

# Converged IT/OT SOC architecture applied to power grids enabling collaboration between control room and security personnel

Maarten de Kruijf  
*Scientist innovator OT*

TNO - Nederlandse Organisatie voor  
toegepast-natuurwetenschappelijk  
onderzoek

HTC25, Eindhoven, Netherlands  
maarten.dekruijf[@]tno.nl

Frank Fransen  
*Senior scientist*

TNO - Nederlandse Organisatie voor  
toegepast-natuurwetenschappelijk  
onderzoek

ZLN, Groningen, Netherlands  
frank.fransen[@]tno.nl

Bart Hofman  
*Scientist*

TNO - Nederlandse Organisatie voor  
toegepast-natuurwetenschappelijk  
onderzoek

HTC25, Eindhoven, Netherlands  
bart.hofman[@]tno.nl

Tom Broumels  
*Supervisor*

Fontys university of applied sciences  
Strijp-TQ, Eindhoven, Netherlands  
t.broumels[@]fontys.nl

Firas Ousta  
*Supervisor*

Fontys university of applied sciences  
Strijp-TQ, Eindhoven, Netherlands  
firas.ousta[@]fontys.nl

**Abstract**—The increasing convergence of Information Technology (IT) and Operational Technology (OT) in critical infrastructures such as power grids introduces both operational efficiencies and significant cybersecurity challenges. This paper proposes a Collaborative Converged Local Control SOC Architecture (CCLCSA) to enhance cyber resilience in Electric Power and Energy Systems (EPES). Building on the Purdue Enterprise Reference Architecture and IEC 62443 standards, the architecture integrates Security Operations Center (SOC) enclaves with OT control environments, enabling federated security monitoring and coordinated incident response. A proof-of-concept (PoC) was developed using open-source tools (Suricata, Wazuh, and SOARCA) and validated in a virtualized IEEE 39-bus power grid model. The approach emphasizes playbook-driven automation with human-in-the-loop safeguards to balance rapid incident response with operational safety. Results demonstrate improved collaboration between SOC personnel and control room operators, supporting semi-automated and automated responses to advanced cyber threats. While promising, the architecture requires further research for real-world deployment and broader adoption.

**Index Terms**—SOC, Security OT, Security IT/OT, ICS, SCADA, Architecture, IT/OT, Converged, distributed, Purdue, PERA

## I. INTRODUCTION

On December 23, 2015, the Ukrainian power grid operated by Kyivoblenergo appeared to be functioning normally. However, behind the scenes, a coordinated cyberattack was unfolding. At 15:35 local time, seven 110 kV and twenty-three 35 kV substations were simultaneously disconnected for three hours, resulting in widespread power outages [1]. This attack was attributed to the Sandworm group, which is associated with Russia [2].

This attack would also signal to other countries like the US and members of the EU that the power grid infrastructure

is vulnerable. Digitalisation in EPES results in introduction and integration of Information Technology (IT) systems into Operation Technology (OT) environments [3], [4], [5], [6]. While convergence improves visibility, efficiency, and remote control it introduces new pathways for adversaries to from IT into OT. With this in mind and current SOC models tailored to IT monitoring and response, organisations struggle to maintain visibility into OT environments. Even when they do so, timely response and safe actions in the distributed OT environments is hard due to integration complexity, maintenance and legacy system integration [7].

This paper will go into the components that are part of the IT and OT domain to detect cyber attacks. We summarise cyber treats of last year summarised by Miller et al. [8] and Ibis et al. [9]. This paper highlights innovations developed in the eFORT project [10] and proposes architecture improvements helping Cyber Security Incident Response Teams (CSIRT) within the Control Room of the Future (CRoF).

## II. BACKGROUND

### A. Process automation

Process automation or often called OT is used to automate everyday processes and functions to operate society [11]. These processes are controlled by hardware and software that will monitor and operate devices that enable these automation processes. One can think of energy generation and distribution, waste water treatment, or the manufacturing of goods. A central piece of equipment in OT is the so called programmable logic controllers (PLC), which handle the control loops based on the monitored inputs and generating the outputs. These PLCs are typically managed by supervisory control and data acquisition (SCADA) systems or distributed control systems (DCS) [12]. In the early days

these systems were not connected to the internet or even networked at all and operated isolated from the enterprise networks. Due to demands such as higher efficiency, insight and just-in-time delivery. The PLCs were connected to the enterprise network [12].

When we look at an enterprise and its networks we can see a clear difference between IT and OT. Where IT's main focus is on (processing) data and has to ensure it's confidentiality, integrity and availability [13]. The focus of OT is on operating and monitoring physical processes. Where safety and availability are the driving factors. This is also reflected in the types of equipment used in OT, as it uses specialised devices and proprietary systems tailored to the specific needs of the process like PLCs. Other devices commonly found in OT are:

- Intelligent Edge Device (IED);
- Human Machine Interface (HMI);
- Remote Terminal Units (RTU);
- SCADA servers;
- DCS servers.

Where in IT general purpose operating systems are used in datacenters and endpoint devices to perform data driven tasks [14].

With the onset of industry 4.0 these worlds have begun to merge into a converged IT/OT environment. The merge of these environment brings operational efficiency, real-time insight and analytics. Although there are many gains of the merger of these environments, there are some challenges like compatibility and security.

The combination can be described using the Purdue Enterprise Reference Architecture (PERA) [15], [16] commonly referred to as the Purdue model. To explain the security challenges in commonly used OT devices and protocols this paper will explore them, with a special interest in devices and protocols used in power grid systems.

### B. Enterprise zoning and organisation segmentation

The Purdue enterprise reference architecture (PERU) was developed to facilitate the generic integration of computer integrated manufacturing (CIM) into any manufacturing facility. Among other things it introduced the hierarchical view or zoning.

These levels provide a structured approach to organizing and managing the various functions within a manufacturing plant. By dividing the system into distinct levels, it allows for clear separation of responsibilities, improved coordination, and efficient operation of the manufacturing process. Each level has specific roles and responsibilities, ensuring that all aspects of the manufacturing process are covered, from physical operations to high-level enterprise management [16]. This also allows for safety boundaries that are coupled to the responsibilities [17].

The summary of the levels as described by Williams [16] are:

- Level 0: Physical Process
  - Content: Includes the actual physical processes and equipment (conveyor belts, reactors, distillation columns etc.) used for manufacturing.

- Role: Actual process execution by physical equipment.
- Level 1: Direct digital control
  - Content: Includes intelligent devices like sensors, actuators, and controllers that directly interact with the physical process.
  - Role: Responsible for data acquisition and direct control of the physical process.
- Level 2: Supervisory control
  - Content: Includes programmable logic controllers (PLCs), distributed control systems (DCS), and other control systems.
  - Role: Manages real-time control and monitoring of the manufacturing process, ensuring that operations are carried out according to plan.
- Level 3: Manufacturing Operations Systems
  - Content: This level encompasses manufacturing execution systems (MES) and other systems that manage production activities.
  - Role: Focuses on the execution of production plans, scheduling, and tracking of production activities, ensuring efficient operation and coordination of manufacturing processes.
- Level 4: Business Planning and Logistics
  - Content: Includes enterprise resource planning (ERP) systems and other business management systems.
  - Role: Handles business-related functions such as production planning, logistics, inventory management, and order processing. This level ensures that manufacturing operations align with business objectives and customer demands.
- Level 5: Enterprise Management
  - Content: This level involves corporate management functions, including strategic planning, financial management, and overall enterprise governance.
  - Role: The focus is on high-level decision-making, setting long-term goals, and ensuring that the entire enterprise operates cohesively and efficiently.

The Purdue model today is often referred to from a security context [15], [18], [19] also in context to zero trust networking which has become more prevalent in IT and is emerging in OT [20].

For electric power and energy systems (EPES) the general architecture is the same but there are some specific devices. Martin et al.[21] describes such an architecture for power grid specifically. The EPES architecture is displayed in Fig. 1.

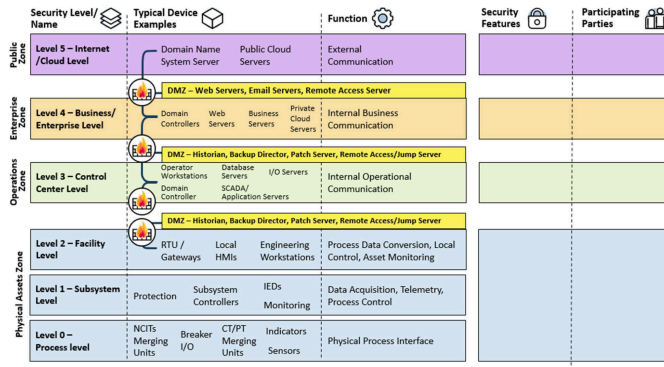


Fig. 1. SEI ETF Reference Architecture for Electric Energy OT.

### C. Security Operations

Cyber resilience is based on different aspects like asset management, hardening, patching, cyber threat intelligence, security monitoring and detection, and incident response. These facets are specified in norms and standards like ISO27002:2022 IEC62443, NIST 800-82r3, and Nist Cyber security framework (CSF) 2.0.

a) *Security Operation Center (SOC)*: Security monitoring and application monitoring is common practice in today's cloud and enterprise environments. SOC's employ many ways to monitor for and respond to cyber threats. The SOC mission as described by Knerler et al. [22]: "A typical midsize SOC's mission statement typically includes the following elements:

- Preventing cybersecurity incidents through proactive measures, including:
  - Continuous analysis of threats
  - Scanning for vulnerabilities
  - Deploying coordinated countermeasures
  - Consulting on security policy and architecture
- Monitoring, detection, and analysis of potential intrusions in real time and through adversary hunting, utilizing a variety of security-relevant data sources
- Responding to confirmed incidents, by coordinating resources and directing use of timely and appropriate countermeasures
- Providing situational awareness and reporting on cybersecurity status, incidents, and trends in adversary behavior to appropriate organizations
- Engineering and operating SOC technologies, such as host sensors, network sensors, log collection, and analysis systems"

To make this mission a success the SOC functions need to have equal mandate to the IT operations [22]. If not done so availability might trump security considerations [22].

b) *SOC Tooling (SIEM)*: In the SOC, SIEM tooling is essential to the operation. There are many SIEM vendors with known vendors like: Splunk [23], Microsoft Sentinel [24], QRadar [25] and Elastic Security [26]. Few of them offer open source tools like Wazuh [27] and Elastic Security. The SIEM combines Cyber Threat Intelligence (CTI) with event logs sources to generate alerts based on rules or anomaly detection algorithms. These days also machine learning (ML)

and artificial intelligence (AI) is used to enrich data and contextualise alerts.

c) *(Automated) response*: Based on generated alerts response needs to be taken this can be done by SOC operators in collaboration with infrastructure colleagues. This is part of the incident response duties of the SOC. Execution of response tasks can be based on loosely defined steps in wiki's, mails, BPMN etc. but we see a shift to playbook driven response [28], [29]. These playbooks can be executed by hand but also be tightly integrated with security orchestration automation response (SOAR) tooling. The known vendors have integrated proprietary formats in their SOAR tools. But there are open formats like Collaborative Automated Course of Action Operation version 2 (CACAOv2) [29]. This can be executed by SOAR tools like SOARCA [30].

d) *Segmentation architectures*: Segmentation is a well known practice for enforcing security measures. Around 2011 Zero Trust has been introduced as a concept [31], [32]. The concept takes a perimeter from device to an access and behaviour approach [32]. This allows for more dynamic access and control to data and assets.

### D. OT Communication Protocols

Protocols in OT are designed for machine to machine operation (M2M) and typically in binary form. Most vendors have their own proprietary protocols like Siemens' S7COMM+. These protocols are typically found in communication between PLCs, sensors and actuators (like motors). These protocols are not engineered to include strong security [33], [34]. Other commonly used protocols are: ModbusTCP/RTU, DNP3, OPC-DA, OPC-UA. and more recent IoT protocols [35] such as MQTT and Kafka. Within certain industries like power grids, specific protocols are used based on the IEC61850 such as: Generic Object Oriented Substation Event (GOOSE), sampled value (SV) and Manufacturing Message Specification (MMS). The traditional or specialised protocols focus on speed of processing and staying within the deadline so they are often based on ISO layer 2 MAC addressing. Although they often have a layer 3 TCP/IP counterpart. The newer protocols focus on integration with IT systems and data insights to power MES and ERP systems.

### E. Incidents

The earlier mentioned Ukrainian cyber attack [1], [2] doesn't stand on its own. In the last years many OT incidents have been taking place. Between 2020 - 2023 alone we see that 133 incidents [9] have occurred. Additional research for 2023 - 2024 has been done added [9]. Many of the attacks have been targeted at the IT level and then pivoting into the OT system [8], [9]. Having granular insight into these attacks is key to track cyber incidents in an enterprise organisation. More recently attacks continue with the attack on the Poland grid as reported by NFP [36].

### III. RELATED WORK

#### A. SOAR in OT

As we discussed automated response which will form the bases of our work. Chatterjee et al. shows that SOAR in oil and gas has been explored and deemed possible [7]. Despite having its benefits like efficiency improvements and reducing mean time to detect MTTD and mean time to response MTTR, integrations remains difficult. Factors like legacy system integration and performing maintenance and updates remain limiting factors. Furthermore, having skilled personnel is mentioned as a problem [7].

#### B. Zero Trust in OT

Zero trust has gained traction in the last years. This allows for effective control point in an infrastructure. It also enables controlled execution of tools like SOAR. Garton et al. [15] introduces Purdue zoning. And zero trust in OT, is described by Nozomi [20]. Paul et al. [37] explored zero trust for smart industry, outlines role based remote access and removing implicit trust between OT devices.

#### C. OT SOC architectures

Based on the principles of deny by default and rigours authentication, architectures are being introduced like ISERA [38]. But these don't address the distributed nature of more complex OT-systems, the collaboration between control room and SOC personnel and automated response combined with zero trust principle like segmentation. Laue et al. [39] described advanced detection in OT with the Wazuh SIEM attempting to perform quick response, in both IT and OT.

### IV. METHODOLOGY

In this section we present the outline of the methodology used in the research. First we describe the phases, then we will outline the experimental setup.

#### A. Research phases

The research has been done in 3 distinct phases: literature study, Architecture PoC development and PoC testing.

a) *Literature study*: To define the state of the art (SotA) we have performed a literature study to establish insights on the security principles used in OT. The following keywords were used to query for relevant material "plc", "security", "OT-SOC", "Converged IT/OT SOC" and "OT operator involvement". This resulted in a basis of scientific papers for these papers we have applied snowballing technique[40] in a moderate form. Besides these papers we have included relevant standards and drafts. Lastly non scientific papers, reports and web material have been added to get a full picture. These inputs have resulted in the definition of an use case and problem definition and requirements. This is depicted in in Fig. 2 with the green rounded rectangle.

b) *Architecture and Proof of Concept development*: To define a relevant architecture we must make sure that our results are based on current standards and architectures out there. That's why we use Purdue[16] and IEC62443-3-3[41] as the

basis of our design. To facilitate the use case the PoC needs to include the components needed for the scenario. The PoC also need to represent current and future components employed by power grid operators and in more general OT-operators. This is shown in Fig. 2 with the yellow rounded rectangle.

c) *Architecture and Proof of concept deployment and testing*: To validate our ideas we have deployed a virtual power grid based on the well known IEEE 39-Bus model[42]. This model is used to show the impact of our architecture adaptations and will be virtualised in the PoC. This is shown in Fig. 2 with the purple rounded rectangle. This results in an Architecture description tested with a PoC concept based on power grid infrastructure (blue rounded rectangle).

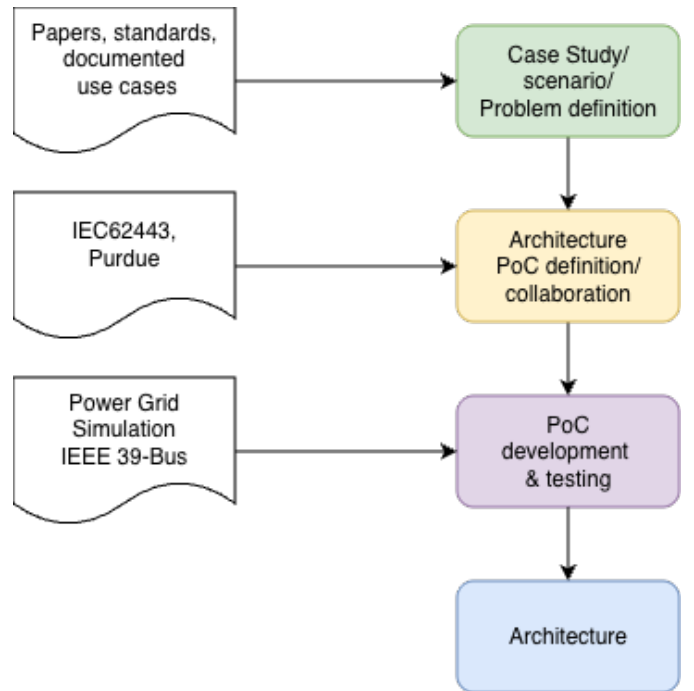


Fig. 2. Methods and resources.

#### B. Experimental setup

For the development of the PoC mainly open source tools were used to construct the environment. The advantages of using open source tools is they can be adapted and changed to the needs of the research. When problems arise they can easily be tackled due to the source being available.

To be able to recreate, start over and adapt the PoC easily all parts of the PoC are implemented with infrastructure as code (IaC). This is done using the Packer, Terraform and Ansible languages. These tools are then used to deploy in a virtual environment on a hypervisor host running Proxmox VE 8.4.16. This host has 768 GB of RAM, 5TB of NVME storage and an AMD EPYC 9354P 32-Core Processor.

For the experiments we have selected the aforementioned IEEE 39-bus [43], but we will also use the SEI ETF Reference architecture as starting point to develop our testbed and PoC.

Scenario's will be executed according to their description. The designed response action will trigger automatically based on their rules and triggers.

## V. RESULTS

We will first describe the requirements, then the PoC scenario. Finally we introduce our security operation center (SOC) enclaves[22] architecture which align with the Purdue levels described in Section II.B. We describe how monitoring and automation is added using network intrusion detection sensors (NIDS), endpoint detection and response (EDR), security incident event management (SIEM) and security orchestration automation and response (SOAR) tools. This together with how operators and security personnel can work together using these tools, and how this could be based on upcoming standards and regulations. Lastly we will describe how we integrated these tools into a PoC testbed.

### A. Requirements

To develop our architecture we have defined requirements to incorporate into the design.

Requirements:

- Usable in power grid infrastructures so must follow Purdue architecture;
- Allow for fully independent operation without any outside connections;
- Multi layered detection capability;
- Capable of using SOAR technologies and playbook actions;
- Enable synergy between control room and SOC to share situational awareness and collaborate on response.

### B. Scenario

To demonstrate the architecture and PoC we have developed a scenario which will show the advantages of the new architecture. The scenario is based on previous events where compromised IT infrastructure will lead to a pathway into the OT infrastructure. This scenario is fictional but based on the referred work of Miller et al.[8] and Ibis et al. [9]. Specific living of the land (LOTL) techniques of Volt Typhoon [44] were used.

This resulted in storyline 1 Fig. 3 where from right to left:

- 1) the attacker infects an IT workstation through phishing mail and malicious file download;
- 2) then the LOTL techniques are used to pivot to an engineering workstation via VPN and leaked credentials from the IT environment;
- 3) then the engineering workstation is used to infect the HMI in the substation;
- 4) the infected HMI is used to control the IED to change the breakers state in the substation and cause a blackout.

This is visualised in Fig. 3 storyline 2 an attack via physical break-in is not discussed in this paper.

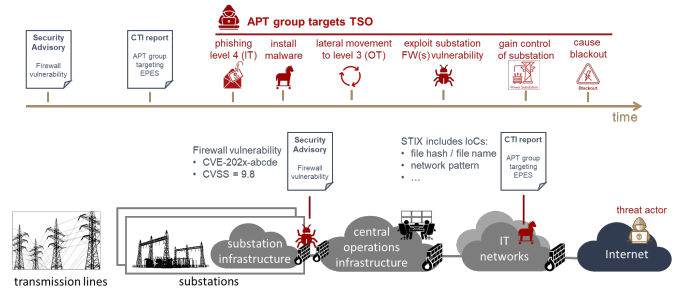


Fig. 3. Storyline 1 eFORT Dutch demo IT lateral movement (right to left)

This multistage attack allows us to have multiple opportunities to detect and respond. The scenario enables us to show the collaboration between control room and SOC by informing the control room of an ongoing attack. To do this we first need to lay out the adapted architecture and SOC zoning.

### C. SOC enclave on integrating with Purdue zoning

The fine grained integration of security tooling in power grid infrastructures allows for close monitoring and fine grained incident response. Knerler et al. [22] describes how SOC's could be structured in different ways. Because responsibilities in OT are located in different ways. Because responsibilities in OT are located in the control room (level 3) and site (level 0 - 2) with oversight of said control room, the SOC should operate accordingly and adopt the federated SOC model. This allows for local incident handling with reporting and assistance from a central SOC. For big substations with permanent operator presence this model could even be adopted to the substation level. This would mean a SOC enclave manned at the substation. In Section V.D we will discuss the interactions involved. The idea here is that SOC enclaves won't reach into vertical segments and only operate horizontally. To illustrate our Collaborative Converged Local Control SOC Architecture (CCLCSA) Fig. 4 shows the Purdue levels and shows the SOC enclaves in the same colours.

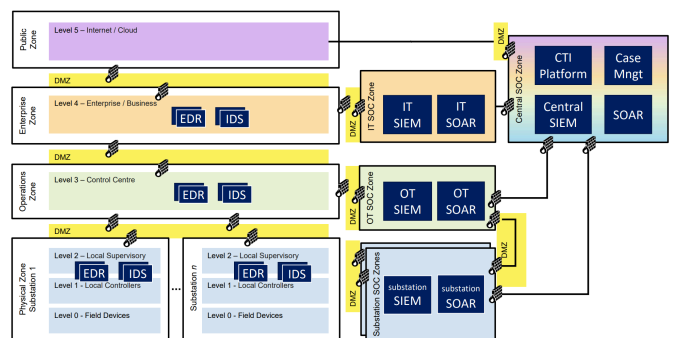


Fig. 4. CCLCSA merged with Purdue levels.

This federated SOC introduces a dependencies between zones, when introduced it should be only to gather data and communicate, so every enclave can work entirely independently. This allows for isolation during incidents like we have seen in Ukraine where the OT is isolated from the IT and internet. We propose SOC operations must follow

the same isolation standards without losing core operation capability and visibility.

To retain complete oversight on the environment we also introduce the converged SOC enclave. This enclave is not connected directly to the organisation's infrastructure but only to the enclaves via demilitarised zones (DMZs). This allows it to receive alerts from and perform queries to other SIEM instances. Specific tool integration is described in Section V.E. This integration is similar to IT sensor data integration and MES/ERP integration in OT processes. These systems are typically integrated into a clone or replication of a historian so they don't reach into the OT environment directly.

For security orchestration the enclaves work in conjunction. SOAR tooling is installed and maintained in each enclave. SOAR tooling should use playbook driven automation to allow for easy maintenance and creation of response actions. The central SOC zone can trigger enclaves SOAR but it can not override or change its playbook. The playbook control is left into the hands of the enclaves to ensure safe (physical safety) operation of the infrastructure as we are dealing with cyber physical systems. Creation and maintenance of playbooks thus must be a joint effort between security personnel and OT operators.

To allow for fine grained control (e.g. confine a single device service) and regulatory requirements playbooks could be constructed so they allow for semi automated execution through a human in the loop (HITL). This allows the execution to be governed by control room personnel and prevent unwanted side effects due to playbook execution. In some cases their could be a hybrid where playbooks could be partially automated to stop threats in its tracks but have some other parts or steps guarded by HITL.

#### D. Control room and SOC

To effectively communicate about security incidents both control room operators and security personnel need to speak the same languages. The introduction of the Network Code on Cyber Security (NCCS) by entsoe defines a new framework for incident severity and criticality. This framework is used to define severity of incidents that are communicated between SOC en control room to achieve synergy.

We don't want to dictate roles in the substation so we want to layout actions and responsibilities to be integrated or executed by control room operators and SOC personnel. We have described the actions that are essential to the collaboration between SOC in Table I. We have distinct initiators, and operations phases when these are used. This allows updates from the SOC to playbooks in normal operation and executions of playbooks during incidents. Note that the Notify for pre-authorized playbook execution is depicted but it should be integral part of the playbook.

TABLE I  
SOC CONTROL ROOM SYNERGY

| Initiator    | Interaction                                  | When            |
|--------------|----------------------------------------------|-----------------|
| SOC          | Request pre-authorisation for playbook       | NO <sup>1</sup> |
| SOC          | Report incidents to control room             | Incident        |
| SOC          | Request authorisation for playbook execution | incident        |
| SOC          | Notify for pre-authorized playbook execution | incident        |
| Control room | Authorise playbook                           | NO              |
| Control room | Authorise playbook execution                 | Incident        |
| Control room | Report incident severity                     | Incident        |

Fig. 5 Depicts a workflow of two actions that could be send during an incident. Where 1 describes the notification of an incident, and 2 describes the request for pre-authorization for a response action that interacts with critical cyber physical systems.

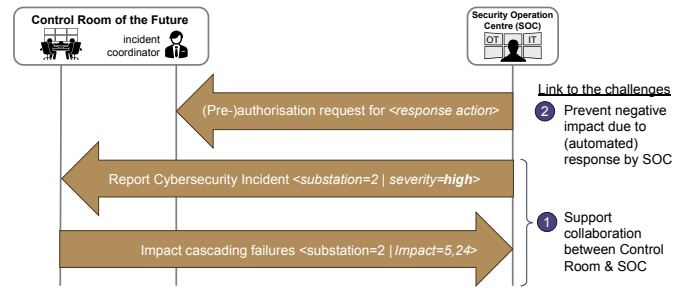


Fig. 5. Collaborative workflow SOC - Control room

a) *Playbooks*: These actions can be translated into the use of playbooks

We have developed different kinds of playbooks where we can divide them into three categories:

- 1) Data enrichment playbooks;
- 2) automated playbooks interacting with non critical cyber physical components or communication;
- 3) (semi)-automated playbooks interacting with critical cyber physical components or communication.

The first type of playbooks are used by the SOC to enrich their SIEM data, automate mondaime tasks and do basic reporting. An example is shown in Fig. 6 where we do a asset lookup in the asset database. This is reported to the control room.

<sup>1</sup>normal operation

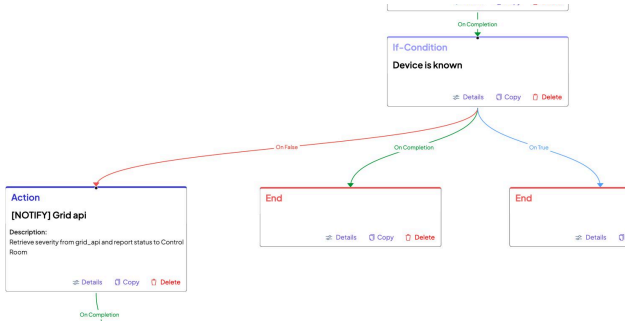


Fig. 6. New device discovered playbook condition and reporting step

The second type of playbook are used by the SOC to isolate hosts in the IT environment or in the non critical parts of the OT environment. This could be unknown hosts or host that do not impact the critical process. An full example is placed in Appendix A where we isolate a PC from the network.

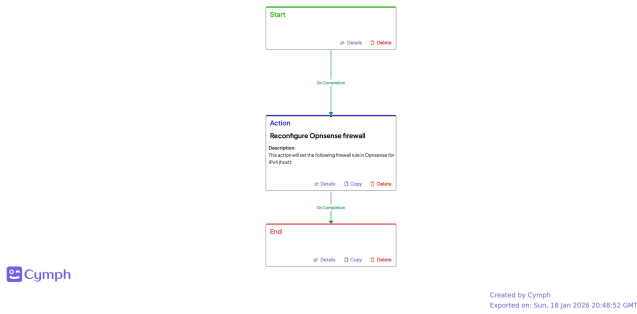


Fig. 7. OPNSense firewall rule playbook

The third type of playbook is used by the SOC together with the control room to intervene with components in the critical process. These playbooks should be safe to operate but can impact visibility or control into the substation. Because it's interacting with critical components and protocols for the operation of IEDs the playbook requires HITL interaction.



Fig. 8. HMI isolation playbook with GUARD as HITL step

The full playbooks are shown in Appendix A.

### E. PoC environment

The goal of the tool selection for our PoC is to allow for: easy implementation, reproducibility and standardisation. So to implement the PoC we have used the common open source security tools Suricata (NIDS), Wazuh (SIEM) and OPNSense (firewall). As these tools don't by them selves implement any SOAR capability and we want to make use of standardised specifications TNO has developed SOARCA. Which is an open source CACAOv2 based playbook executor engine developed by TNO [30].

#### a) SOARCA adaptations:

To allow for integration between SOARCA en Wazuh we had to develop a way to trigger Playbooks from events and alerts in the SIEM. We have integrated with Wazuh their custom integration [45] the example config can be found on GitHub [46]. This integration allows us to trigger on any event so we can enrich or activate responses based on that.

SOARCA didn't allow for playbook HITL actions so we had to add this function to it. SOARCA achieves this by executing a manual step and waiting for response. The response can be given by either a API call or a GUI interactions (which uses the same call). When a action is ignored a timeout is used to continue execution. The step will be considered failed. A playbook can also specify a timeout duration otherwise a default within SOARCA is used.

#### b) Deployed SOC:

We can see the deployed instances of our SOC enclaves in Fig. 9 where we have the IT, OT, and converged SOC enclaves. The full deployed network diagram can be found in Appendix B.

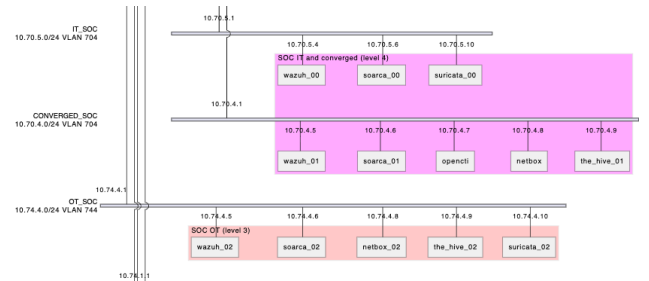


Fig. 9. Proof of Concept environment

The way the Wazuh SIEM handles this converged layout is using remote database access. This allows multiple instances to read the database and gather alerts. This approach does allow to have unfiltered access to the events and set alerts in each enclave or instance based on their needs and preferences.

## VI. DISCUSSION

The CCLCSA architecture has only been demonstrated in the described PoC environment. The proposed federated SOC is implemented in the Wazuh SIEM tool, which demonstrates it operational feasibility. Through the NCCS based reporting and HITL interactions between SOC and control room synergy could be reached in EPES environments. The adoption of the architecture could be integrated into existing

environments due to the adoption of the Purdue model through the SEI ETF Reference Architecture Fig. 1.

Although the proposed architecture is only tested in a lab setup it was presented during the ARES 2025 and ONE Conference 2025 multiple (inter)national parties, inside and outside of the energy domain, have showed high interest in the CCLCSA architecture and the tools developed in the eFORT project. This industrie recognition shows potential in the approach and should be researched further.

The usage of SOAR is controversial in EPES but the current setup allows for the discussion to be started. Many considerations need to be figured out as described by [7] but we think this could provide needed scaffolding to both integrate security functions and keep separation.

Playbook usage is still new in EPES, but it allows easy modification of response actions by personnel with limited software engineering skills both in the SOC as control room. This enables it to a powerful yet flexible tool to automate security operations.

#### A. Limitations

A point of consideration is that the CCLCSA architecture is based on the Purdue model. But other OT zoning models are used like the Namur Open Architecture (NOA) [47]. NOA is focused on cloud integration of OT environments. For the EPES use case NOA was not relevant as almost all organisations use the Purdue model but for other industries this might be an interesting topic to research.

Limitations of the chosen response strategy by using playbooks based on alerts is that events must have happened and logged in the SIEM. So a response might be “too late” as an attack might already have happened. This is in the nature of the chosen technology, catching threats early and preventing steps in the kill chain is the principle of the converged design. We didn’t perform benchmark testing for the responses in our research. Future research might focus on more immediate response options.

As we only performed the testing with playbooks on a simulated environments with only one substation we can’t make any determinations about the scalability of the architecture. Although the Wazuh SIEM can be scaled using both horizontal (more resources per instance) as vertical techniques (more instances) we don’t know the impact of the responses.

As we have engineered specific scenario’s we can’t generalise our outcomes using playbooks. MITRE D3FEND [48] and ATT&CK [49] as well as Open Cybersecurity Schema Framework (OCSF) [50] could help here but this was not part of our research.

#### B. Future work

The CCLCSA is mainly focused on the technical architecture and we have defined some interaction between control room and SOC. This interaction should be further researched on effectiveness, communications standards, wording and responsibilities. Also other actions like the engineering phase, recovery and regulatory interactions have opportunities for future research. Expansion to other industries like

Water, Critical infrastructure and manufacturing could bring new insights and have research opportunities. Especially the potential integration with NOA.

## VII. CONCLUSION

This paper demonstrates that SOC can be improved in EPES environments by introducing the CCLCSA architecture for the SOC. The findings mark the potential and limitations of automated cyber response collaboration in power grid systems. To address these and further explore possibilities, improvements and real world validation future research should be conducted.

## REFERENCES

- [1] A. Shehod, “Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US,” *Sustainable Energy*, 2016.
- [2] M. Pollard, “A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States.”
- [3] C. M. Coman and A. Florescu, “Electric grid monitoring and control architecture for industry 4.0 systems,” in *2018 International Symposium on Fundamentals of Electrical Engineering (ISFEE)*, Bucharest, Romania: IEEE, Nov. 2018, pp. 1–6. doi: 10.1109/ISFEE.2018.8742435.
- [4] F. Li *et al.*, “Smart Transmission Grid: Vision and Framework,” *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 168–177, Sep. 2010, doi: 10.1109/TSG.2010.2053726.
- [5] I. Alotaibi, M. A. Abido, M. Khalid, and A. V. Savkin, “A Comprehensive Review of Recent Advances in Smart Grids: A Sustainable Future with Renewable Energy Resources,” *Energies*, vol. 13, no. 23, p. 6269, Nov. 2020, doi: 10.3390/en13236269.
- [6] G. R. Santos, E. Zancul, G. Manassero, and M. Spinola, “From conventional to smart substations: A classification model,” *Electric Power Systems Research*, vol. 226, p. 109887, Jan. 2024, doi: 10.1016/j.epsr.2023.109887.
- [7] S. Chatterjee, “Using SIEM and SOAR for Real-Time Cybersecurity Operations in Oil and Gas,” vol. 6, no. 2, 2020.
- [8] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, “Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems,” *International Journal of Critical Infrastructure Protection*, vol. 35, p. 100464, Dec. 2021, doi: 10.1016/j.ijcip.2021.100464.
- [9] R. Ibis, “Cyberattacks on industrial control systems between 2020 - 2023,” Den Haag, technical report, Jun. 2024.
- [10] eFORT, “Making European power grids more resilient and secure.” Accessed: May 14, 2025. [Online]. Available: <https://efort-project.eu/>
- [11] Gartner, “Operational Technology (OT).” Accessed: Apr. 26, 2025. [Online]. Available: <https://www.gartner.com/en/information-technology/glossary/operational-technology-ot>
- [12] Rapid7, “Operational Technology (OT).” [Online]. Available: <https://www.rapid7.com/fundamentals/what-is-operational-technology-ot/>
- [13] J. Ledesma, “What is the CIA Triad?” [Online]. Available: <https://www.varonis.com/blog/cia-triad>
- [14] M. Jansson, “What Is the Difference Between IT and OT? | IT vs. OT.” [Online]. Available: <https://www.paloaltonetworks.com/cyberpedia/it-vs-ot>
- [15] D. Garton, “PURDUE MODEL FRAMEWORK FOR INDUSTRIAL CONTROL SYSTEMS & CYBERSECURITY SEGMENTATION,” technical report 4–14, Nov. 2019.
- [16] T. Williams, “A Reference Model for Computer Integrated Manufacturing from the Viewpoint of Industrial Automation,” *IFAC Proceedings Volumes*, vol. 23, no. 8, pp. 281–291, Aug. 1990, doi: 10.1016/S1474-6670(17)51748-6.
- [17] M. Security, “Microsoft Azure Defender for IoT: IT vs. OT - What is OT and how is it different from IT.” [Online]. Available: [https://youtu.be/ThTTB6Do8?si=ELd-41sk35k4C1\\_D&t=1706](https://youtu.be/ThTTB6Do8?si=ELd-41sk35k4C1_D&t=1706)
- [18] Zpedia, “What Is the Purdue Model for ICS Security?.” [Online]. Available: <https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security>

- [19] Fortinet, "Purdue Model for ICS Security." [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/purdue-model>
- [20] M. C. Nozomi, "Don't Trust But Verify: Getting to Zero Trust for OT and IoT." Accessed: Feb. 26, 2025. [Online]. Available: <https://www.nozominetworks.com/blog/dont-trust-but-verify-getting-to-zero-trust-for-ot-and-iot>
- [21] M. Martin, S. Chanoski, S. Granda, S. Kunsman, and M. Sachs, "Reference Architectures as a Means of Influencing Electric Energy Operational Technology/Industrial Control System Security Outcomes." [Online]. Available: <https://secureenergy.inl.gov/content/uploads/27/2024/12/SEI-ETF-Reference-Architecture-for-EEOT.pdf>
- [22] K. Knerler, I. Parker, and C. Zimmerman, *11 Strategies of a world-class cybersecurity operations center / Kathryn Knerler, Ingrid Parker, Carson Zimmerman*, Second edition. Bedford, Massachusetts: MITRE, 2023.
- [23] Splunk, "The market-leading SIEM." Accessed: Jan. 02, 2026. [Online]. Available: [https://www.splunk.com/en\\_us/products/enterprise-security-essentials.html](https://www.splunk.com/en_us/products/enterprise-security-essentials.html)
- [24] Microsoft, "AI-GEREED PLATFORM Microsoft Sentinel." Accessed: Jan. 02, 2026. [Online]. Available: <https://www.microsoft.com/nl-nl/security/business/siem-and-xdr/microsoft-sentinel>
- [25] IBM, "IBM QRadar." Accessed: Jan. 02, 2026. [Online]. Available: <https://www.ibm.com/products/qradar>
- [26] E. B.V., "AI-driven SIEM that is open source and affordable." Accessed: Jan. 02, 2026. [Online]. Available: <https://www.elastic.co/security/siem>
- [27] Wazuh, "The Open Source Security Platform." Accessed: Jan. 02, 2026. [Online]. Available: <https://wazuh.com/>
- [28] D. Schlette, P. Empl, M. Caselli, T. Schreck, and G. Pernul, "Do You Play It by the Books? A Study on Incident Response Playbooks and Influencing Factors," May 2024, p. . doi: 10.1109/SP54263.2024.00060.
- [29] A. T. Bret Jordan, "CACAO Security Playbooks Version 2.0." Accessed: Apr. 19, 2025. [Online]. Available: <https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html>
- [30] TNO, "Security Orchestrator for Advanced Response to Cyber Attacks." Accessed: Apr. 19, 2025. [Online]. Available: <https://cossas.github.io/SOARCA/>
- [31] J. Kindervag, "Applying Zero Trust To The Extended Enterprise," 2011.
- [32] M. Shore, S. Zeadally, and A. Keshariya, "Zero Trust: The What, How, Why, and When," *Computer*, vol. 54, no. 11, pp. 26–35, Nov. 2021, doi: 10.1109/MC.2021.3090018.
- [33] E. López-Morales and U. Planta, "SoK: Security of Programmable Logic Controllers."
- [34] V. M. Iguere, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Computers & Security*, vol. 25, no. 7, pp. 498–506, Oct. 2006, doi: 10.1016/j.cose.2006.03.001.
- [35] L. Thames and D. Schaefer, "Software-defined Cloud Manufacturing for Industry 4.0," *Procedia CIRP*, vol. 52, pp. 12–17, 2016, doi: 10.1016/j.procir.2016.07.041.
- [36] N. Daniel Tilles, "Poland suffers major cyberattack on power grid, says Russia likely responsible." Accessed: Jan. 14, 2026. [Online]. Available: <https://notesfrompoland.com/2026/01/14/poland-suffers-major-cyberattack-on-power-grid-says-russia-likely-responsible/>
- [37] B. Paul and M. Rao, "Zero-Trust Model for Smart Manufacturing Industry," *Applied Sciences*, vol. 13, no. 1, p. 221, Dec. 2022, doi: 10.3390/app13010221.
- [38] P. Acharya, H. Ramachandran, K. A. David, R. Smith, and T. Al-Hadhrani, "Towards Net Zero Resilience: A Futuristic Architectural Strategy for Cyber-Attack Defence in Industrial Control Systems (ICS) and Operational Technology (OT)," *CMC*, vol. 82, no. 2, pp. 3619–3641, 2025, doi: 10.32604/cmc.2024.054802.
- [39] T. Laue, T. Klecker, C. Kleiner, and K.-O. Detken, "A SIEM Architecture for Advanced Anomaly Detection," p. 2473 KB, 2022, doi: 10.25968/OPUS-2321.
- [40] M. Naderifar, H. Goli, and F. Ghaljaie, "Snowball Sampling: A Purposeful Method of Sampling in Qualitative Research," *Strides Dev Med Educ*, vol. 14, no. 3, Sep. 2017, doi: 10.5812/sdme.67670.
- [41] "Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels," no. IEC 62443-3-3. 2019.
- [42] A. Pai, *Energy function analysis for power system stability*. Springer Science & Business Media, 1989.
- [43] T. Athay, R. Podmore, and S. Virmani, "A Practical Method for the Direct Analysis of Transient Stability," in *IEEE Transactions on Power Apparatus and Systems*, IEEE, 1979, pp. 573–584.
- [44] N. C. I. P. P. H. (C. I.-S. C. P. N. N. C. I. V. S. P. A. N. Ai Kimura NEC Corporation; Manikantan Srinivasan, "Volt Typhoon." Accessed: Jan. 02, 2026. [Online]. Available: <https://attack.mitre.org/versions/v18/groups/G1017/>
- [45] Wazuh, "integration - Local configuration (ossec.conf) - Wazuh documentation." Accessed: Oct. 19, 2025. [Online]. Available: <https://documentation.wazuh.com/current/user-manual/reference/ossec-conf/integration.html>
- [46] M. de Kruijf, "Wazuh SOARCA integration." Accessed: Jan. 02, 2026. [Online]. Available: <https://github.com/thecyberproject/SOARCA-wazuh-integration>
- [47] T. Himmelsbach, "NAMUR OPEN ARCHITECTURE." Accessed: Jan. 02, 2026. [Online]. Available: <https://www.namur.net/en/work-areas-and-project-groups/focus-topics/namur-open-architecture.html>
- [48] The MITRE Corporation, "MITRE D3FEND™: A Knowledge Base of Cybersecurity Countermeasures." [Online]. Available: <https://d3fend.mitre.org/>
- [49] The MITRE Corporation, "MITRE ATT&CK®: The Adversarial Tactics, Techniques, and Common Knowledge Knowledge Base." 2025.
- [50] "Open Cybersecurity Schema Framework." Accessed: May 14, 2025. [Online]. Available: <https://schema.ocsf.io/1.7.0/?extensions=>

APPENDIX A



Fig. 10. New device discovered playbook condition and reporting step

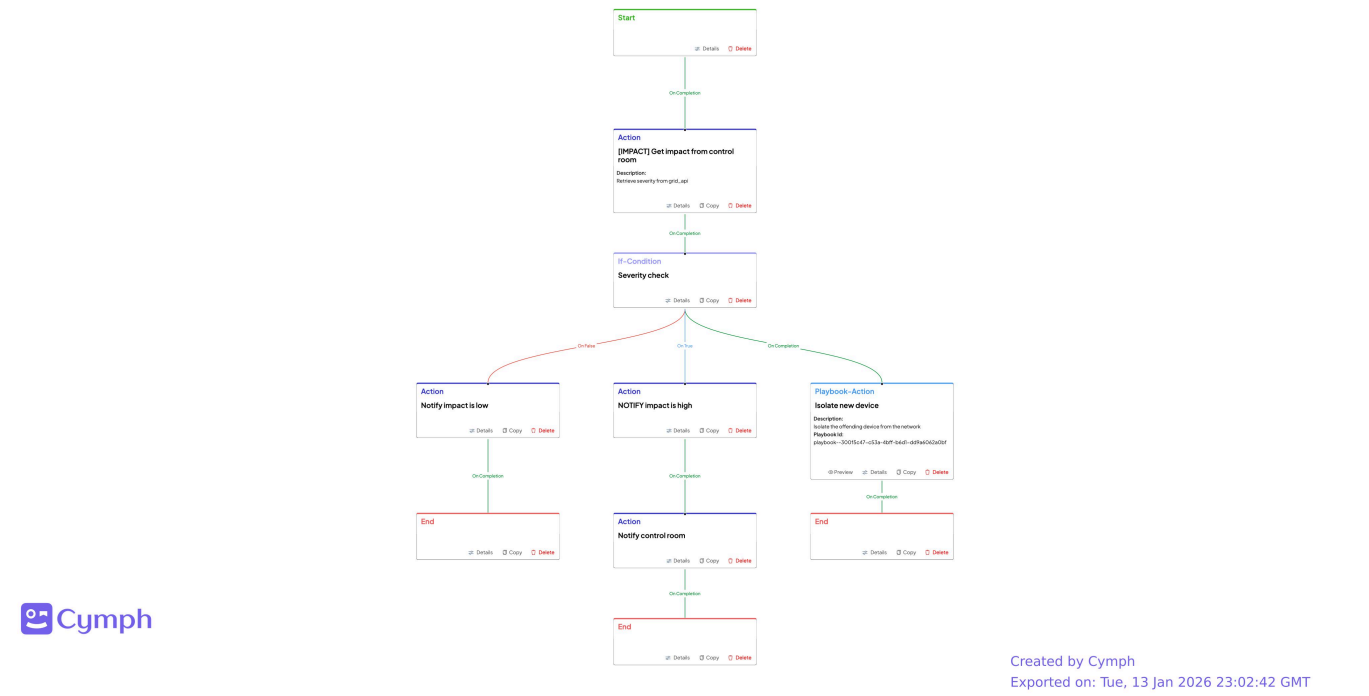
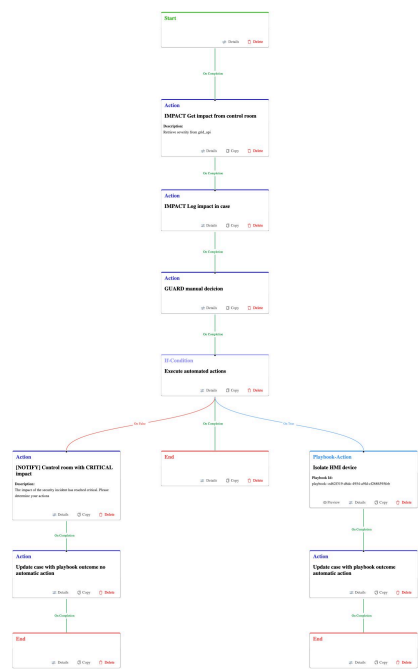


Fig. 11. OPNSense firewall rule playbook



Created by Cymph  
Exported on: Tue, 13 Jan 2026 23:03:13 GMT

Fig. 12. HMI isolation playbook with GUARD as HITL step

APPENDIX B

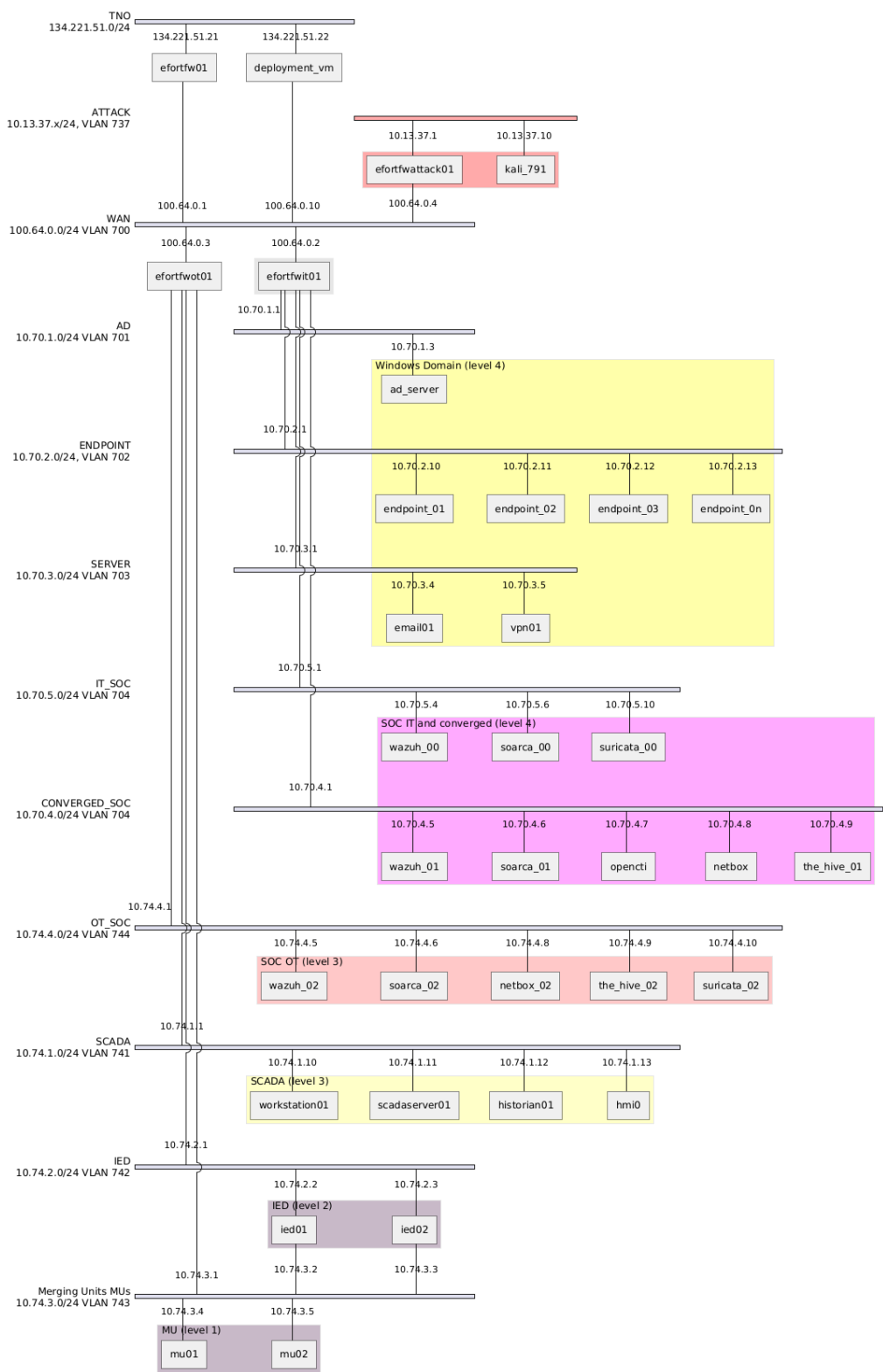


Fig. 13. Full architecture of the PoC environment