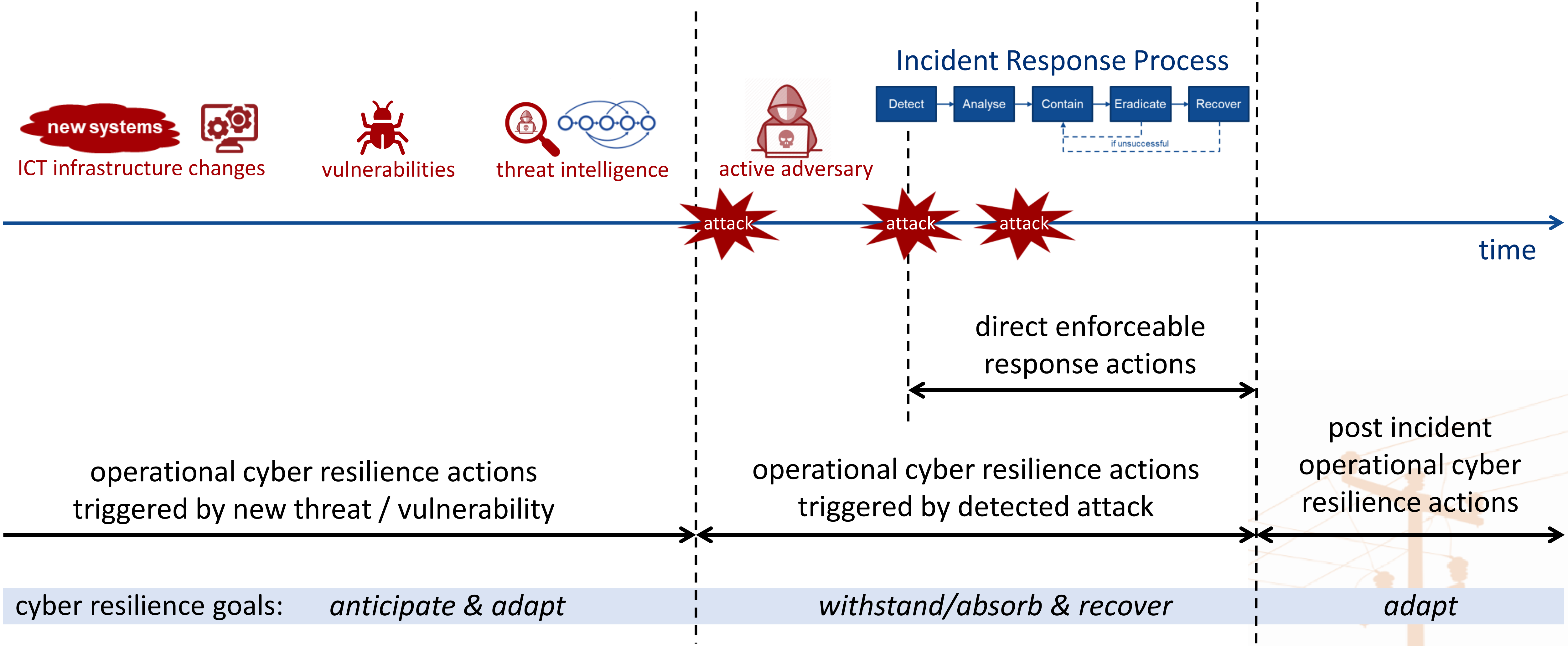
- Adaptive Response
- Analytic Monitoring
- Coordinated Defense
- Deception
- Diversity
- Dynamic Positioning
- Dynamic Representation
- Non-Persistence
- Privilege Restriction
- Realignment
- Redundancy
- Segmentation
- Substantiated Integrity
- Unpredictability

Figure 1. Cyber Resiliency Engineering Framework

NIST SP 800-160 Volume 2 (rev 1) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Operational cyber resilience actions



ICT infrastructure changes

vulnerabilities

threat intelligence

active adversary

Incident Response Process

time

direct enforceable response actions

operational cyber resilience actions triggered by new threat / vulnerability

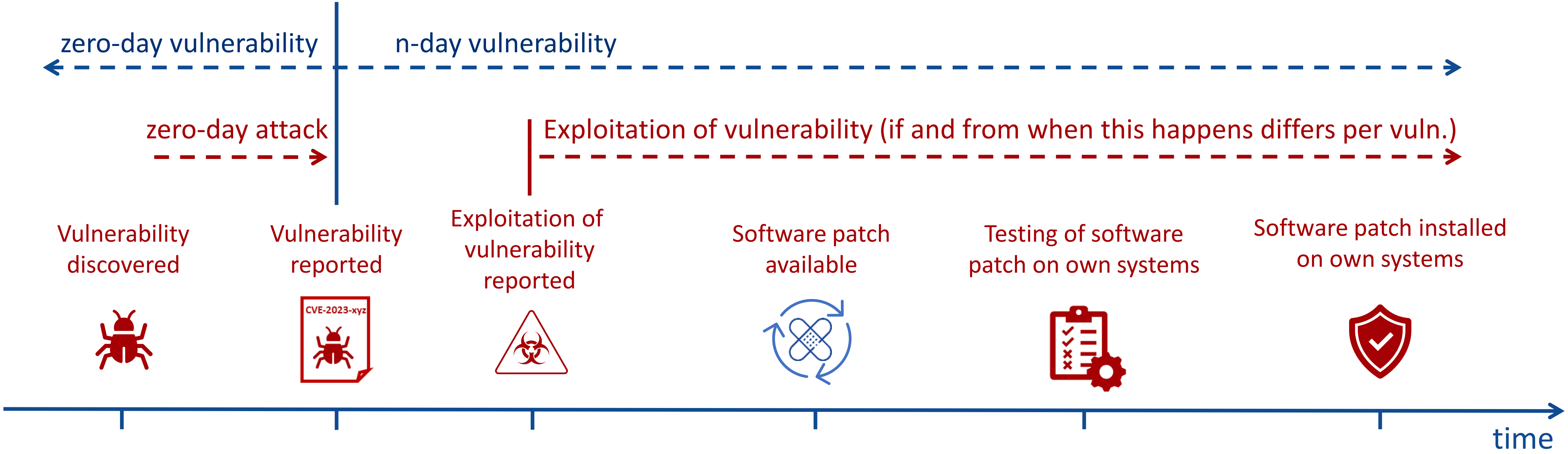
operational cyber resilience actions triggered by detected attack

post incident operational cyber resilience actions

cyber resilience goals: *anticipate & adapt* *withstand/absorb & recover* *adapt*

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Operational cyber resilience actions – new vulnerability



zero-day vulnerability

n-day vulnerability

zero-day attack

Exploitation of vulnerability (if and from when this happens differs per vuln.)

Vulnerability discovered

Vulnerability reported

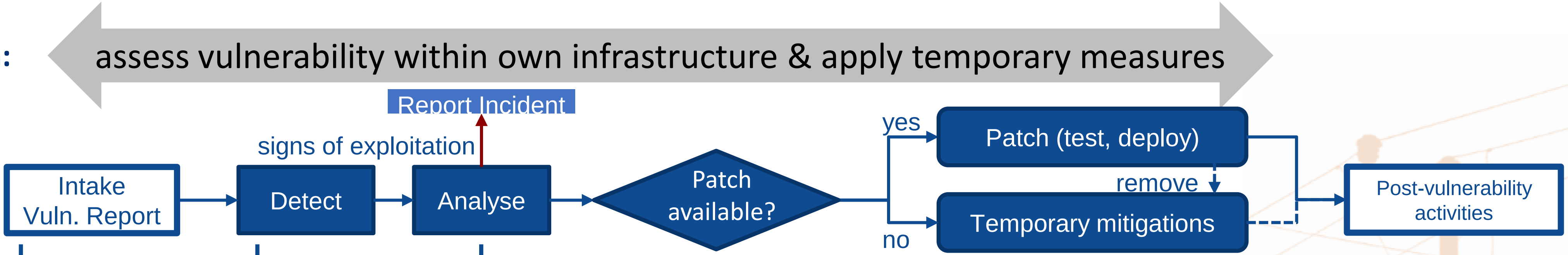
Exploitation of vulnerability reported

Software patch available

Testing of software patch on own systems

Software patch installed on own systems

EPES operator action:



assess vulnerability within own infrastructure & apply temporary measures

Vulnerability Response Process

- New vuln.
- Changes in status (exploited in the wild)

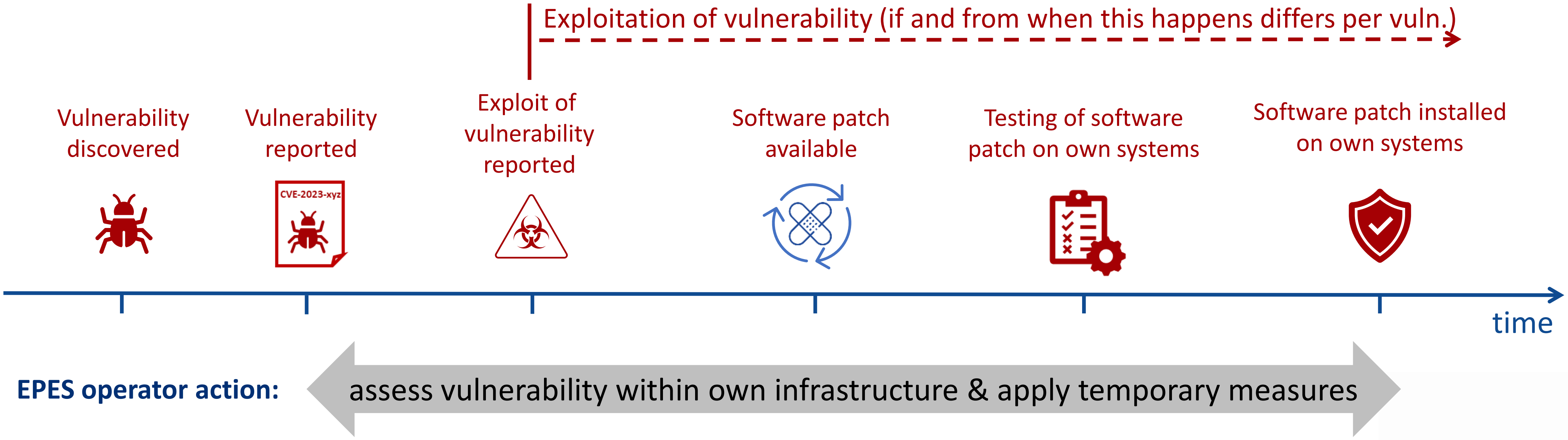
Identify vuln. assets in infrastructure

- Check for signs of exploitation
- Assess exposure
- Assess consequence of exploitation
- Prioritise

Reporting - Network Code

This project has received funding from the European Union's **Horizon** r Grant Agreement No **824388**.

Vulnerability Management



Exploitation of vulnerability (if and from when this happens differs per vuln.)

Vulnerability discovered

Vulnerability reported

Exploit of vulnerability reported

Software patch available

Testing of software patch on own systems

Software patch installed on own systems

time

EPES operator action: assess vulnerability within own infrastructure & apply temporary measures

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Summary

Main objective of the eFORT Project is…

… to make **European power grids more resilient and reliable to failures, cyberattacks, physical disturbances** and **data privacy issues**.

How?

To this end, a set of **technological innovations** will be developed for the **detection, prevention** and **mitigation** of risks and vulnerabilities with positive impacts on power system operation and stability.

The eFORT solutions will be demonstrated at **TSO, DSO, substation** and **consumer levels** in **4 real demonstration grids** that have been selected considering their complementarities and relevance to tackle the main threats of current European power systems.

This project has received funding from the European Union’s **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

References

- Cyber Security Control Frameworks (ISO/IEC 27000, IEC 62443 part 2-1, NIST SP 800-82r3)
  - In cyber security it is common to map to NIST framework: Identify, Protect, Detect, Respond, Recover
  - Cyber Resilience Engineering - NIST SP 800-160, VOLUME 2
- NIST SP 800-160 Volume 2 (rev 1) Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
- System life cycle => controls assigned to Security Operations Center
- eFORT - https://efort-project.eu/about/

This project has received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

Thank you!

Swarna Kumarswamy-Das, TNO

swarna.kumarswamy@tno.nl

- eFORT Linkedin
- eFORT Twitter
- eFORT YouTube

This project has received funding from the European Union’s **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.