Security operations in the Electrical Power and Energy System

A Concept Paper

Authors: Swarna Das, Frank Fransen, Bart Hofman, Maarten de Kruijf, Alexandru Ștefanov and Reinder Wolthuis

eFORT

TNO innovation for life

Table of contents

Executive Summary

European society is heavily dependant on Europe's Electrical Power and Energy System (EPES) for a stable electrical power supply. But the stability of the EPES is increasingly threatened by sophisticated cyber-attacks. Cybersecurity measures that are addressing both IT and OT environments are needed to protect the EPES against these attacks. But at the same time, both in the threat landscape and in cybersecurity measures, disrupting developments are ongoing due to rapid introduction of new technology such as virtualisation, AI & Agentic AI.

One of the key protections of the EPES against cyber-attacks is monitoring, detection and response, usually operated in a SOC. A SOC is becoming automation enabled, embedding autonomous actions and operations and using (agentic) AI to enhance its processes for monitoring, detection and response. Implementing a SOC in EPES operations, however, comes with challenges regarding automation, network segmentation, collaboration between SOC and OT control room and incident response in highly critical OT infrastructure.

In this vision paper we present several solutions to these challenges by introducing a playbook driven incident response approach using open source and standards based SOAR tooling, a federated SOC covering all network segments and a converged SOC concept, that introduces structured communication and collaboration between SOC and control room teams. The solutions have been partially developed, implemented and evaluated in a demonstrator[1] as part of the EU funded eFORT project.

The paper concludes with recommendations on continuous cyber defense innovation, implementing automation and a playbook driven approach in incident response, trying out new concepts, being careful with using non-deterministic AI in EPES cyber response and using digital twinning in incident response. We also present some scenarios that sketch potential future changes in cyber-attack monitoring, detection and response in EPES environments.

1 https://efort-project.eu/demo-netherlands/

1 Introduction and motivation

The digital transformation of our societies and electrification in general, has increased the dependence on stable electrical power supply enormously. Over the years the European Electrical Power and Energy System (EPES) has provided reliable power through a largely centralized model, in which energy flows from large generation plants through transmission networks to distribution grids and consumers. While this structure has supported efficiency, it now faces increasing stress from decarbonisation goals, electrification, climate risks, and sophisticated cyber threats. At the same time, we see a rapid growth of Distributed Energy Resources (DERs), such as rooftop Photo-Voltaic (PV) systems, charging stations for Electric Vehicles and battery storage facilities. These types of digitally connected systems are bringing new challenges to the existing power grid infrastructure.

The EU is therefore transitioning toward a smart and digitalised grid[2]. Smart grids integrate advanced metering, real time monitoring, substation automation, and distributed control systems. These types of digitalised grid systems support bidirectional energy flows, changes in demand flexibility, and allow for more integration of DERs. Digitalisation will, however, also increase the vulnerability of the EPES for system failures and cybersecurity threats. Cybersecurity threats are an increasing concern, given the continuous rise of cyber-attacks by financially motivated ransomware groups and state-sponsored threat actors. Furthermore, due to the recent increase in geopolitical tensions, and reported state-sponsored and ransomware cyber-attacks against power grids these concerns have intensified (see textbox List of known cybersecurity incidents targeting EPES).

List of known cybersecurity incidents targeting EPES

- 2015 — State-sponsored cyber-attack against Ukraine power grid caused regional blackout (230.000 consumers) [1], [2].
- 2016 — State-sponsored cyber-attack against Ukraine power grid caused partial blackout in capital city Kiev [3].
- 2022 — Wind turbine manufacturer Nordex and maintenance provider Deutsche Windtechnik (DWT) were hit by overlapping ransomware cyber-attacks [4], [5].
- 2023 — A coordinated cyber-attack on Danish vital infrastructure compromised 22 energy companies. Attackers used a zero-day vulnerability in Zyxell firewall. SektorCERT prevented disruption of the grid [6].
- 2023 - 2026 — Multiple German municipal electricity utilities, so called Stadtwerke, have been successfully targeted by ransomware groups impacting local utility operations [7], [8].
- 2023 — CISA released a report on the Chinese Advanced Persistent Threat (APT) group Volt Typhon. The report describes how this state sponsored APT group performed cyber-attacks on critical infrastructure, including electricity utilities in the USA [9].
- 2025 — A coordinated cyber-attack against multiple wind and solar farms in Poland did not result in power outages but did cause Operational Technology (OT) equipment in these facilities functionally inoperable [10].

2 Smart grids in EU - https://cinea.ec.europa.eu/smart-grids-eu-innovation-deployment_en

To address the increasing cybersecurity concerns with respect to critical infrastructures, and EPES in particular, the EU has issued new regulations and directives, such as the Critical Entities Resilience (CER) Directive [11], Network and Information Security 2 (NIS2) Directive [2], Cyber Resilience Act (CRA) [13], and the EU Network Code for CyberSecurity (NCCS) of cross-border electricity flow [14]. The NIS2 directive and NCCS are particularly relevant for EPES operators, as they mandate specific cybersecurity measures to be implemented by EPES operators. The NCCS for instance defines so called high-impact and critical-impact entities[3] and mandates that these entities implement cybersecurity risk-management measures, reporting of cybersecurity incidents with significant impact, and establish a CyberSecurity Operation Centre (CSOC). A CSOC is a team of experts within an organisation that provides operational cybersecurity services to the organisation. The NCCS mandates that the CSOC shall at least provide:

- log collection and security monitoring to detect anomalies and cyber-attacks;
- assessing and address vulnerabilities within network and information systems;
- analyse and respond cybersecurity incidents;
- participate in the information collection and sharing with the National CSIRT and other entities.

Over the last couple of years, many organisations have setup their own SOC in response to the increasing demand to deal with cybersecurity challenges in their enterprise IT infrastructure. Other organisations may have outsourced these operational security tasks to a Managed Security Service Provider (MSSP).

Implementing a SOC in EPES operations, however, comes with some challenges. In this vision paper we highlight the results. In section two the challenges are introduced. Section three, four and five introduce solutions that support in overcoming the challenges: playbook driven SOC automation (featuring the open-source SOAR tool developed by TNO), setting up a SOC infrastructure that aligns with the strict network segmentation principles used in OT environments, and enhanced collaboration between SOC and OT control room. The paper concludes with an overall perspective and recommendations in section six.

For the remainder of this paper, we use the term SOC instead of CSOC, as it is more commonly used in the cybersecurity industry. In the text box below, the concept of a SOC is briefly introduced.

Security Operations Centre

A Security Operations Centre (SOC) is an operational function within an organisation responsible for the continuous monitoring, detection, and analysis of cybersecurity incident analysis, and can be responsible for handling these incidents [15]. In larger organisations, SOCs focus on monitoring and detection while a separate Computer Security Incident Response Team (CSIRT) handles incident response [16]. In smaller organisations, CSIRT and SOC are integrated in one entity that handles all monitoring, detection and response functionalities. SOC teams use tooling for their automation purposes such as Security Information and Event Management (SIEM), Cyber Threat Intelligence (CTI) platforms and Security Orchestration, Automation and Response (SOAR). These tools are described in detail in Section 3. A SOC brings together several capabilities such as detection, event analysis, threat hunting, and tool lifecycle support. The SOC is both a consumer and producer of CTI, contributing to and benefiting from the ongoing exchange of cyber threat information. A SOC is becoming automation enabled, embedding autonomous actions and operations and using (agentic) AI to enhance its processes for monitoring, detection and response. However, in more OT digital infrastructures, the use of AI in security operations is still limited for autonomous actions.

3 Entities that carry out a process with respect to cross-border electricity flow and were a cybersecurity incident on such process may have impact above the high- or critical-impact threshold (NCCC art. 19(3)).

2 Challenges for SOC in Electricity grids

Implementing an effective SOC in the EPES domain is not a straightforward extension of existing IT security operations. Power system operators must balance cybersecurity requirements with the primary objective of maintaining the safe, continuous and reliable operation of the electricity grid. Unlike traditional enterprise environments, power grids consist of highly interconnected Operational Technology (OT) systems that are subject to strict operational constraints, very high continuity demands, safety requirements, and regulatory obligations. At the same time, the consequences of a successful cyber-attack can be severe, potentially resulting in large-scale outages and societal disruption. As the time between the initial compromise and physical impact on grid operations may be very short, incident response must be both rapid and effective across the cyber and physical domains. This creates several challenges for EPES operators when establishing and operating a SOC.

2.1 Challenge 1: Cybersecurity automation

The increasing scale and sophistication of cyber threats, combined with a persistent shortage of qualified cybersecurity personnel, place growing pressure on SOC operations. At the same time, the attack surface of EPES environments continues to expand as more digital technologies, and distributed energy resources are connected to the grid. During disruptive cyber-attacks, the available response window can be extremely short, leaving little time for manual investigation and decision-making. To maintain an effective level of protection, SOCs must therefore leverage automation wherever possible. Automated detection, analysis, and response capabilities can significantly reduce reaction times and improve consistency. However, given the critical nature of electricity infrastructure, automation must be applied in a controlled manner. Rapid and aggressive automated actions may be appropriate for low-risk scenarios, while actions that could directly affect power system operations should retain human oversight.

2.2 Challenge 2: Network Segmentation

EPES environments are typically designed according to the Purdue Enterprise Reference Architecture (See Figure 1) and IEC 62443 standards-based zone-and-conduit principles. These architectures deliberately segment networks and restrict communication flows to reduce the likelihood that failures or cyber-attacks propagate between systems. While segmentation is an essential security measure, it also complicates the collection of security data, centralised monitoring, and incident response activities. A SOC must therefore be able to obtain sufficient visibility into OT environments without violating the architectural principles that underpin the security and reliability of the grid. As a result, cybersecurity monitoring solutions must be designed to support and strengthen the existing segmentation model rather than bypass it.

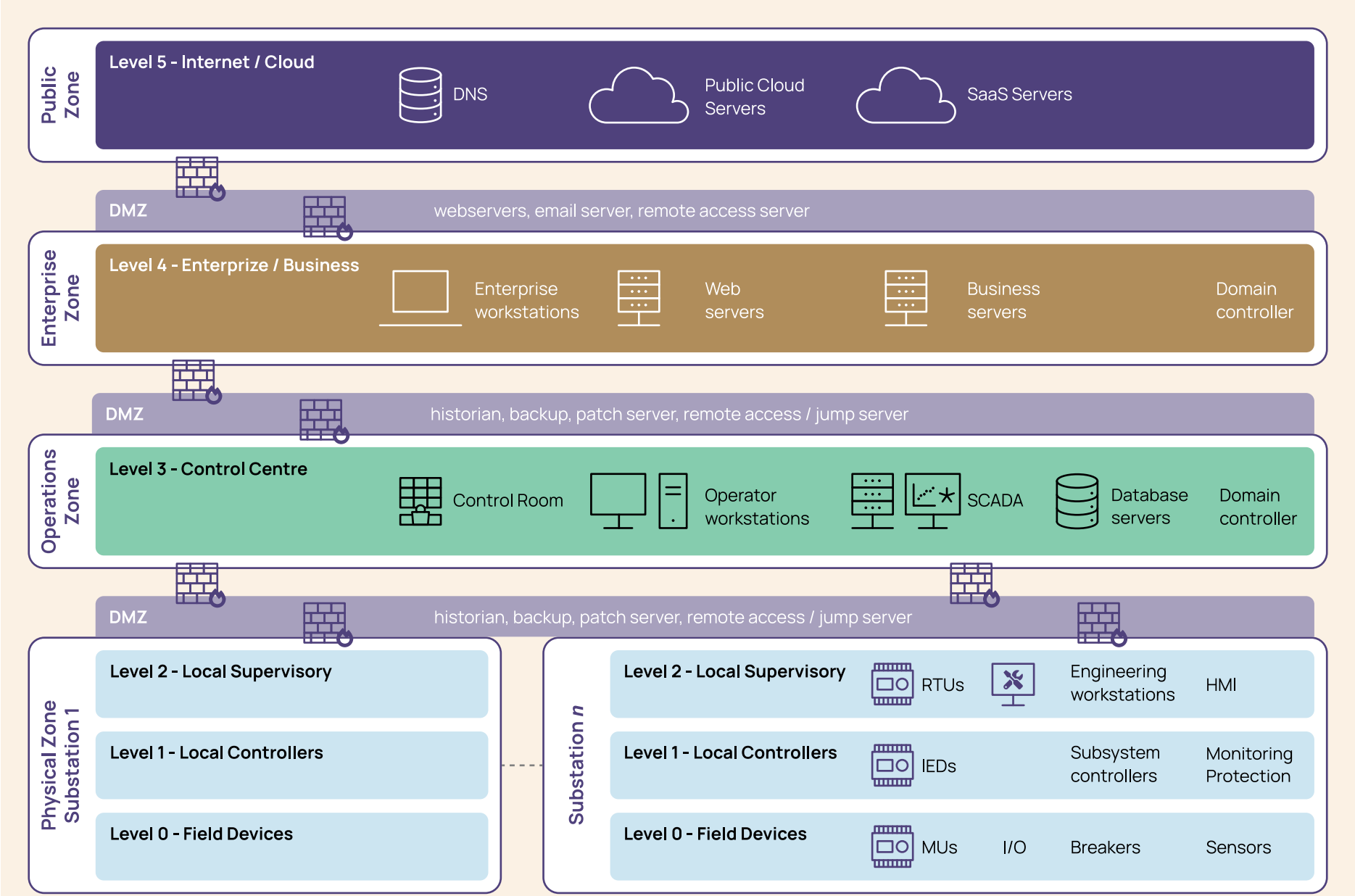

Figure 1: Visual of Purdue Enterprise Reference Architecture

2.3 Challenge 3: Collaboration between the Control Room and the SOC

Effective response to cyber incidents in EPES requires close collaboration between the Control Room and the SOC. While the SOC is responsible for detecting, analysing, and responding to cyber threats, Control Room operators are responsible for maintaining the physical operation and stability of the power grid. Consequently, cyber incidents cannot be assessed solely from a cybersecurity perspective; their potential impact on grid operations must also be considered. This is particularly relevant in the context of regulatory requirements such as NCCS incident reporting obligations, where the operational impact of an incident may determine reporting thresholds and response priorities. However, Control Room and SOC personnel often operate in different organisational cultures and possess different expertise, terminology, and objectives. Establishing effective communication processes, shared situational awareness, and coordinated decision-making is therefore a key challenge.

2.4 Challenge 4: Incident Response in OT

Responding to cyber incidents in IT environments often involves automated actions such as isolating systems, blocking communications, or reconfiguring network components. In OT environments, however, such actions may have unintended consequences for power system operations. A cybersecurity response that disrupts communications or removes access to critical systems may reduce the ability of Control Room operators to monitor, control, or recover grid assets. As a result, response actions in OT environments require careful consideration of both cybersecurity and operational risks. This creates a need for clearly defined response playbooks, governance structures, and pre-authorisation mechanisms that specify which actions may be executed automatically and which require human approval.

2.5 Addressing the challenges

Addressing these challenges requires a converged approach to security operations that integrates cybersecurity expertise with operational power system knowledge. Such a model should support independent operation of the SOC on all levels of the Purdue model while enabling close collaboration with Control Room personnel during incidents. Furthermore, it should employ automation to achieve the speed necessary to counter modern cyber threats, whilst ensuring that human operators remain involved whenever actions may affect critical grid functions. Finally, any solution must operate within the constraints imposed by OT architectures, supporting rather than compromising existing segmentation principles. In this context, the challenge is not only to detect cyber-attacks, but to coordinate timely and effective response actions across both the cyber and physical domains while maintaining the safe and reliable operation of the electricity grid.

3 Playbook driven SOC Automation

As described in challenge 1 in the previous section, SOCs must leverage automation wherever possible, while taking into account the critical nature of electricity infrastructure. A playbook driven automation approach provides pre-defined plans while having guardrails in place (such as authorisation checks and manual approvals). This section explains the playbook driven approach and how it can be applied in the EPES environment.

3.1 What is playbook driven SOC Automation?

Security operations playbooks specifically are designed to support incident handlers and execute simple and repetitive steps automatically in the incident handling process. Playbooks are security-event-driven, which means that playbooks are triggered to address a particular security event, such as trigger incident response after detection of a cyber-attack, trigger threat hunting after receiving new CTI, trigger vulnerability assessment after receiving a security advisory warning of a new vulnerability in software. When they first emerged, they were executed manually by security analysts, but with the introduction of Security Orchestration, Automation and Response (SOAR) tooling, security playbooks became automated. Playbooks steps can now include fully automated interactions with other security tools, analysis of results, and presenting the results to a human security analyst and ask for a decision on how to proceed (human in the loop). Automated playbooks can be triggered manually by the security analyst or by other security tools like a SIEM or CTI platform (see textbox Traditional SOC tools).

A SOAR playbook contains a collection of clear repeatable step-by-step actions and roles & responsibilities that outline a standardized process to support incident detection and response. A single playbook usually can handle a specific attack or specific process(step) in the incident handling process, e.g. a playbook to a handle a phishing incident. Therefore, a typical SOC will have many playbooks for many different situations. Playbooks can contain either machine-readable steps or documented checklists and decision points or both. Playbooks can be expressed in a myriad of different ways, such as wiki pages, Business Process Model and Notation (BPMN) diagrams, vendor-specific machine formats. Each format may be structured in different degrees, if at all, and each format can be highly environment specific.

Traditional SOC tools

SIEM

A Security Information and Event Management (SIEM) system is one of the main components in modern cybersecurity tooling, as referenced from the National Institute of Standards and Technology (NIST) [17]. A SIEM integrates Security Information Management (SIM) and Security Event Management (SEM) functions to provide real-time analysis of security alerts generated by network applications. Its primary function is to aggregate and analyse log data and other security related information from various sources within an organisation's digital infrastructure. By correlating data, a SIEM system can detect patterns, anomalies, and (potential) cybersecurity incidents that might indicate malicious activities or breaches. This enables security analysts to respond to threats, ensuring the Confidentiality, Integrity and Availability (CIA) triad of an organisation's assets. A SIEM system supports compliance with regulatory requirements by providing detailed logging and reports. A SIEM facilitates incident response by integrations with SOC operations and other cybersecurity tooling.

CTI platform

CTI refers to the collection, analysis, and dissemination of information about current and potential cyber threats, threat actors, and their tactics, techniques, and procedures (TTPs). The primary goal of CTI is to provide actionable insights that enable organizations to proactively defend against cyber threats, enhance their security posture, and make informed decisions. By using CTI, analysts can better understand the threat landscape, identify potential vulnerabilities, and implement effective countermeasures. CTI sources can include open-source intelligence (OSINT), commercial threat intelligence feeds, information sharing and analysis centres (ISACs), and internal security data. In OT environments CTI plays an important role in enhancing and enriching information from systems that monitor and control physical processes.

3.2 SOAR

A SOAR supports a SOC by orchestrating several security tools, automating repetitive and time critical tasks, and importantly coordinating incident response workflows. ENISA [15] describes a SOAR as an enabler that integrates people, processes and technologies by connecting several different security tools, enriching alerts with necessary contextual information, and executing predefined or dynamically generated response actions through playbooks. The primary purpose of a SOAR, is to reduce response time, improve operational consistency and limit human error. This allows SOC analysts to focus on analytical and decision making tasks, while maintaining human-in-the-loop for critical actions. Especially in OT environments, where (physical) safety is an important consideration, this is very important. A SOAR does not intend to replace human operators or incident response teams, but aids and integrates SOC operations by supporting automatable, scalable and auditable security operations, especially in complex (IT and OT) digital environments which are facing increased alert volumes, cybersecurity skills shortages, and ever increasing cyberattacks.

The market for SOAR solutions has matured significantly over the past years, and present-day products support sophisticated automation workflows and a wide array of integrations with external security tools and data resources. Widely used products like Cortex XSOAR from Palo Alto Networks, Swimlane Turbine and Splunk SOAR (now part of Cisco), use their own proprietary security playbook formats which limits sharing of playbooks between organisation and by national CSIRTs.

To overcome this, the Organization for the Advancement of Structured Information Standards (OASIS) Open has developed a standard for describing cybersecurity playbooks called the Collaborative Automated Course of Action Operation (CACAO).

3.3 CACAO playbooks

The CACAO specification from OASIS Open[4] was developed to standardise and describe security operations [18]. CACAO introduces a format for cybersecurity operational playbooks with several benefits:

- It provides an interoperable, vendor-neutral language for cybersecurity operations, making it understandable across different tools and teams using these.
- The language supports defining playbooks at various levels of abstractions and details, from broad strategic planning to specific technical steps, and allows for assembling these different components.
- Since the language is serialised in a machine-readable format, security operations outlined in CACAO playbooks can be executed automatically as designed.
- It also facilitates the secure sharing and validation of security operation techniques between different organisations and CERTs.

A feature of CACAO playbook is its capacity to issue a wide array of commands to infrastructure, either automatically or with required human operator approvals. It collects data in variables, and applies conditional logic throughout the various steps of any playbook.

A CACAO playbook being used by a SOAR, demonstrating the capabilities of executing steps and control logic is shown in Figure 2.

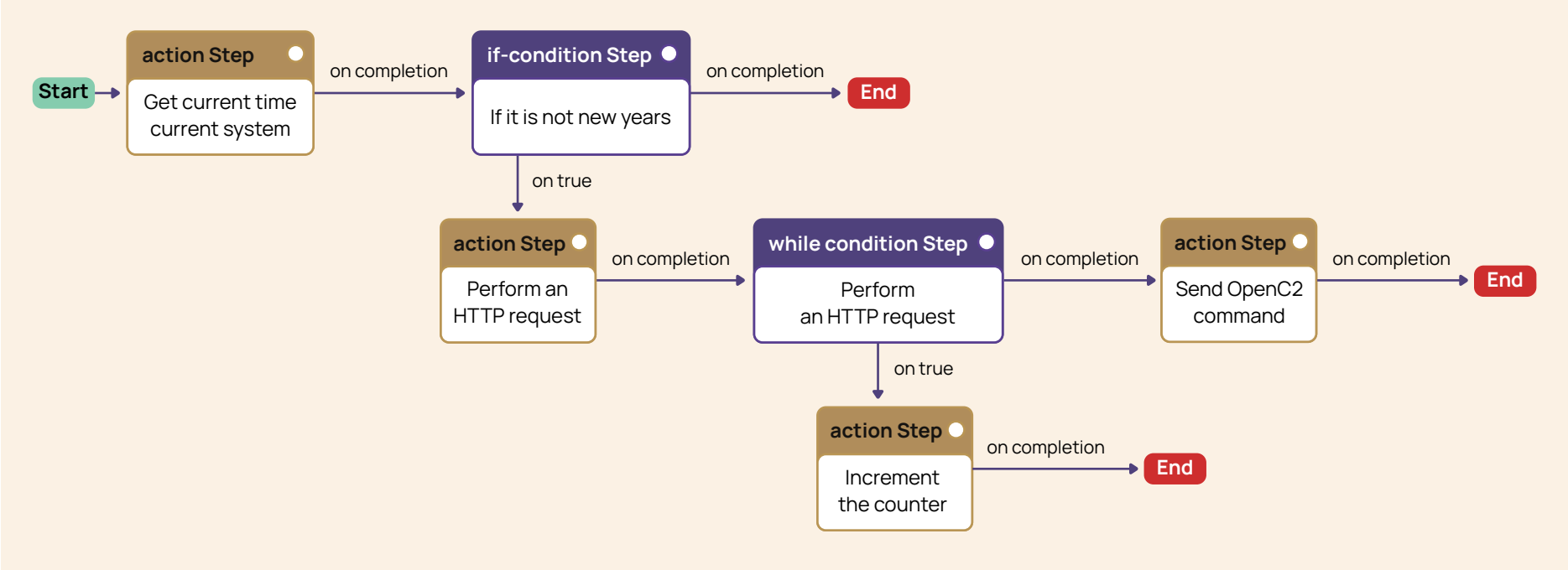

Figure 2: CACAO playbook in use by a SOAR

4 https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cacao

To facilitate the creation and inspection of CACAO playbooks, several tools have been developed for graphical editing and visualization. Examples include the open-source CACAO Roaster[5] from the Open Cybersecurity Alliance initiative[6] and the Cymph playbook management platform[7]. TNO has developed SOARCA, an open-source SOAR platform that supports the execution of CACAO v2.0 playbooks. SOARCA is discussed in more detail in the following section.

3.4 SOARCA

Most current SOAR technologies are proprietary and not easily adaptable for research and experimentation purposes. To overcome these limitations, TNO developed SOARCA as an open-source alternative SOAR solution that is free of vendor dependencies and supports standardized formats and technologies where applicable. SOARCA offers native support for the execution of CACAOv2 playbooks. SOARCA also supports OpenC2, an OASIS Open standardized language for the command and control of cyber defence technologies. In essence OpenC2 provides a vendor agnostic language and interface through which so called security actuators (e.g. firewalls or IAM solutions) can be reconfigured automatically.

SOARCA is available under the Apache 2.0 license from the Community for Open-Source Security Automation Software (COSSAS),[8] and via Github including documentation.[9] A conceptual overview of SOARCA is depicted in Figure 3. The use of open-source SOAR tooling like SOARCA, is not only relevant for automation, but also for complex orchestration workflows, attack and defence simulations and other cybersecurity functionalities.

3.5 SOC automation in EPES

The SOC automation focuses on enhancing situational and option awareness for cybersecurity analysts in the Security Operations Centre (SOC) of EPES organisations. This enables operators to make informed decisions regarding (incident response) actions to possible cyber threats and in cases of cyberattacks with greater accuracy and speed, while maintaining human-in-the-loop for critical infrastructure such as power grids. Additionally, the playbook driver-automation facilitates response actions, whether these are pre-authorised or done in real-time by operators. This ensures that control room operators are notified of any cybersecurity concerns which may hinder their operational control resulting from cyber incidents or mitigation actions.

These objectives are achieved through playbook-driven cybersecurity automation and integration with an incident case management system, enabling a coordinated execution of both human-in-the-loop and completely automated tasks. This type of automation uses SOAR tools to systematically manage these processes, such as TNO's open-source SOARCA. In section 5, the challenges of SOC automation in EPES are further addressed.

5 https://github.com/opencybersecurityalliance/cacao-roaster
6 https://opencybersecurityalliance.org
7 https://www.cymph.io
8 https://cossas-project.org/portfolio/SOARCA/
9 https://cossas.github.io/SOARCA/docs/

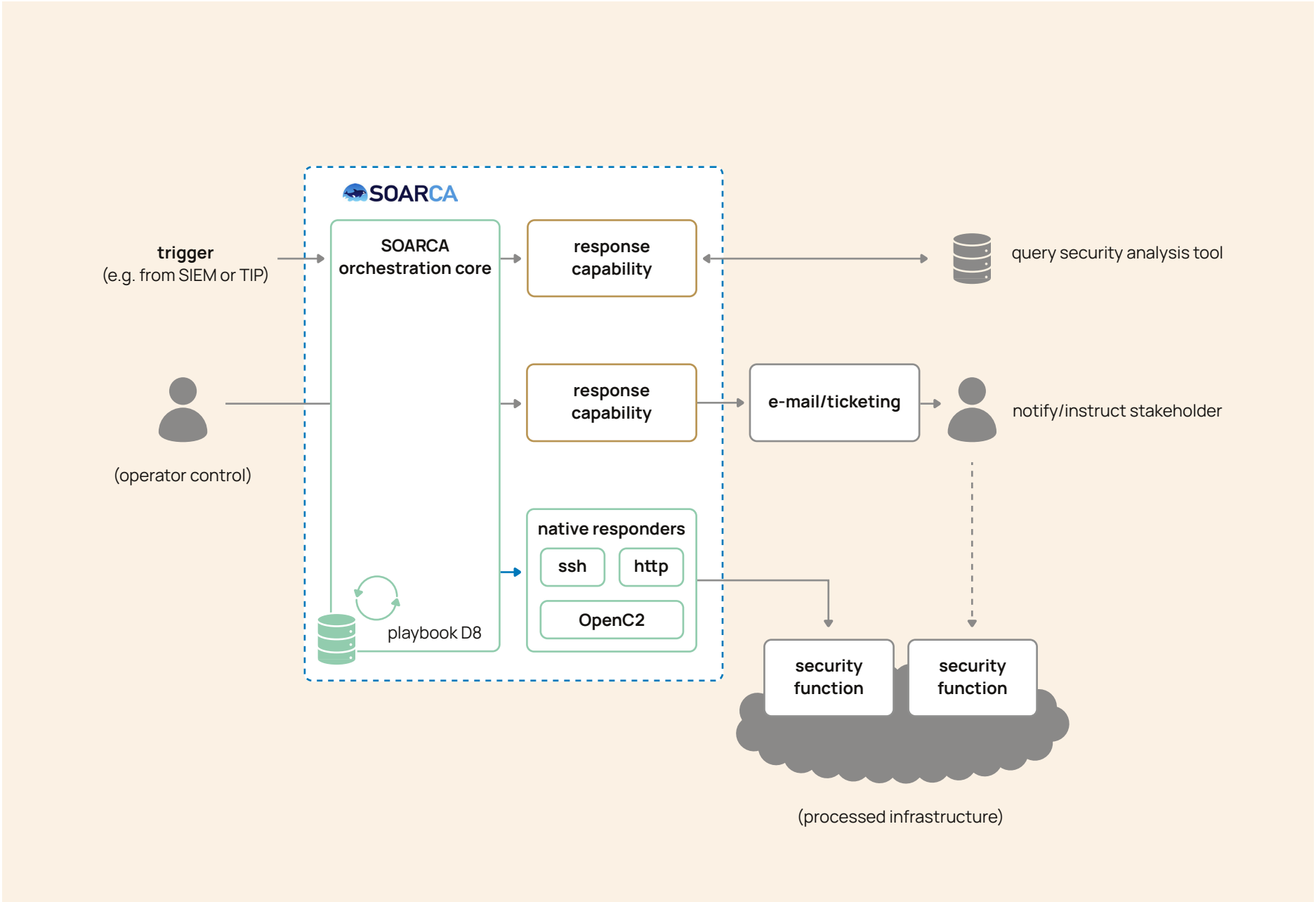

Figure 3: SOARCA with its core components

4 Network Segmentation & Cybersecurity Operations

Challenge 2, described in section 2.2, describes the complications related to network segmentation and cybersecurity operations. It specifies: A SOC must therefore be able to obtain sufficient visibility into OT environments without violating the architectural principles that underpin the security and reliability of the grid. The following paragraphs address the concept of segmentation related to the IEC standards, the Purdue model and the ETF SEI reference architecture.

4.1 Purdue Model & IEC 62443-3-2 Zone-Conduit model

The Purdue model for control systems architecture, also known as the Purdue Enterprise Reference Architecture (PERA), which is a framework applied to Operational Technology (OT) environments to help with the design and implementation of regular operations which includes cybersecurity of critical infrastructure [19]. In the context of EPES, this model helps to structure and segment complex environments such as substations, control centres, and field devices into hierarchical layers. This makes a clear separation between operational layers thereby enhancing security, safety and reliability. The Purdue model approach ensures that networked devices such as SCADA systems, remote terminal units (RTUs), programmable logic controllers (PLCs), and intelligent electronic devices (IEDs), are organised in a manner which supports secure communication in separate layers and its operations. These operational layers then are used in cybersecurity for example during incident response, digital forensics and so forth. For grid operators, this model is valuable in industrial control system (ICS) and SCADA contexts, as it helps to manage the flow of information and control signals between field assets and central monitoring systems. By defining clear boundaries and interfaces between process control, supervisory control, and site operations, the Purdue model supports the resilience and cybersecurity of the power grid against emerging threats while maintaining operational efficiency.

4.1.1 Overview of the Purdue Model

The Purdue model is organised into several levels, each representing different layers of the control system hierarchy, see Figure 1. These levels are designed to help the flow of information and control signals while maintaining a clear separation of operational domains. The model is divided into six main levels:

Level 0: Process

This level represents the physical processes being controlled, such as manufacturing equipment, sensors, and actuators. It includes the actual machinery and physical components that perform the operational tasks.

Level 1: Intelligent Devices

This level consists of intelligent field devices, such as programmable logic controllers (PLCs), remote terminal units (RTUs), and other field instruments. These devices collect data from the process and execute control algorithms.

Level 2: Supervisory Control

This level includes supervisory control and data acquisition (SCADA) systems, human-machine interfaces (HMIs), and other supervisory control systems. It monitors and controls the field devices and provides a higher-level view of the process.

Level 3: Site Operations

This level encompasses site-level operations, including manufacturing execution systems (MES), production management systems, and other operational management tools. It focuses on optimizing production processes and ensuring operational efficiency.

Level 4: Site Business Planning and Logistics

This level involves business planning, logistics, and enterprise resource planning (ERP) systems. It integrates operational data with business processes to support decision-making and strategic planning.

Level 5: Enterprise Resource Planning

This level includes enterprise-wide systems, such as ERP, supply chain management (SCM), and customer relationship management (CRM) systems. It supports high-level business operations and strategic decision-making.

While the Purdue model uses clear functional layering, it does not inherently provide segmentation in the level or zone. Moreover, it is a mapping of functions, not a set of trust boundaries. Two devices can sit on the same Purdue level and have nothing to do with each other, yet the model treats the level as one flat space. Nothing in Purdue stops a compromised Human Machine Interface (HMI) on Level 2 from reaching every PLC on Level 1. The IEC 62443-3-2 defines zones and conduits for this purpose [20].

4.1.2 Zones and conduits: adding segmentation to the Purdue model

The IEC 62443-3-2 defines a process for splitting a system into zones and conduits based on risk rather than function alone. Zones and conduits are defined in IEC 62443-3-2 as follows: a Zone is a group of assets with the same security requirement, and a conduit is a controlled pathway between zones. These ideas are complementary to Purdue model. Purdue tells you roughly where a device lives, and IEC 62443-3-2 tells you which devices should be allowed to trust and reach each other.

So, if we combine them, we get a fine-grained network of devices that only can communicate if needed. This fine-grained control allows us to introduce a security zone in the different levels of the Purdue model. Each Purdue level can hold several zones, and conduits can run inside or across levels. The demilitarized zone (DMZ) between the control network (Level 3) and the enterprise (Level 4) is the classic example of that. It's a zone dedicated to brokering traffic, reachable only through conduits on either side, so IT and OT are never connected directly.

4.1.3 A reference design for EPES: the SEI ETF architecture

The model stays abstract until it's mapped onto real equipment, and for electric power the clearest mapping is the SEI ETF Reference Architecture for Electric Energy OT [21]. It takes the Purdue levels, fills them with grid-specific devices, and groups them into named security zones. Most grid operators recognise this design, which makes it a sensible baseline we build on rather than starting from a blank hierarchy. The mapping of devices and services to Purdue levels in Figure 1, is based on the SEI ETF Reference Architecture for Electric Energy OT.

The reference architecture maps the six Purdue levels into four tiers. The tiers don't touch directly. Each crossing between them runs through a DMZ that brokers the traffic allowed to pass, usually a historian replica, a patch server, and a remote-access or jump server. Those DMZs are the conduits. They're the only sanctioned routes between zones and the place where inter-zone traffic gets inspected and filtered. An operator query for a measurement, a patch pushed down to a substation, a historian feeding business reporting: each has a defined path, and anything without one doesn't cross.

Zones also sit side by side within a single level. Two substations at Level 1 that never need to exchange data are separate zones on the same tier, with no conduit between them, so a fault or a compromise in one can't reach the other.

4.2 Collaborative Converged Local Control SOC Architecture

Putting a SOC inside a highly segmented OT environment creates tension with the zone-and-conduit model that must be resolved. A SOC needs to see into all the zones to be useful, but a monitoring plane that reaches into every zone is itself a path an attacker can ride from IT down to the field. Solve the visibility problem carelessly and you've built the next cross-level pathway out of your own security tooling.

The Collaborative Converged Local Control SOC Architecture (CCLCSA) answers this by applying to the SOC the same segmentation the reference design applies to the process network [22]. Instead of one SOC that spans

levels, the CCLCSA uses federated SOC enclaves, each aligned to a zone and each operating horizontally within it. An enclave watches its own zone and does not reach vertically into the zones above or below. Responsibilities in a grid already fall this way: the control centre owns Level 3 and the site owns Levels 0 to 2, so a SOC that mirrors that split fits how operators already work. For a large substation with staff on site, an enclave can sit at the substation itself.

Each enclave is self-contained. It carries its own detection and response tooling and keeps working when its zone is cut off from the rest of the network. That matters for the Ukraine scenario, where operators islanded the OT from IT and the internet to regain control. A single central SOC loses visibility the moment that happens. A SOC built as enclaves keeps monitoring the islanded zone from inside it.

The enclaves are tied together the same way the process zones are, through conduits. A converged SOC enclave sits above the others but does not connect directly into the organisation's infrastructure. It reaches the individual enclaves only across DMZs, receiving their alerts and querying their data through what amounts to a historian replica rather than a live link into the zone. The security tooling obeys the same rule as everything else on the network: it crosses a zone boundary only through a conduit, never through a back door opened for convenience.

Response follows the same discipline. Each enclave runs its own SOAR and has control over the response playbooks that stays local to the enclave. A playbook that can act on a substation is a physical-safety concern and not only a cybersecurity one. The central SOC can trigger an enclave's automation but cannot rewrite or override its playbooks. Actions that touch critical cyber-physical components are held behind a human in the loop, so a control-room operator authorises anything that could move a breaker before it runs.

The result is a SOC that inherits the grid's own zone-and-conduit structure, see Figure 4. It sees each zone from within, crosses boundaries only through conduits that can be watched and closed, and hands the riskiest decisions to the people responsible for keeping the lights on. The monitoring meant to catch an attacker never becomes the route the attacker takes.

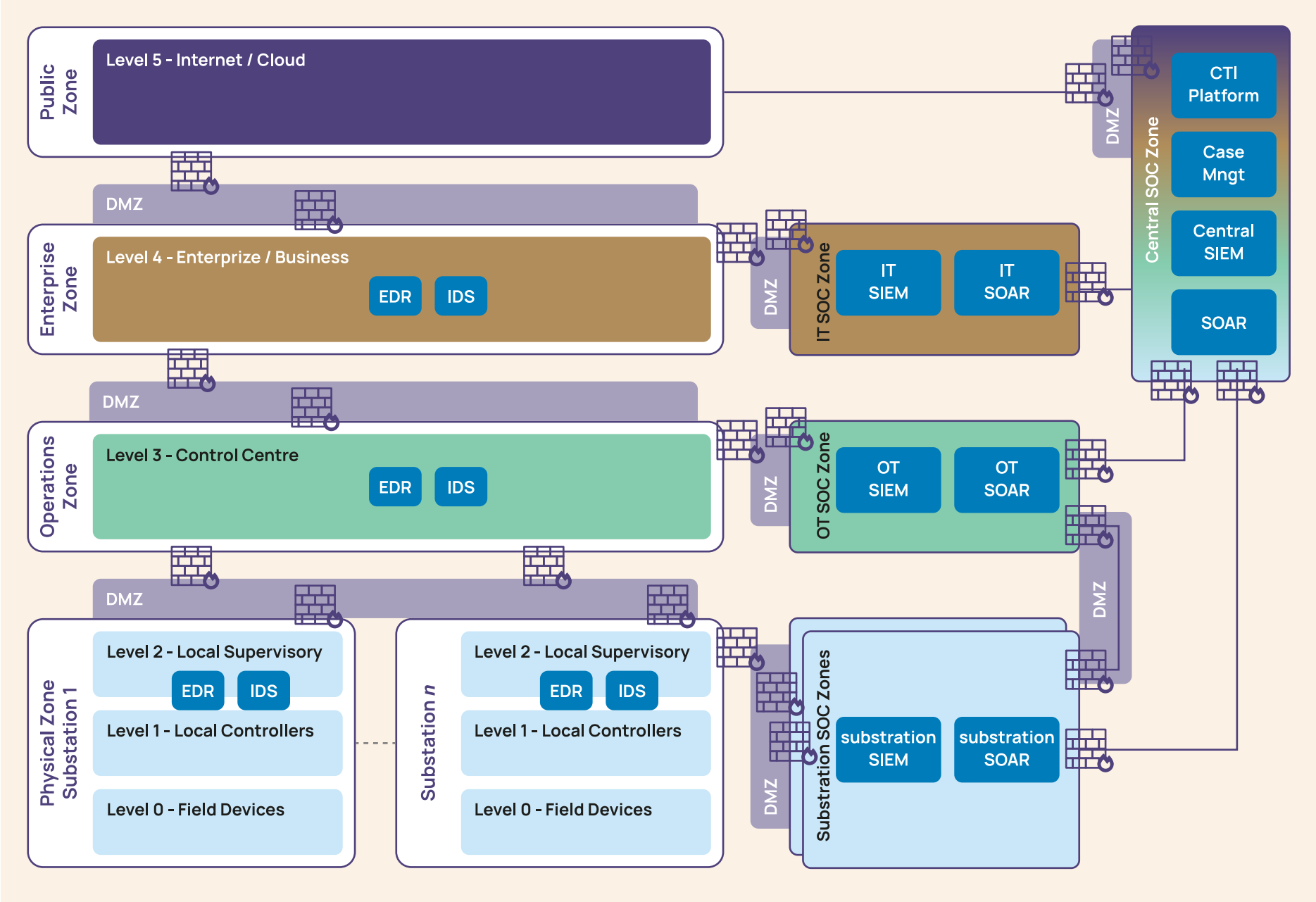

Figure 4. Collaborative Converged Local Control SOC Architecture is depicted on the right of Purdue Reference Architecture

5 Control Room – SOC collaboration

The increasing digitalisation of EPES environments requires closer collaboration between Control Room operators and SOC-personnel. Traditionally, these functions have operated largely independently. Control Room operators focus on maintaining the safe and stable operation of the power grid, while SOC personnel focus on detecting, analysing, and responding to cyber threats. However, modern attacks against power grids increasingly cross the boundary between cyber and physical systems. A cyber incident may rapidly develop into an operational incident affecting substations, DERs, grid stability, or the continuity of electricity supply. As a result, effective cyber resilience requires coordinated decision-making across both domains.

A key challenge is that Control Room operators and SOC analysts often work with different tools, terminology, priorities, and success criteria. Security personnel assess indicators of compromise, attacker behaviour, and network activity, whereas Control Room operators assess operational conditions such as grid stability, breaker states, load, and system availability. For effective incident response, both groups must establish a shared understanding of the situation and its potential consequences. The converged SOC concept therefore introduces structured communication between both teams, enabling cybersecurity findings to be translated into operational risk and operational observations to be incorporated into the cyber response process.

To support the reporting of cybersecurity incidents mandated by the Network Code for CyberSecurity (NCCS), a framework for assessing cybersecurity incidents was introduced by ENTSO-e[10] and DSO Entity[11]. It defines a scale for the gravity of a cyber-attack and for the severity of a cyber-attack (potential impact on electricity operations). This enables cybersecurity events detected by the SOC to be evaluated in the context of grid operations and provides a common language for coordinated decision-making between both parties. The decision matrix that decides if an incident is a cyber-attack can be seen in Figure 5.

The objective of the collaboration is to move from reactive response to proactive mitigation. Many attacks against power systems follow a multi-stage attack path, where attackers first compromise IT systems before moving towards OT assets and eventually affecting physical processes. This progression creates opportunities to detect and disrupt attacks before operational impact occurs.

The SOC continuously monitors both IT and OT environments for indicators of malicious activity. Early warning signals may include compromised workstations, abnormal authentication behaviour, unusual network communications, or unauthorised access attempts towards engineering or operational systems. These indicators are analysed by the SOC and correlated with information from OT monitoring systems. When sufficient evidence exists that an attack may affect power system operations, the Control Room is informed and operational impact assessments using a digital twin is initiated (See the textbox on Digital Twins in EPES for further information).

10 ENTSO-E, the European Network of Transmission System Operators for Electricity; https://www.entsoe.eu/
11 DSO Entity is the association for Distribution System Operators (DSOs) in Europe; https://eudsoentity.eu/

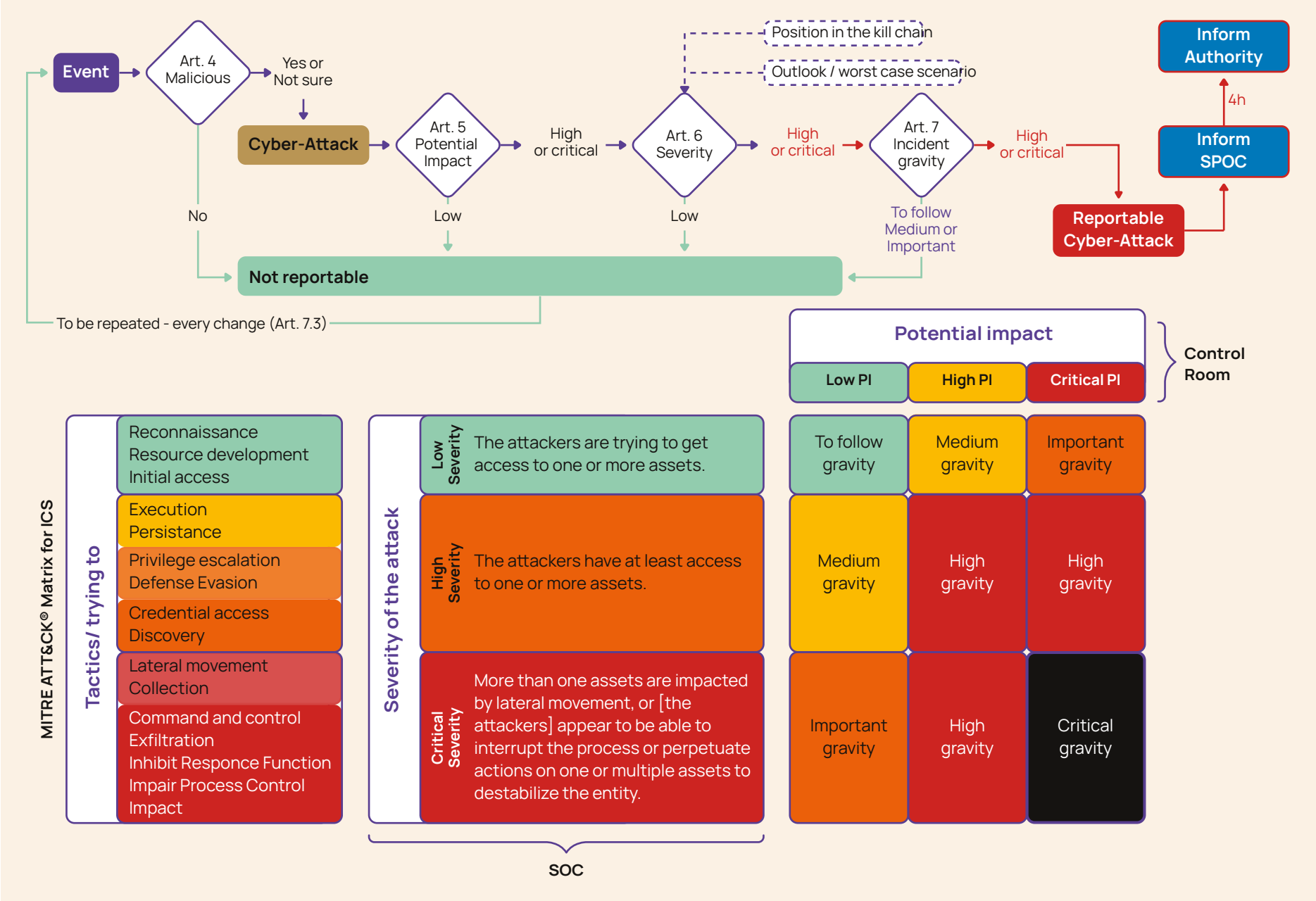

Figure 5. Proposed NCCS process for reporting cybersecurity incident with the cyber-attack classification scale methodology [26].

Digital Twins in EPES

In recent years we have seen an increase in adoption of digital twin technology for dealing with the complexity of the transition to renewable energy and the dynamic nature of modern power grids. A Digital Twin is a digital representation of a physical system, asset, process, or environment that is kept aligned with the real-world counterpart. Such digital twin can be used to do simulation for analysis, prediction, optimisation, etc. A digital twin of an electricity grid can be used to perform simulations to provide essential information to operators on how to keep the grid stable.

As an example, TU Delft has worked on using a digital twin to investigate the consequence of a cyber-attack on the electricity grid [23]. In particularly, what are the cascading failures of a potential compromise of a substation [24]. In the EU funded eFORT project, this was further improved and extended with a digital twin-based analysis on how to best isolate (a potentially compromised) substation from the rest of the grid to reduce cascading failures [25]. This enables a grid operator to identify potential preventative measures on the physical layer in response to a cyber-attack on a substation.

This process allows potential physical consequences to be evaluated before damage occurs. For example, a compromise of an engineering workstation may directly increase the likelihood of unauthorised control actions towards substations or protection systems. Although no physical impact may yet be visible, the Control Room can already assess possible consequences and prepare operational measures to maintain system stability if the attack progresses further.

Given the critical nature of power systems, response actions cannot be improvised during an incident. Countermeasures must therefore be developed, validated, and agreed upon in advance through jointly developed response playbooks. These playbooks define both cybersecurity actions and operational decision points, ensuring that response measures are safe, repeatable, and aligned with operational requirements.

The proposed architecture distinguishes between three categories of response actions:

1. Information gathering and enrichment actions.
2. Automated actions affecting non-critical IT or OT assets.
3. Actions affecting critical operational systems or communications.

The first two categories can often be executed automatically by the SOC. The third category requires explicit involvement of Control Room personnel because these actions may influence visibility, control capabilities, or operational safety. Examples include isolation of Human-Machine Interfaces (HMIs), modification of communications with substations, or actions affecting protection and control systems. In these situations, a Human-in-the-Loop (HITL) approval mechanism is required before execution.

To reduce response delays during fast-moving incidents, organisations may also establish pre-authorised response actions. These are agreed upon beforehand between the Control Room and SOC and may be executed automatically when predefined conditions are met. The SOC notifies the Control Room when such actions are triggered, ensuring continued shared situational awareness while minimising response times.

Time is a critical factor during cyber incidents affecting power systems. Historical incidents have demonstrated that attackers can move from initial compromise to disruption of operational systems within a short timeframe. Once operational technology systems are affected, the available response window may be measured in seconds rather than minutes.

Maintaining grid stability therefore requires a response process that combines rapid cyber detection with rapid operational decision-making. The SOC must identify and assess threats as early as possible, while the Control Room

simultaneously evaluates potential impacts on power system operations using a digital twin of the EPES. As incident severity increases, predefined countermeasures can be progressively activated, ranging from enhanced monitoring and containment measures to isolation of compromised assets and operational mitigation procedures on both the cyber and physical level.

This coordinated approach enables defensive actions to be performed before attackers can successfully transition from cyber compromise to physical disruption. At the same time, the involvement of Control Room operators prevents cybersecurity actions from unintentionally reducing operational capabilities during a critical event. The result is a response model that balances speed with safety and ensures that both cybersecurity and grid reliability objectives remain aligned.

The resulting workflow can be summarised as follows:

1. The SOC detects early indicators of malicious activity.
2. The incident is assessed and classified according to its severity and potential operational impact.
3. The Control Room is informed and evaluates potential grid consequences using a digital twin.
4. Predefined response playbooks are selected.
5. Non-critical actions are executed automatically where possible.
6. Actions affecting critical operational systems require Control Room authorisation or previously granted pre-authorisation.
7. The Control Room can take preventative actions within grid operations to limit operational impact.
8. Both teams maintain shared situational awareness throughout the incident and jointly determine escalation, recovery, and reporting actions.

This collaborative operating model recognises that cybersecurity incidents in EPES are no longer purely cyber events. Their ultimate impact is determined by physical consequences on the electricity grid. Effective incident response therefore requires continuous cooperation between SOC analysts and Control Room operators, supported by common severity classifications, predefined playbooks, and clearly defined authorisation processes.

6 Overall Perspective, recommendations and vision

6.1 Overall perspective

The digital transformation of our societies is ongoing at a high pace. One of the key elements in this transformation is Europe's Electrical Power and Energy System (EPES), that is evolving into a smart and digitalised grid (the Smart Grid). We see that Digitalisation will, however, also increase the vulnerability of the EPES for system failures and cybersecurity threats. Cybersecurity measures that are addressing both IT and OT environments are needed to protect the EPES against cyber-attacks. But at the same time, both in the threat landscape and in cybersecurity measures, disrupting developments are ongoing due to rapid introduction of new technology such as virtualisation, AI & Agentic AI.

To protect the EPES against cyber-attacks, a balanced set of preventative, proactive and reactive security measures need to be implemented. An important reactive security measure is cyber incident monitoring, detection and response, usually operated in a SOC and a CSIRT that provide operational cybersecurity services to the organisation. A SOC is becoming automation enabled, embedding autonomous actions and operations and using (agentic) AI to enhance its processes for monitoring, detection and response. Implementing a SOC in EPES operations, however, comes with some challenges.

Challenge 1: Cybersecurity automation.
During disruptive (automated) cyber-attacks, the available response window can be extremely short, leaving little time for manual investigation and decision-making. To maintain an effective level of protection, SOCs must therefore leverage automation wherever possible. Automated detection, analysis, and response capabilities can significantly reduce reaction times and improve consistency. However, given the critical nature of electricity infrastructure, automation must be applied in a controlled manner. Rapid and aggressive automated actions may be appropriate for low-risk scenarios, while actions that could directly affect power system operations should retain human oversight.

We solve this issue by introducing a playbook driven approach using SOAR tools that are (CACAO) standards based to systematically manage these processes. Specifically, we have implemented a SOAR with TNO's open-source SOARCA, enabling a coordinated execution of both human-in-the-loop and completely automated tasks. The SOC automation focuses on enhancing situational and option awareness for cybersecurity analysts in the SOC of EPES organisations. This enables operators to make informed decisions regarding (incident response) actions to possible cyber threats and ongoing cyberattacks with greater accuracy and speed, while maintaining human-in-the-loop for critical infrastructure such as power grids. Additionally, the playbook-driven automation facilitates response actions that are either pre-authorised or done in real-time by operators. This ensures that control room operators are aware of any mitigative cybersecurity actions which may hinder their operational control.

Challenge 2: Network Segmentation.

EPES environments are typically designed according to the Purdue network segmentation and IEC 62443-3-2 zone-and-conduit principles, in which networks are segmented, and communication flows are restricted. Consequently, centralised collection of data and incident response by a SOC is complicated.

We solve this issue by applying to the SOC the same segmentation as the Purdue (IEC) 62443 zone-and-conduit principles; instead of one SOC that spans levels, we use federated SOC enclaves, each aligned to a zone. An enclave watches its own zone and does not reach vertically into the zones above or below. Responsibilities in a grid already have been organized this way, so a SOC that mirrors this organization perfectly aligns with how operators already work. For a large substation with staff on site, an enclave can sit at the substation itself. Each enclave is self-contained and carries its own detection and response tooling and keeps working when its zone is cut off from the rest of the network. Each enclave also runs its own security orchestration and automation, and control over the response playbooks stays local to the enclave. The central SOC can trigger an enclave's automation but cannot rewrite or override its playbooks. Actions that touch critical cyber-physical components are held behind a human in the loop, so a control-room operator authorises anything that could move a breaker before it runs.

Challenge 3: Collaboration between the Control Room and the SOC.

Effective response to cyber incidents in EPES requires close collaboration between the Control Room and the SOC. Cyber incidents cannot be assessed solely from a cybersecurity perspective; their potential impact on grid operations must also be considered. However, Control Room and SOC personnel often operate in different organisational cultures and possess different expertise, terminology, and objectives. Establishing effective communication processes, shared situational awareness, and coordinated decision-making is therefore a key challenge.

Challenge 4: Incident Response in OT.

Responding to cyber incidents in IT environments often involves automated actions such as isolating systems, blocking communications, or reconfiguring network components. In OT environments, however, such actions may have unintended consequences for power system operations. A cybersecurity response that disrupts communications or removes access to critical systems may reduce the ability of Control Room operators to monitor, control, or recover grid assets. As a result, response actions in OT environments require careful consideration of both cybersecurity and operational risks.

We solve the issues from challenge 3 and 4 by introducing a converged SOC concept, that introduces structured communication and collaboration between both teams. One of the key elements in this communication is the use of the framework introduced by ENTSO-e and DSO Entity for assessing cybersecurity incidents; it defines a common language for coordinated decision-making between SOC and control room and introduces a scale for the gravity of a cyber-attack and for the severity of a cyber-attack (potential impact on electricity operations). Countermeasures are developed, validated, and agreed upon in advance through jointly developed response playbooks with three categories of response actions: Information gathering and enrichment, automated actions affecting non-critical IT or OT assets and actions affecting critical operational systems or communications. The third category requires explicit involvement of Control Room personnel (human in the loop), the other categories can be fully automated. Organisations may establish pre-authorised response actions, to speed up the detection response process.

6.2 Recommendations

In this concept paper, we have introduced new approaches in security monitoring, detection and response for EPES that deal with the challenges as identified in section 2. We have demonstrated that these approaches can be viable solutions, but they are not production-ready yet. And not all challenges that might hinder the smooth implementation of security operations in EPES are addressed in this concept paper. Therefore the main recommendation is to continue the work: research institutes to address remaining challenges with research and innovation, industry to develop commercial products based on the approaches described in this paper and organisations that manage EPES to implement them in their operations.

We also have formulated the following concrete recommendations, based on the previous sections in this paper:

- Because of the high pace of digital transformation, evolving threat landscape and technology development, an innovative mindset is essential in maintaining an optimal cyber defense against attacks. Continuous improvement and assessment of cyber defense and response capabilities involving a converged IT and OT environment is needed, especially when not dealing with an ongoing attack. Don't wait for the next attack but prepare for it;
- When not already done, start to implement security monitoring, detection and response on all network segment levels and start to automate a selection of the monitoring, detection and response activities;
- The challenges of automating monitoring, detection and response will be different for every organisation. Therefore, we recommend trying the concepts out in practice, assess how they can apply to a specific organization and infrastructure and see where practical issues arise;
- AI-powered tooling will inherently introduce non-deterministic behaviour. Therefore, it is recommended to be careful with monitoring, detection and response that apply fully automated steps implemented with AI technology. Always have a human in the loop in decisions that might impact EPES stability and continuity;
- We recommend adopting a playbook-driven approach for cybersecurity operations:
  - Playbooks can guide the process and ensure that roles, ownership and responsibilities are clear, both between IT SOC and control room and within (different levels of) an IT SOC and control room;
  - A playbook driven approach can involve pre-authorization to save time; it can embed predefined trigger conditions for pre-authorized actions;
  - A playbook driven approach can reduce the chance of misconfiguration of (repetitive) actions compared to manual actions by analysts;
  - A playbook driven approach can drastically shorten the response time and consequently reduce business impact of attacks;
- Consider the use of a digital twin of the EPES to simulate possible response and mitigating actions before implementing them.

Abbreviations

Abbreviation	Description
APT	Advanced Persistent Threat
AI	Artificial Intelligence
BPMN	Business Process Model and Notation
CACAO	Collaborative Automated Course of Action Operations
CER	Critical Entities Resilience
CERT	Computer Emergency Response Team
CoA	Course of Action
COSSAS	Community for Open Source Security Automation Software
CRA	Cyber Resilience Act
CSIRT	Computer Security Incident Response Team
CSOC	CyberSecurity Operation Centre
CTI	Cyber Threat Intelligence
DER	Distributed Energy Resources
DMZ	Demilitarized zone
EPES	Electrical Power and Energy System
HMI	Human Machine Interface
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Devices

Abbreviation	Description
IP	Internet Protocol
MSSP	Managed Security Service Provider
NCCS	Network Code for CyberSecurity
NIS2	Network and Information Security 2
NIST	National Institute of Standards and Technology
OIE	Orchestration & Integration Engine
OASIS	Organization for the Advancement of Structured Information Standards
OpenC2	Open Command and Control
OT	Operational Technology
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable logic controller
PV	Photo-Voltaic
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SEM	Security Event Management
SIEM	Security information and event management
SIM	Security Information Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operation Centre

References

Abbreviation	Description
[1]	"MITRE ATT&CK Campaign C0028 - 2015 Ukraine Electric Power Attack," MITRE, [Online]. Available: https://attack.mitre.org/campaigns/C0028/. [Accessed 26 07 2026].
[2]	CISA, "Ukraine power grid caused regional blackout," 20 07 2021. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. [Accessed 26 07 2026].
[3]	"MITRE ATT&CK Campaign C0025 - 2016 Ukraine Electric Power Attack," MITRE, [Online]. Available: https://attack.mitre.org/campaigns/C0025/. [Accessed 26 07 2026].
[4]	Press releases of Deutsche Windtechnik, "Cyber attack on Deutsche Windtechnik", 22 April 2022. Available: https://www.deutsche-windtechnik.com/nl/news/press-releases/detail/cyber-attack-on-deutsche-windtechnik/ [Accessed 29 07 2026].
[5]	Press releases of Nordex, "Update on cyber security incident", 12. April 2022. Available: https://www.nordex-online.com/en/2022/04/update-on-cyber-security-incident/ [Accessed 29 07 2026].
[6]	SectorCERT, "The attack against Danish, critical infrastructure," SectorCERT, 2023.
[7]	"SafePay Ransomware Strikes Stadtwerke Clausthal-Zellerfeld," DeXpose, 17 12 2025. [Online]. Available: https://www.dexpose.io/safepay-ransomware-strikes-stadtwerke-clausthal-zellerfeld/. [Accessed 26 07 2026].
[8]	"eGovernment Verwaltung Digital - Cyberangriffe auf Stadtwerke und Versorger," 23 10 2024. [Online]. Available: https://www.egovernment.de/cyberangriffe-auf-stadtwerke-und-versorger-a-e6adf60be1d12e997a37a3b7b06d59e0/. [Accessed 26 07 2026].

Abbreviation	Description
[9]	CISA, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," CISA, 2024.
[10]	CERT.PL, "Energy Sector Incident Report - 29 December," CERT Polska, 2026.
[11]	Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. 14 December 2022. Available: http://data.europa.eu/eli/dir/2022/2557/oj
[12]	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
[13]	Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements. 23 October 2024. Available: http://data.europa.eu/eli/reg/2024/2847/oj
[14]	Commission Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows. 11 March 2024. Available: http://data.europa.eu/eli/reg_del/2024/1366/oj
[15]	ENISA, "How to setup CSIRT and SOC," ENISA, 2020.
[16]	F. Fransen and R. Wolthuis (Eds.), "SOCCRATES Vision, Roadmap & Guidance for SOC", SOCCRATES Horizon Europe 2020 programme - grant agreement number 833481, 2022. Available: https://www.soccrates.eu/wp-content/uploads/2022/05/SOCCRATES_D2.4_v1-Final-version.pdf [Accessed 29 July 2026]

Abbreviation	Description
[17]	NIST, "Guide for Security-Focused Configuration Management of Information Systems," NIST Special Publication, 2011.
[18]	Jordan, B., & Thomson, A. (Eds.), "*CACAO security playbooks version 2.0*"; OASIS Open, 27 November 2023. Available: https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html. [Accessed 26 07 2026].
[19]	Williams, T. J., "The Purdue Enterprise Reference Architecture", IFAC Proceedings Volumes, 26(2), 559–564. Available: https://doi.org/10.1016/S1474-6670(17)48532-6
[20]	IEC standard 62443-3-2:2020, "Security for industrial automation and control systems — Part 3-2: Security risk assessment for system design", International Electrotechnical Commission, 2020.
[21]	Martin, M., Chanoski, S., Granda, S., Kunsman, S., & Sachs, M., "Reference Architectures as a Means of Influencing Electric Energy Operational Technology/Industrial Control System Security Outcomes", U.S. Department of Energy, March 2022.
[22]	Maarten de Kruijf, Frank Fransen, Bart Hofman, Tom Brouwels, and Firas Ousta, "Converged IT/OT SOC architecture applied to power grids enabling collaboration between control room and security personnel", TNO, 2025. Available: https://publications.tno.nl/publication/34646502/QpEa1VOK/Kruijf-2026-Converged.pdf
[23]	Rajkumar, Vetrivel Subramaniam, et al. "Cyber attacks on protective relays in digital substations and impact analysis." *2020 8th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems*. IEEE, 2020.
[24]	Semertzis, I., Rajkumar, V. S., Ştefanov, A., Fransen, F., and Palensky, P., "Quantitative risk assessment of cyber attacks on cyber-physical systems using attack graphs." *2022 10th Workshop on Modelling and Simulation of Cyber-Physical Energy Systems (MSCPES)*. IEEE, 2022. Available: https://palensky.org/pdf/Semertzis2022.pdf
[25]	Alexandru Ștefanov, et al. "D5.1 Report on demonstration D2", eFORT, June, 29th, 2026. (available upon request from the Dutch eFORT partners).
[26]	"CYBER-ATTACK CLASSIFICATION SCALE METHODOLOGY", ENTSO and EU DSO entity, 2025 Available: https://consultations.entsoe.eu/ictc/pc-cyber-attack-classification-methodology/supporting_documents/CACS%20Methodology.docx

Acknowledgments

This vision paper is based on work in the eFORT project. The eFORT project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no. 101075665. https://efort-project.eu/

We specifically want to thank the eFORT colleagues of TU Delft, ENCS, Tennet and DNV for the productive and pleasant collaboration on the Dutch pilot.


eFORT
TNO
innovation
for life