Network Security Monitoring for the Electric Sector

Gergő Gyebnár[1], Ferenc Hegedűs[2], Imre Négyesi[3] and Sándor Magyar[4]

[1] Ludovika University of Public Service, H-1083 Budapest, 2 Ludovika tér, gyebnar.gergo@uni-nke.hu

[2] Black Cell Magyarország Ltd., H-1027Budapest, Fekete Sas u. 2, ferenc.hegedus@blackcell.io

[3] Ludovika University of Public Service, H-1083 Budapest, 2 Ludovika tér, negyesi.imre@uni-nke.hu

[4] Ludovika University of Public Service, H-1083 Budapest, 2 Ludovika tér, magyar.sandor@uni-nke.hu

Abstract: *The increasing digitalization and interconnectivity of the electric power sector creates new cybersecurity risks that threaten the safety and reliability of the energy supply. Network Security Monitoring (NSM) plays a crucial role in the early detection of threats and the enhancement of system resilience. This research focuses on improving network monitoring systems within electrical substations and microgrid environments. It examines the effectiveness of tools based on protocol-specific analysis and anomaly detection, as well as network traffic mirroring techniques aimed at optimizing data collection and detection accuracy. The comparison of TAP, SPAN, and packet broker solutions reveals trade-offs between data fidelity, performance and integration complexity. The findings indicate that effective NSM implementation requires a context-aware architecture tailored to the specific characteristics of the infrastructure. This study contributes to the modernization of cybersecurity within the energy sector, through targeted technological solutions and best practices, that are adapted to the sector's unique requirements.*

Keywords: Cybersecurity, Network Security, Suricata, Zeek, IDPS

1 Introduction

Industrial Control Systems (ICS) are designed to manage critical industrial processes, including power generation, water utilities, oil and gas, and transportation systems. Historically, ICS lacked built-in security features since these devices were not planned to ever be connected directly to the internet. These

systems are often based on outdated technologies that were not designed to meet today's cybersecurity requirements. [1] Over the past two decades, advancements in remote management capabilities driven by the increasing use of the Internet have led ICS to become interconnected with Information Technology (IT) systems. This integration, known as the convence of ICS or Operational Technology (OT) and IT in the era of Industry 4.0 has introduced numerous vulnerabilities from IT systems. [2][3] Cyber-attacks, previously confined to IT systems, have begun targeting ICS. These attacks have caused significant environmental, safety, societal and physical harm, to ICS asset owners, governments and the public. One of the earliest examples of an ICS cyber-attack is the Stuxnet malware incident, which targeted Iran's nuclear facility. Stuxnet specifically infected programmable logic controllers (PLCs), leading to the destruction of approximately 1000 centrifuges, integral to Iran's nuclear program. [4] Another notable case occurred in 2015 when the BlackEnergy3 malware infiltrated Ukraine's power grid, resulting in power outages that affected nearly a quarter-million customers [5], also in May 2021, a cyber-attack struck the Colonial Pipeline, responsible for supplying 45% of fuel consumed along the U.S. East Coast. [6] This attack forced the company to suspend operations for several days, leading to fuel shortages, price increases, and widespread panic buying. ICS differ from traditional IT systems due to their distinct performance and reliability requirements. These systems operate in real-time, where delays or disruptions in control data – such as latency or jitter – are unacceptable. Such issues are often the primary contributors to ICS-related incidents. Furthermore, if ICS alerting mechanisms or Safety Instrumented Systems (SIS) fail or are compromised, critical incidents may go undetected and unmitigated. [7] In such cases, operators might not even receive the necessary alerts on their dashboards, leaving the system vulnerable. [8]. Special protocols used in industrial automation were developed for efficiency, reliability, and real-time operation, so all unnecessary features, including security elements, were often omitted. As a result, these protocols pose security risks to users. [9] Since more than 250 unique protocols are used in ICS environments, including specific processes and equipment, it is advisable to analyze them in a sector-specific manner. This paper discusses network monitoring capabilities in the control technology of electrical industry systems, with particular emphasis on applied protocols such as GOOSE (Generic Object-Oriented Substation Events), Manufacturing Message Specification (MMS), and IEC 104 (widely used in Europe, with DNP3 serving a similar role in North America), Modbus, and IT protocols.

Mass power outages not only cause political and social tensions, but also have psychological effects that influence the country's international reputation. [10] In the context of securing the electric sector against increasing cyber threats, this research aims to address challenges in network security monitoring specific to ICS used in electrical substations. This study investigates how network security monitoring systems can effectively detect and mitigate cyber-attacks that target ICS protocols in electrical substations.

The research objectives were:

RO1: To evaluate and demonstrate the deployment and effectiveness of network security monitoring tools, including protocol-specific analysis and anomaly detection.

RO2: To analyze and compare network traffic mirroring techniques and their integration with security monitoring frameworks to optimize data capture, detection accuracy, and resource utilization in electric sector microgrid environments.

Consequently, the research study has identified the following research questions to be addressed:

RQ1: How can network security monitoring systems effectively detect and mitigate cyber-attacks targeting ICS protocols in electrical substations?

RQ2: What are the challenges and best practices for implementing network traffic mirroring and data collection strategies to enable comprehensive security monitoring in electric sector microgrid testbeds?

This work aligns with the broader imperative to modernize energy network security through targeted technological solutions and best practices tailored to the unique requirements of the power sector.

2 Methods

The methodology for data harvesting involved capturing network traffic through network mirroring, which allows the passive duplication of data packets from the ICS network without affecting normal operations. This mirrored traffic was then subjected to detailed analysis using protocol parsers, such as those implemented in tools like Zeek, to extract meaningful protocol-specific information from raw network data. Zeek was chosen because it is a hybrid, signature- and anomaly-based Intrusion Detection System (IDS), whose analysis engine converts collected network traffic into various events [11].

The MMS, GOOSE and IEC 60870-5-104 (IEC 104) protocols were selected for the publication because they play a key role in network security monitoring and substation communication in the electricity sector. MMS is a communication protocol used in industrial control systems that enables data exchange and control between intelligent electronic devices (IEDs), facilitating the interoperability of equipment from different manufacturers in the field of substation automation [12]. In contrast, the GOOSE protocol provides extremely fast, event-driven data transfer, enabling real-time transmission of protection commands and status information, increasing system responsiveness and reliability [13]. IEC 60870-5-

104 (IEC 104) is used for remote control and monitoring of power systems, using TCP/IP-based communication for remote control of substations and ensuring seamless integration with other protocols [14] such as MMS and GOOSE.

Protocol parsing enabled the identification and decoding of critical communication elements within MMS, IEC 104, and GOOSE protocols, including vendor parameters, control commands, and message types. The parsed data was further analyzed using machine learning algorithms and signature-based detection rules within Security Information And Event Management (SIEM) systems, facilitating anomaly detection by establishing baselines and flagging deviations such as unexpected device identifiers or unauthorized control messages. This approach provided a comprehensive understanding of normal and potentially malicious behavior in ICS communications, supporting effective monitoring and incident response.

The methodology for data harvesting involved capturing network traffic through network mirroring, enabling passive collection of communication data from the ICS environment without disrupting operations. The mirrored traffic was then analyzed through protocol parsing using tools like Zeek, which extract detailed protocol-specific information from raw data packets. This parsing allowed the identification of key attributes such as vendor parameters, control commands, and message types across MMS, IEC 104, and GOOSE protocols.

Subsequent data analysis employed machine learning algorithms and signature-based detection within SIEM platforms, to establish behavioral baselines and identify anomalies, such as unusual vendor identifiers, unauthorized parameter modifications, or new devices on the network. This combined approach of network mirroring and protocol parsing facilitated effective detection of malicious activities by uncovering deviations from normal communication patterns.

3 Results

3.1 Architecture

This section describes the test bed environment in which the Microgrid has been built, including its physical characteristics and the incorporation of the IEC 62443-4-2 standard for industrial automation security.

3.1.1 Microgrid

The test environment consists of a previously built Microgrid that was extended with a substation. The test bed has been built in accordance with the IEC 62443 standard, which focuses on security for industrial automation and control systems.

The core Microgrid includes a PCB, on which components are applied using a screen-printing technique. The system has three input units: the grid supply, the wind turbine, and the solar panel. Each is connected to a main switch, a power unit, and a power meter. These three energy sources charge the central battery unit, which supplies electricity to the lighting of two barracks, represented by two conventional bulbs to illustrate consumption in an understandable manner.

The Microgrid also contains an IED, which acts as a microcontroller. Its role is to orchestrate the charging process and overall energy management. This microcontroller is equipped with software designed to manage inputs from various energy sources, such as solar panels, wind turbines, and grid supplies, ensuring the optimal charging of the central battery unit.

Additionally, a PLC, equipped with both digital and analog cards, serves as a versatile and efficient component in the Microgrid testbed environment. Its primary function is to provide reliable control and automation of Microgrid operations, enabling the integration and management of various energy sources, storage solutions, and load demands. With the ability to handle both digital (on/off) and analog (variable) signals, the PLC can monitor and control a wide range of devices and parameters.

Other minor modules and features contribute to the overall functionality of the Microgrid. A web server acts as the backbone for data management and the user interface, hosting applications that collect, process, and display data from the Microgrid while facilitating remote monitoring, control, and optimization of testbed operations. The operator workstation serves as the central hub for human operators, equipped with software tools for system monitoring, data analysis, and decision-making. This is where strategies are formulated and deployed, leveraging data provided by the web server. A network switch manages data flow within the Microgrid network, ensuring efficient communication between devices, sensors, and control systems while supporting network segmentation for improved performance and security. Finally, a firewall protects the Microgrid's digital infrastructure from external threats and unauthorized access, ensuring that only legitimate communication and control commands pass through to the Microgrid components. [15]

Since one of the main objectives of this paper is to understand network traffic in electrical substations, access to relevant traffic data is required. To achieve this, we established a partnership with Prolan Power cPlc, which installed the necessary virtual machines on Proxmox, the hypervisor managing the entire testbed. The two deployed devices play a crucial role in simulating electric sector-specific network traffic – one HMI and one substation simulator. With these devices, we were able to generate IEC 104, MMS, and GOOSE traffic.

The HMI is a web application. In its dedicated environment, alongside the application’s backend, an additional service runs to handle data collection and

protocol conversion. These two components communicate internally within the system (localhost) using a custom protocol over TLS.

Non-local connections, which extend beyond the HMI system, typically transmit data to the substation data collector using the IEC 60870-5-104 protocol. The data collector then communicates with the simulator using one of the previously mentioned protocols, including IEC 60870-5-104, MMS, GOOSE, and Modbus.

3.1.2 Network Security Monitoring

The network detection ecosystem can be divided into two major components, the Network Security Monitoring (NSM) system and the log management platform or SIEM. By definition, an NSM is a combination of hardware and software designed to perform data collection, detection, and analysis. Within the NSM, various tasks can be executed. For data collection, it can capture PCAP files, collect NetFlow data, generate Protocol-Specific Traffic Reconstruction (PSTR) data from PCAP files, or produce throughput graphs using NetFlow data. For detection, it can perform signature-based, anomaly-based, and reputation-based detection. Additionally, it can identify the usage of known-bad PKI credentials using custom tools or detect potentially malicious strings in PDF files with specialized software.

To effectively analyze ICS protocols, implementing an Intrusion Detection and Prevention System (IDPS) and a protocol analyzer is essential. Proper planning for deployment and maintenance is crucial, as the NSM plays a key role in the network security ecosystem by facilitating the collection process. Without carefully designed and well-implemented sensors, efforts to detect network threats may be undermined or create a false sense of security. When designing sensor deployment within a network, three primary architectural considerations must be addressed: hardware resources, proper sources of the network traffic, and the tools installed on the sensors for data collection and detection.

3.1.3 Hardware resources

In production environments dedicated physical hardware is recommended, especially when monitoring high volumes of traffic, to prevent resource competition. While NSM can be virtualized, it is essential to allocate sufficient resources to ensure optimal performance. In the Microgrid we used Ubuntu VMs.

CPU requirements are particularly high for Suricata and Zeek, both of which are CPU-intensive. The more traffic being monitored, the more CPU cores are needed. A rough estimate is approximately 200Mbps per Suricata or Zeek worker. For instance, if a fully saturated 1Gbps link is being monitored using Suricata for NIDS alerts and Zeek for metadata, at least five Suricata workers and five Zeek workers are required. This setup would necessitate at least ten CPU cores dedicated to Suricata and Zeek In environments with high traffic and limited CPU cores, using

Suricata for both alerts and metadata can eliminate the need for Zeek, improving CPU efficiency.

RAM usage depends on several factors, including the enabled services, the type and volume of monitored traffic, and the acceptable level of packet loss for the organization. To achieve the best performance, RAM should be over-provisioned to allow for the complete disabling of swap. A rough guideline for RAM allocation assumes the use of Suricata, Zeek. A quick evaluation of NSM in a virtual machine requires a minimum of 12GB of RAM, though more is preferable. For production deployment in a small network (100Mbps or less), at least 16GB is recommended, while medium networks (100Mbps–1000Mbps) require 16GB–128GB or more. Large networks (1000Mbps–10Gbps) should plan for 128GB–256GB or more. When purchasing a new server, maximizing RAM is advised, as additional memory improves performance and is relatively inexpensive.

Storage capacity is a critical factor for NSM deployments. For example, monitoring a link with an average of 50Mbps results in approximately 540GB of data per day. The required storage capacity depends on the number of days of PCAP data that need to be retained for forensic investigations. The more disk space available, the greater the PCAP retention, which enhances post-incident analysis capabilities. Investing in ample storage is recommended, as disk space is relatively inexpensive and directly impacts the system's ability to store and analyze historical traffic data. [16].

In our environment we allocated 12GB of RAM, 6 Vcores and 250 GB of storage.

3.1.4 Mirroring strategies

The fundamental task of network signatures is to identify malicious and suspicious patterns in network traffic. [17] This can be achieved on two fronts: external-facing and internal-facing traffic. On perimeter security devices, such as Intrusion Prevention Systems (IPS), signatures are typically deployed in IPS mode, requiring a more rigorous selection of the ruleset to avoid hindering legitimate processes. Another solution, which has become almost mandatory as an extension of network security, is the inspection of internal network traffic. It is worth noting that we differentiate between North-South and East-West traffic. North-South traffic typically refers to traffic that passes through the firewall/switch, while East-West traffic is typically within, for example, a virtualization cluster. Both data sources are necessary since in the case of North-South traffic, there may be no visibility for techniques such as lateral movement.

Network traffic mirroring is essential for network monitoring. [18] It involves duplicating network traffic and forwarding it to a monitoring tool (to the NSM). There are three primary approaches to traffic mirroring strategies – a network tap, Switched Port Analyzer (SPAN) ports, and packet brokers. Each method has its own

advantages and limitations, making it crucial to choose the right approach based on the requirements.

Network tap is a hardware device placed between two network devices (such as a switch and a router) to passively copy all traffic without affecting network performance. TAPs operate at Layer 1 (Physical Layer) and come in various forms, including active TAPs (which require power) and passive TAPs (which do not require power). Since TAPs are dedicated hardware solutions, they introduce minimal latency and do not drop packets under high loads. They can capture both the ingress (incoming) and egress (outgoing) traffic simultaneously without packet loss and may be used in legislative cases since most courts accept their integrity. Taps require physical installation between devices, which can be costly and complex in large networks. Each TAP is dedicated to a specific network link, meaning multiple TAPs are needed for broader visibility. We used a SharkTap Gigabit Network Sniffer in order to get the traffic from and to the PLC.

A SPAN port, also known as port mirroring, is a feature found on manageable network switches that duplicates traffic from one or more ports to a designated monitoring port. It is a software-based approach that allows network engineers to capture packets without requiring additional hardware. It can be configured to mirror specific traffic based on VLANs, source/destination ports, or protocols. This option may drop the "bad packets"; however, it is the most widely used solution for traffic analysis. We used OpenSwitch in the Proxmox environment, therefore we are able to get not just the North-South but, the East-West traffic as well. This is a highly considerable methodology, to mirror the hypervisors internal traffic as well, not just sniffing from the physical switches.

A packet broker (is an advanced traffic mirroring solution that aggregates, filters, and distributes traffic to multiple monitoring tools. It sits between TAPs, SPAN ports, and monitoring devices, ensuring that each tool receives the right data without being overloaded. It can filter and aggregate traffic, sending only relevant packets to monitoring tools, reducing unnecessary load, and can handle large-scale deployments across multiple network segments.

3.1.5 Tools

In order to gain visibility into enterprise IT and electric-specific protocol stacks, two major topics must be addressed – the protocol parser and the IDPS. It should be noted that since the system operates on mirrored traffic, the prevention function is out of scope. The response options are discussed later in this paper.

Protocol analysis

One highly recommended tool for protocol parsing and analysis is Zeek, formerly known as Bro. Zeek is not a traditional signature-based IDS; while it does support standard IDS functionality, its scripting language enables a much broader range of approaches to identifying malicious activity. It is a passive, open-source network

traffic analyzer widely used by operators to support investigations of suspicious or malicious activity.

One of Zeek's key strengths is its extensive set of logs that describe network activity in detail. Regarding the enterprise protocol stack, Zeek captures HTTP sessions, including requested URIs, key headers, MIME types, and server responses; DNS requests with replies; SSL certificates; key content of SMTP sessions; and much more. By default, Zeek writes this information into well-structured tab-separated or JSON log files, making it suitable for post-processing with external software. In our environment, we process this data within the NSM, where it is analyzed and presented for querying in the SIEM system. It also offers a wide range of built-in functionalities for analysis and detection. These include extracting files from HTTP sessions, detecting malware by interfacing with external registries, reporting vulnerable software versions seen on the network, identifying popular web applications, detecting SSH brute-force attacks, validating SSL certificate chains, and much more. Furthermore, Zeek is a fully customizable and extensible platform for traffic analysis. It provides users with a domain-specific, Turing-complete scripting language to define custom analysis tasks. All default Zeek analyses, including logging, are implemented via scripts –no specific analysis is hardcoded into the system's core. [19]

While Zeek can be used for protocol analysis, the actual parsing is handled by a Zeek plugin called Spicy. Spicy itself is application-independent, but its seamless integration into Zeek has been a key development goal. Historically, using Spicy parsers with Zeek required an external Zeek plugin, but since Zeek version 5.0, built-in Spicy support has been included. This allows users to directly add new protocol, file, and packet analyzers to Zeek through Spicy without writing additional code. [20]

Spicy is a powerful parser generator that simplifies the creation of robust parsers for network protocols, file formats, and other data structures. Its integration with Zeek enables the development of custom Zeek analyzers for protocols, packets, and files. This capability is particularly valuable for industries with specialized communication protocols, such as the electric sector, where protocols like IEC 104, MMS and GOOSE are essential for substation automation and Supervisory Control and Data Acquisition (SCADA) communications.

By leveraging Spicy within Zeek, these electric-sector-specific protocols can be parsed and analyzed effectively. GOOSE, a critical protocol for real-time protection and control in substations, can be decoded to monitor abnormal messaging patterns or potential cyber threats. MMS, used for communication between SCADA systems and substations, can be analyzed to detect unauthorized access attempts or protocol anomalies. IEC 104, which extends IEC 101 for remote control over TCP/IP networks, can be inspected for suspicious activities, misconfigurations, or malicious command injections. Each of these protocols has distinct structures that must be accounted for in the parsing process.

GOOSE is an Ethernet-based protocol using the ISO/IEC 8802-3 (Ethernet) data link layer. It carries time-sensitive messages encoded in ASN.1 (Abstract Syntax Notation One) and uses Generic Substation Events (GSE) for peer-to-peer communication. GOOSE messages are encoded in ASN.1 using BER (Basic Encoding Rules). The parser needs to extract critical fields such as, AppID (Application Identifier), GoID (GOOSE Identifier), Timestamp, StNum (State Number), SqNum (Sequence Number).

MMS operates over TCP/IP using ASN.1 encoding with ACSE (Association Control Service Element) to establish and manage SCADA communication between IEDs and control centers. MMS messages are also ASN.1-encoded and transported via TCP. Parsing MMS involves, Session and Presentation Layer parsing ACSE (Association Control Service Element) decoding, extracting MMS service requests and responses.

IEC 104 extends IEC 101 over TCP/IP and follows a structured Application Protocol Data Units (APDU) format with Type Identifiers (TIs) for SCADA telemetry and control operations. It uses APDUs with TIs that determine the message type. Each APDU consists of Start Byte (0x68); Length; Control Field Information Objects (carrying telemetry data like analog values, digital inputs, etc.)

After defining Spicy parsers, they must be integrated with Zeek to generate events and logs. Spicy parsers are compiled into High-Level Typed Objects (HLTO) and loaded into Zeek with a .spicy file that links the parser to network traffic. Once Spicy parsers extract protocol fields, Zeek scripts can generate structured logs that can be integrated in Elastic via the native Zeek connector. Once logs have been on-boarded it can use the extracted data for advanced monitoring.

Intrusion detection system

IDSs play an essential role in monitoring and securing network traffic within substations. [21] The two most prominent IDPS engines are SNORT and SURICATA. Typically, SNORT is deployed for perimeter IPS tasks and is integrated into major firewall vendor appliances such as Sophos and FortiGate. In contrast, SURICATA is primarily used as an internal traffic IDS, although the roles can sometimes be reversed. Both solutions are open-source and rely on rule-based detection and Deep Packet Inspection (DPI) to identify malicious activity within network traffic.

SURICATA offers several advantages over SNORT. Its native multi-threading enables significantly higher performance and can be further accelerated using graphical computing capacity (CUDA). Another advantage is its ability to store network traffic as PCAP files under specific conditions, allowing for deeper forensic analysis. The tool produces rich JSON-formatted event logs (EVE logs), which are particularly useful for NSM. These logs can be seamlessly consumed by Elastic in our environment thanks for the native connector, but other SIEM solutions may be used for threat correlation and analysis. SURICATA operates by

continuously monitoring incoming network traffic and comparing it against a predefined rule set. When traffic matches a rule, SURICATA triggers an alert, enabling security teams to swiftly respond to potential threats. SURICATA is built on the Extended Snort Language, offering enhanced flexibility and functionality. One of its standout features is its ability to extract files from protocols such as HTTP and SMTP, providing deeper insights into potential malware or data exfiltration attempts. Additionally, it integrates GeoIP and reputation-based analysis, allowing it to correlate network traffic with geographic locations and known threat intelligence sources.

By integrating SURICATA and Zeek from electric-sector-specific protocols such as GOOSE, MMS, and IEC 104, it can significantly enhance substation protection. Zeek extracts rich metadata from these protocols, enabling SURICATA to correlate its rule-based detection with deeper protocol analysis. For example, GOOSE messages contain state numbers and sequence numbers that should increment predictably—SURICATA can trigger an alert if Zeek identifies an out-of-sequence message or unauthorized GOOSE event injection. Similarly, MMS traffic between SCADA systems and IEDs can be monitored for unauthorized access attempts or protocol misuse, with SURICATA rules detecting malformed MMS packets, unauthorized MMS commands, or excessive failed authentication attempts. In the case of IEC 104, Zeek can extract key APDU information, and SURICATA can enforce rules to detect unauthorized SCADA commands, telemetry manipulations, or abnormal communication patterns.

The following example Suricata rule detects unauthorized MMS Write Requests:

alert tcp any any -> any 102 (msg:"Unauthorized MMS Write Command"; flow:established, to_server; content:"\x81"; offset:0; depth:1; content:"\x02\x01\x01"; distance:1; within:3;

pcre:"/writeRequest/"; sid:100002; rev:1;)

The rule inspects MMS packets directed at TCP port 102 (standard MMS port) and checks for a writeRequest pattern in the payload, indicating a possible unauthorized SCADA modification attempt.

If Zeek logs indicate that the same GOOSE event is repeatedly sent without a state number change, this suggests a possible replay attack. A SURICATA rule can be written to detect such anomalies by monitoring traffic for repeated GOOSE messages with the same StNum and SqNum values:

alert ether any any -> any any (msg:"GOOSE Replay Attack Detected"; ether proto 0x88b8;

flow:established; content:"\x00\x01"; offset:6; depth:2; detection_filter:track by_src,count 10, seconds 2; sid:100001; rev:1;)

This rule watches for ten identical GOOSE messages within two seconds, indicating a replay attack. Zeek can pre-filter and feed this data to SURICATA, reducing noise and focusing on relevant traffic.

Since Zeek extracts APDU control fields and TIs from IEC 104 traffic, Zeek is able to detect an unexpected control command (e.g., an ON command issued from an unrecognized source) and SURICATA can flag it:

alert tcp any any -> any 2404 (msg:"Unauthorized IEC 104 Control Command";

flow:established, to_server; content:"\x68"; offset:0; depth:1; content:"\x0F"; within:1; distance:2; pcre:"/actcon|actterm/"; sid:100003; rev:1;)

The rule above inspects IEC 104 packets on TCP port 2404, looking for control commands (actcon or actterm) that should only originate from authorized sources. If an attacker attempts to send rogue commands, the alert is triggered.

By combining Zeek's deep protocol inspection with SURICATA's high-speed rule matching, we are able to detect threats targeting substations with GOOSE anomaly detection. If Zeek logs indicate an unexpected sequence number reset, SURICATA can alert or block the traffic. In case of MMS unauthorized commands, if Zeek sees an MMS write request from an unknown source, SURICATA can trigger intrusion detection alerts or drop packets. Regarding IEC 104 command injection, Zeek extracts SCADA control commands, and SURICATA flags unauthorized actions to prevent cyber-physical attacks.

3.1.6 SIEM

To effectively analyze security events generated by the NSM solution, a log manipulation or SIEM system is required. The sheer volume of data generated by network traffic monitoring tools like Suricata and Zeek necessitates an efficient and scalable system to process, store, and analyze these logs in real time. After evaluating several options, we decided to utilize Elasticsearch as our core log management platform due to its scalability, performance, and powerful search capabilities.

Elasticsearch is a distributed search and analytics engine that excels in handling large volumes of data, making it an ideal choice for environments with high data throughput, such as those found in NMS. One of the main reasons for selecting Elasticsearch is its ability to scale horizontally, allowing it to handle the growing volumes of log data without compromising performance. This scalability ensures that as the network infrastructure expands and generates more data, Elasticsearch can efficiently scale to meet these demands without significant reconfiguration. It integrates with native collectors for Suricata and Zeek, that we used in the NSM. These integrations provide a streamlined approach for ingesting data from both tools into Elasticsearch, simplifying the process of storing and analyzing security-

related logs. Suricata and Zeek produce large amounts of network traffic data, including intrusion detection alerts, protocol metadata, and other critical network activity logs. By utilizing Elasticsearch's native collectors, we ensure that these logs are efficiently ingested and indexed, allowing for fast and powerful searches across massive datasets. Another compelling reason for choosing Elasticsearch is its built-in support for Machine Learning. Machine learning capabilities in Elasticsearch enable the automatic detection of anomalies and patterns in network traffic, which is vital for identifying potential security incidents or emerging threats. Machine learning models can be trained to recognize unusual patterns in data, helping security teams identify subtle threats that might not be detectable through traditional signature-based methods. These capabilities allow for proactive threat hunting and automated alerts, based on deviations from established baselines, improving the overall security posture.

3.2 Attacking scenarios

As previously mentioned, most OT protocols were developed at a time when security was not a major consideration, their design predates current threats and IT-OT convergence. The main emphasis was on reliability and real-time control and the integration with IT networks was unforeseen. ICS networks were typically isolated and often air-gapped. The different protocols used in these networks frequently lack basic security features, and the general lack of encryption makes them vulnerable to a variety of attacks. Today, with everything being connected, a new challenge emerges to secure them. The following representative attacks, categorized by protocol, serve to demonstrate this scenario.

3.2.1 Manufacturing Message Specification

To present the vulnerable nature of the Manufacturing Message Specification (MMS) protocol, we developed a realistic attack scenario. In this scenario, a malicious actor connects a rogue device to the ICS network. Typically, physical security systems detect physical intrusions, however, most substations are unguarded, resulting in a variable timeframe between the intrusion and security personnel arriving at the substation. Overcoming physical barriers designed to prevent intrusions makes it possible to connect a rogue device to the ICS network, especially if the attack takes place in a coordinated manner affecting multiple substations. A newly introduced rogue device, if carefully hidden, can remain active long enough to disrupt operations. As part of this attack, using the newly introduced rogue device, the attacker conducts reconnaissance by querying objects on a targeted device. Following the initial reconnaissance, the attacker discovers a promising object on the targeted device. First, an attempt is made to read the object's value. This attempt being successful, the attacker then tries to write a new value to the object. Since the MMS protocol lacks authentication mechanisms, the

attacker can read and write values. This capability can potentially cause significant damage, ranging from equipment malfunctions and service outages to, in severe cases, endangering human life. For a clearer understanding, we can break down this attack into distinct steps and analyze them within the context of the MITRE ATT&CK for ICS framework. Introducing a rogue device capable of ICS communication maps to MITRE ICS technique T0848 (Rogue Master), falling under the Initial Access tactic. Querying objects on devices within the industrial environment corresponds to MITRE ICS technique T0888 (Remote System Information Discovery), part of the Discovery tactic. Modifying a parameter aligns with MITRE ICS technique T0836 (Modify Parameter) categorized under the Impair Process Control tactic.

Effective methods for detecting these activities are presented in the following section.

3.2.2 IEC 60870-5-104 (IEC 104)

With the rogue device still present, the attacker can further explore the network and observe the communication between various industrial devices. Upon noticing the presence of IEC 104 communication on the network, the malicious actor attempts to issue a control command to a targeted device using a parameter value likely to cause significant damage. If built-in protection does not prevent this action, the consequences could be severe. In an effort to further disrupt operations, the attacker develops a simple script designed to inject Stop Data Transfer (STOPDT) messages into the existing IEC 104 communication. This action prevents any querying or control of the affected devices.

Mapping these activities to the MITRE ATT&CK for ICS framework provides better insight into the attack. [22] Issuing unauthorized control commands aligns with T0836 (Modify Parameter) which was also relevant in the previously discussed MMS scenario. Employing the script to inject STOPDT messages and disrupt communication corresponds to technique T0813 (Denial of Control), which falls under the Impact tactic.

3.2.3 GOOSE

With the rogue device still active on the network, the adversary may analyze traffic and can identify GOOSE messages being exchanged between IEDs . Recognizing that GOOSE is used for time-critical control operations such as circuit breaker status and protection relays, the attacker crafts and transmits forged GOOSE messages with false control commands. By mimicking a legitimate publisher IED and injecting a false trip signal, the attacker can trigger unnecessary protective actions—such as opening a circuit breaker—leading to a loss of power in part of the grid. If no robust authentication or message integrity validation is in place, the system may accept and act on the malicious command. To prolong the disruption, the attacker

can move forward to inject periodic false GOOSE messages, creating instability and making it difficult for operators to distinguish between real and forged events. Mapping this attack to the MITRE ATT&CK for ICS framework, the injection of unauthorized control signals corresponds to T0836 (Modify Parameter), as it manipulates the control logic of the target system. The repeated false signaling designed to degrade or halt operation aligns with T0813 (Denial of Control), supporting the Impact tactic by interfering with the normal operation of substations.

3.3 Detections

Effective detection design requires aligning the method with the particular attack behavior and available data. While signature-based detection works in certain cases, analyzing protocol parser data for specific patterns or anomalies is often more suitable. We found the following detections to be effective for the attack scenarios we designed.

3.3.1 Manufacturing Message Specification

A newly introduced MMS-capable rogue device will have a defined vendor parameter. If this vendor parameter differs from those typically observed in the environment, it can be flagged by anomaly detection, highlighting the significance of machine learning. Due to the nature of machine learning, it is not required to have and maintain an asset inventory, our machine learning jobs can learn a baseline and can alert for deviations, like a new vendor appearing in our environment. All unsuccessful read and write attempts generate specific error responses from the targeted devices. These error messages can be detected using network signatures. An unsuccessful write request, for example, will result in a specific pattern, which can be used to create a signature such as:

alert tcp any [102:110] -> any any (msg:"MMS: Invalid Object Write Attempt"; content:"|a5 03 80 01 0a|"; endswith; classtype:misc-activity; sid:124; rev:1;)

3.3.2 IEC 60870-5-104 (IEC 104)

Regarding the IEC 104 protocol the malicious actor decided to issue a control command. Detecting control commands from a source that has not previously been observed issuing commands is possible but requires both a protocol parser and an appropriately configured anomaly detection algorithm monitoring the extracted network data. The machine learning algorithm can analyze incoming data to establish a baseline profile of which sources normally issue control commands. Any deviation from this learned baseline can then trigger an alert.

Concerning the introduced malicious script, detection is also possible. STOPDT messages themselves are not inherently suspicious, as they are part of normal

protocol operation. However, a sudden increase in their volume or frequency can indicate malicious activity and should prompt an investigation. Individual STOPDT messages can be identified with basic signature matching. A simple signature to recognize the pattern of a STOPDT message could look like this:

> *alert tcp any any -> any any (msg:"IEC-104: STOPDT (Stop Data Transfer)"; content:"|68 04 13 00 00 00|"; endswith; classtype:protocol-command-decode; sid:125; rev:1;)*

The number of SURICATA alerts required to trigger a SIEM alert can be tuned to our environment.

3.3.3 GOOSE

Regarding the GOOSE protocol, the attacker's method involved injecting false control messages into the substation network. While GOOSE messages are inherently trust-based and designed for high-speed operation, detecting such malicious activity is possible by monitoring for anomalies in the network layer.

One effective detection approach is to track the appearance of new MAC vendor or previously unseen IP addresses within the substation's VLAN. GOOSE communications are typically limited to a known set of IEDs with static MAC/IP mappings. The sudden appearance of a device sending GOOSE messages—especially with a MAC address from an unrecognized vendor – can be an early indication of malicious activity. This method requires maintaining an inventory of known device identifiers and continuously correlating incoming traffic against this trusted list. A detection rule might include logic such as alert on any GOOSE message originating from a MAC address that is not in the approved inventory or trigger an alert if the Organizationally Unique Identifier (OUI) of the MAC address does not match known vendor prefixes associated with approved IEDs. The following sample signature that could be used to match GOOSE messages and flag unknown MAC addresses (pseudocode):

> *alert ethernet any any -> any any (msg:"GOOSE: Unknown MAC Vendor"; ether[6:3] != {00:1A:4B, 00:0C:15, 00:1D:9C}; classtype:anomaly-detection; sid:201; rev:1;)*

Similar profiling can be applied to detect new IP sources attempting to communicate on the control VLAN.

3.3.4 Quantitative evaluation

In quantitative evaluation, the effectiveness of the proposed monitoring approach can be interpreted through operational security metrics commonly used in Security Operations Centers (SOC), namely Mean Time to Detect (MTTD), Mean Time to Acknowledge (MTTA), Mean Time to Respond/Recover (MTTR), and the derived dwell time. In the presented architecture, dwell time, defined as the period between

initial compromise and remediation can be reduced by improving detection and triage efficiency. While MTTA can be directly measured and enforced through Service Level Agreements (SLA), MTTD and MTTR are influenced by the quality of detections and the integration of NSM with SIEM workflows. The combination of protocol-aware detection (Zeek) and rule-based alerting (Suricata) contributes to lowering MTTD by enabling earlier identification of anomalous ICS-specific behaviors. MTTR is improved through structured alerting and enriched context, allowing faster analyst response. Although precise numerical values depend on deployment scale and operational maturity, the framework supports measurable improvements in dwell time by systematically optimizing these metrics.

The quantitative evaluation of detection performance, Receiver Operating Characteristic (ROC) analysis. By adapting ROC curves to a specific use case, it becomes possible to evaluate multiple variations of detection logic or overlapping detections of the same activity. This approach helps determine whether incremental changes in detection logic provide sufficient performance improvements to justify the additional workload imposed on SOC analysts when triaging false positives. Since we have tested with specific conditions this approach not affected, since all attacks/detect pairs are a true positive.

Regarding system latency, it is important to distinguish between operational technology (OT) constraints and monitoring system performance. Electrical substations often rely on communication technologies operating at microsecond or even nanosecond levels, particularly for protection mechanisms such as GOOSE messaging. However, the proposed monitoring approach is passive and operates out-of-band via mirrored traffic, ensuring that it does not introduce latency into control processes. From an operational perspective, the definition of “real-time” monitoring in the context of energy sector operations does not necessarily align with sub-second control system performance. While protection and control mechanisms in substations operate at microsecond or even nanosecond levels, cybersecurity monitoring follows a different timescale driven by operational requirements. In practice, real-time security monitoring is typically interpreted within an operational window of several minutes. In this study, the achieved analysis and alerting latency remains within a 5-minute threshold, which satisfies practical real-time requirements regarding Department of War definition

4 Discussion

The results of this study demonstrate that network security monitoring, when adapted to the specific characteristics of industrial control systems in the electric sector, can provide a meaningful improvement in both visibility and detection capability. Rather than relying on traditional IT centric approaches, the combination of protocol aware analysis and behavioral detection proved to be essential in

addressing the unique constraints of substation environments, such as deterministic communication patterns, limited protocol diversity, and strict availability requirements. With respect to RQ1, the findings confirm that effective detection of cyber-attacks targeting ICS protocols is achievable when monitoring systems incorporate deep protocol understanding. The use of protocol parsers for MMS, IEC 104, and GOOSE enabled the extraction of semantically rich information from network traffic, which is not accessible through conventional packet inspection alone. This enriched visibility allows security mechanisms to move beyond simple signature matching and instead evaluate the intent and context of communications. The integration of Zeek-based parsing with Suricata rule evaluation demonstrated that combining metadata-driven analysis with high-performance detection engines can significantly improve detection fidelity while maintaining operational efficiency.

At the same time, anomaly detection based on learned baselines proved to be particularly valuable in ICS environments, where communication patterns are typically stable and predictable. Unlike more dynamic IT networks, substations exhibit relatively static device roles, vendors and communication flows. This makes deviations strong indicators of potential compromise. The application of machine learning within the SIEM environment enabled the identification of such deviations without requiring a fully predefined asset inventory, which is often difficult to maintain in legacy or heterogeneous ICS deployments. However, it is important to note that the effectiveness of anomaly detection depends heavily on the quality and duration of the training phase, as well as on the stability of the monitored environment and can hardly be interpreted as a reactive alert, but, in fact is proactive.

Regarding RQ2, the study highlights that data collection is not merely a technical prerequisite, but a critical design decision that directly influences detection outcomes. The comparison of traffic mirroring techniques revealed that there is no universally optimal solution. Instead, each approach introduces trade-offs between completeness, performance, and deployment complexity. TAP-based monitoring provides the highest fidelity and reliability, ensuring that no packets are lost even under high load conditions, which is particularly important for forensic analysis and precise anomaly detection. However, its deployment complexity and cost may limit scalability in larger or distributed infrastructures.

In contrast, SPAN-based mirroring offers flexibility and ease of deployment, especially in virtualized environments such as the presented microgrid testbed. Its ability to capture both North-South and East-West traffic is a significant advantage for detecting lateral movement, which is increasingly relevant in ICS threat scenarios. Nevertheless, the potential for packet loss and selective filtering introduces uncertainty into the monitoring process, which may impact detection accuracy. Packet brokers, while offering advanced filtering and aggregation capabilities, introduce additional architectural complexity and are typically justified only in large-scale or highly segmented environments. Resource allocation plays a

decisive role in the effectiveness of NSM deployments. The performance characteristics of tools such as Suricata and Zeek require careful planning of CPU, memory, and storage resources. Insufficient provisioning can lead to packet loss, delayed processing, or incomplete analysis, ultimately undermining the reliability of the monitoring system. This is particularly critical in ICS environments, where missed events may correspond to safety-relevant incidents.

The results suggest that over-provisioning, especially in terms of memory and storage, is a practical strategy to ensure stability and support retrospective analysis.

References

[RC1] megjegyzést írt:

[1] WELANDER, Peter. Securing legacy control systems. Control Engineering, 2009, 56.7: 26-31.

[2] Paredes, Ignacio, "IT/OT Convergence – Cybersecurity Beyond Technology." Paper presented at the Abu Dhabi International Petroleum Exhibition & Conference, Abu Dhabi, UAE, November 2020. doi: https://doi.org/10.2118/203093-MS

[3] MURRAY, Glenn, et al. Detection techniques in operational technology infrastructure. 2018.

[4] IEEESpectrum, The real story of stuxnet, https://spectrum.ieee. org/the-real-story-of-stuxnet, 2 (2013)

[5] ŠTEFKO, Róbert, et al. Cybersecurity Challenges in the Power Sector: Analysing Attacks on Electrical Grids and Substations. In: 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI). IEEE, 2025. p. 000459-000464.

[6] BEERMAN, Jack, et al. A review of colonial pipeline ransomware attack. In: 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW). IEEE, 2023. p. 8-15.

[7] NININ, Pierre; SALATKO, Cyrille; VALBOM, Jérémie. Safety status: an innovative concept for maintaining the safety integrity level of operational safety systems. International journal of safety and security engineering, 2018, 8.1: 139-149.

[8] KOAY, Abigail MY, et al. Machine learning in industrial control system (ICS) security: current landscape, opportunities and challenges. Journal of Intelligent Information Systems, 2023, 60.2: 377-405

[9] DRIAS, Zakarya; SERHROUCHNI, Ahmed; VOGEL, Olivier. Taxonomy of attacks on industrial control protocols. In: 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS). IEEE, 2015. p. 1-6.

[10] KAZANCI, Baybarshan Ali. The strategic importance of cyber security in electric energy policies. International Journal of Energy Economics and Policy, 2024, 14.4: 599-605.

[11] TIWARI, Asheesh, et al. Refinements in Zeek IDS. In: 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS). IEEE, 2022. p. 974-979.

[12] MAZUR, David C.; KAY, John A.; KREITER, James H. Benefits of IEC 61850 standard for power monitoring and management systems in forest products industries. In: Conference Record of 2013 Annual IEEE Pulp and Paper Industry Technical Conference (PPIC). IEEE, 2013. p. 69-75.

[13] LEÓN, Héctor, et al. Simulation models for IEC 61850 communication in electrical substations using GOOSE and SMV time-critical messages. In: 2016 ieee world conference on factory communication systems (wfcs). IEEE, 2016. p. 1-8.

[14] SHOBOLE, Abdulfetah Abdela; ABAFOGI, Motuma; COLAK, Ilhami. Practical Implementation of Multithreaded Communication Protocols in Modern Protection Relays. Electric Power Components and Systems, 2023, 1-15.

[15] GYEBNÁR, Gergő, Building an OT Security Microgrid Testbed, Academic And Applied Research In Military and Public Management Science 23: 3 pp. 5-19. , 15 p. (2024)

[16] Security Onion, Hardware Requirements

[17] BEAVER, Justin M.; SYMONS, Christopher T.; GILLEN, Robert E. A learning system for discriminating variants of malicious network traffic. In: Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop. 2013. p. 1-4.

[18] ZHANG, Jian; MOORE, Andrew. Traffic trace artifacts due to monitoring via port mirroring. In: 2007 Workshop on End-to-End Monitoring Techniques and Services. IEEE, 2007. p. 1-8.

[19] About Zeek, https://docs.zeek.org/en/master/about.html

[20] Zeek Integration, https://docs.zeek.org/projects/spicy/en/latest/zeek.html

[21] QUINCOZES, Silvio E., et al. A survey on intrusion detection and prevention systems in digital substations. Computer Networks, 2021, 184: 107679.

[22] BHOSALE, Pushparaj; KASTNER, Wolfgang; SAUTER, Thilo. Mapping ics vulnerabilities: prioritization and risk propagation analysis with MITRE ATT&CK framework and bayesian belief networks. In: 2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, 2024. p. 1-8.