Validation of Sensor Data Integrity in OT Environments Through Multisource Data Sensors

Jussi Simola, Arttu Takala, Riku Lehkonen, Tapio Frantti and Reijo Savola
University of Jyväskylä, Finland

Jussi.hm.simola@jyu.fi
arttu.h.takala@jyu.fi
riku.p.lehkonen@jyu.fi
tapio.k.frantti@jyu.fi
reijo.m.savola@jyu.fi

Abstract: This research paper focuses on detecting cyber threats from the OT environment by combining data from multiple sources. Monitoring cyber security or hybrid threats in an industrial OT environment is difficult due to different equipment, protocols, environments, personnel management and training, etc. However, the OT environment can also be observed with a multisource sensor system, which can be used to collect data. By combining IT and OT data, additional cyber threats can be found. Especially concerning the integrity of OT command-and-control data. We deal with the key concepts and differences of the industrial operating environment, which create challenges compared to the traditional IT environment. This is important because the policies defined at the European level for the NIS2 regulation are coming to touch all member countries, regardless of what the national implementation schedule is. The increased standards for OT environment cyber security implementation and development will also have an impact on the personnel management and training to support the onboarding of the standards in practice. Critical infrastructure protection is important because, without the protection of critical infrastructure, vital functions cease to function. Hostile actors cause security challenges among Western actors. In this study, we delve into whether it is possible to find threats concerning OT command-and-control process. The increased data surface collected from the IT/OT environment improves the capabilities for the system to detect malicious attacks towards the OT system. With the help of test equipment, the goal is to demonstrate that it is possible to find threats by combining data from multiple sources. With the help of test equipment, we find out IT and OT capabilities, which we load with various attacks and anomalies. We produce added value compared to traditional monitoring method test cases by comparing data obtained from different sources. The research paper shows the importance of detecting OT threats. By monitoring IT and OT environments and combining their data, we can find hidden threats. Only one test equipment configuration has been used in the study, but the results can be generalized and classified. The study also provides guidelines for how the detection of cyber threat capabilities should be developed.

Keywords: Testbed Environment, Sensor Integration, Sensor Data Integrity, Operational Technology, Cybersecurity

1. Introduction

The purpose of the CSG (Cybersecurity Governance of Operational Technology in the Smart Energy) project is to develop a governance model for operational technology ecosystems to minimize Operational Technology risks and create a new standardized operating environment for the industrial environment. The main aim of the CSG project is to develop a Governance model for the Operational technology-related environments. The study's results will be used to design processes for the governance model in the OT-SOC environment where the Industrial Control System (ICS) is a crucial operative factor in an industrial environment.

EU's cybersecurity strategy set the framework for the formation of national-level cybersecurity (European Commission, 2020, 2022; ENISA, 2023). The NIS2 directive by the European Commission (2022) states that every European Union member state must adopt a National Cybersecurity Strategy (NCSS) and establish a cyber security governance model. The European Strategic Energy Technology plan aims to boost the transition towards a climate-neutral energy system (European Parliament 2023).

At a general level, as a part of corporate governance, several elements are related to the formation of cybersecurity governance. The frameworks are essentially connected to each other. Crucial vulnerability elements of security and cyber security consist of people, processes, and technical aspects (European Commission 2022, 2023).

The operational technology environment, especially the energy sector, is critical for every vital function. If cyberattacks disrupt energy supply chain systems, all connected operational technology systems will shut down soon or later. Therefore, it is important also to apply cybersecurity supply chain risk management guides (GSA, 2014). The research concentrates on monitoring process control at the operational and technical levels. It is important to enhance detection capabilities because of the digitalization of the OT environment. NIS2 (2023) requires enhanced information sharing regarding cyber threats and incidents because it has been seen that

critical infrastructure protection is not possible to maintain without new regulations. The visibility of the cyber threat control mechanism and the capability to detect and share threat information are important parts of continuity management, which depends on the continuity of business operations.

The paper concentrates on comparing data from different places in the testbed environment. The data will be used to verify the integrity of the operational technology process. We will use several data monitoring points. The focus is on how to see events in different places. We compare the output data to the threat information.

2. Importance of Critical Infrastructure Protection

2.1 Operational Technologies in various industries and connections.

Networking and Information Systems directive NIS2 sets requirements for the companies and their strategic, operational, and technical functions (European Parliament, 2022). In addition, the Cyber Resilience Act (European Commission, 2022) supports the goals of the NIS2, and it endorses the aims of the CER Cyber Resilience directive. CRA consists of requirements for the manufacturing process of digitalized products, industrial companies, and cyber security training methods for the personnel and management of security operations (European Commission, 2022).

The Cybersecurity and Infrastructure Security Agency CISA (2020) lists critical infrastructure in 16 sectors which are Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Dams Sector, Defense Industrial Base Sector, Emergency Services Sector, Energy Sector, Financial Services Sector, Food and Agriculture Sector, Government Facilities Sector, Healthcare and Public Health Sector, Information Technology Sector, Nuclear Reactors, Materials, and Waste Sector, Transportation Systems Sector, Water and Wastewater Systems Sector.

Operational technology is vital to critical infrastructures because of the interconnected and mutually dependent physical systems and a host of information and communications technologies (Peerenboom, 2001). Critical infrastructures are called a “system of systems” because of the interdependencies that exist between various industrial sectors and the interconnections between business partners (Peerenboom, 2001; Rinaldi, 2001). An incident in one sector of the crucial infrastructure can, directly and indirectly, affect other infrastructures through cascading and escalating failures. Therefore, visibility into network traffic and device behaviors in OT networks is important. It is less than adequate across the sector regardless of the capability of a particular organization (U.S. Department of Energy (2021). By better understanding the organization's OT environment, they may be able to correlate a more minor anomaly to a potential attack, moving the asset owner’s threat detection capability earlier into an attack campaign and preventing more significant impacts on operations (U.S. Department of Energy, 2021).

2.2 Vulnerabilities in Grid Power Systems

According to the NIST (2023), the electrical power transmission and distribution grid industries use geographically distributed SCADA control technology that operates highly interconnected and dynamic systems that consist of countless public and private utilities and rural cooperatives for supplying electricity to end users NIST (2023). Regarding Eto et al. (2016), the electric power system is a complex network of electric components designed to generate, transport, and deliver electricity across two distinct yet integrated systems, but is not clearly defined the interruptions due to factors affecting the bulk power system and factors affecting the distribution system. The same type of fundamental problems is mostly related to the vulnerabilities against cyber-attacks and lack of standardization. According to the IDAHO (2016), distribution and local delivery of electricity are generally not considered part of the U.S. bulk Electric System and are overseen by state public utility commissions. Implementing cyber security standards varies in the breadth of protections and backup measures for distribution utilities. Cyber-attacks on distribution elements can have consequences that reach the Bulk Electric System. The first known hack to affect a power grid occurred in Ukraine in 2015 when a distribution system served as the attack plane. Adversaries used malware to access IT infrastructure and then hijacked the SCADA distribution management system to cause changed states to the distribution electricity infrastructure and attempt to delay restoration by wiping SCADA servers after they caused the outage, while simultaneously preventing calls reporting power outages from reaching customer service centers, resulting in a couple of hours outage. The attackers conducted months of reconnaissance before the attack, planning to execute the attacks that took multiple substations offline and disabled backup power from two distribution centers simultaneously (IDAHO, 2016; Zetter, 2016). Operational technology-related Energy distribution systems are vulnerable because

the adversaries understand how important the energy supply chain is to all operational environments. Enemy nations have an interest in manipulating workable systems.

In the connection of Operational Technology, several industrial control system devices include remote access capabilities, and industrial control systems are increasingly connected to corporate business networks (GAO, 2018). According to the GAO (2018), attackers' remote access is an increasingly potential cyber threat target for manipulating ICS devices. Because functionalities depend on the energy supply, there is a need to develop OT environments that are more protected against cyber-attacks. Cyberthreat detection capabilities are a crucial part of overall cybersecurity. The paper concentrates on the requirements of the cyber threat/ event detection capabilities.

2.3 Enhancing Cyber Security Situational Awareness at the Operational Level

The ENISA (2022), Governance model has been divided into four levels. Political, strategic, operational, and technical levels. The technical level of administration aims to link the implementation strategy so that technical and technological development takes place simultaneously, which is essential in cyberspace, a rapidly developing field where new threats and challenges arise simultaneously as new technological opportunities and solutions. The operational/ technical level is crucial for the formation of situational awareness. Technical, network and software-based data-sharing capabilities are crucial, and human interaction affects the ground-level transformed information.

Defense in Depth is based on the military concept that provides barriers to impede the progress of intruders from attaining their goals while monitoring their progress and developing and implementing responses to the incident to repel them (Homeland Security, 2016). As Homeland Security (2016) states, an organization must recognize the relationship between intruders and vulnerabilities to the controls (standards and countermeasures) put in place to protect operations, personnel, and technologies. According to the Defense-in-Depth Protection to Industrial Control Systems, the connection between Information Technology and Control Systems in an organization's security functions is crucial. The defense-in-depth strategy consists of the following elements, as Table 1 illustrates (Homeland Security, 2016).

Table 1: The elements of the defense-in-depth strategy (Homeland Security, 2016)

Defense-In-Depth Strategy Elements	
Risk Management Program	• Identify Threats • Characterize Risk • Maintain Asset Inventory
Cybersecurity Architecture	• Standards/ Recommendations • Policy • Procedures
Physical Security	• Field Electronics Locked Down • Control Center Access Controls • Remote Site Video, Access Controls, Barriers
ICS Network Architecture	• Common Architectural Zones • Demilitarized Zones (DMZ) • Virtual LANs
ICS Network Perimeter Security	• Firewalls/ One-Way Diodes • Remote Access & Authentication • Jump Servers/ Hosts
Host Security	• Patch and Vulnerability Management • Field Devices • Virtual Machines
Security Monitoring	• Intrusion Detection Systems • Security Audit Logging

Defense-In-Depth Strategy Elements	
	• Security Incident and Event Monitoring
Vendor Management	• Supply Chain Management • Managed Services/ Outsourcing • Leveraging Cloud Services
The Human Element	• Policies • Procedures • Training and Awareness

According to (Homeland Security, 2016), organizations can use five principles for countermeasures to drive activities in ICS environments. The following steps will pave the way toward a more robust security environment and significantly reduce the risk to operational systems.

- Identify, minimize, and secure all network connections to the ICS.
- Harden the ICS and supporting systems by disabling unnecessary services, ports, and protocols, enable available security features and implement robust configuration management practices.
- Continually monitor and assess the security of the ICS, networks, and interconnections.
- Implement a risk-based defense-in-depth approach to securing ICS systems and networks.
- Manage the human—clearly identify requirements for ICS; establish expectations for performance; hold individuals accountable for their performance; establish policies; and provide ICS security training for all operators and administrators.

3. Data Integrity Validation and Process Integrity

3.1 Managing Information Security in IT and OT Environments

3.1.1 CIA and AIC Triad

Confidentiality, Integrity, and Availability (CIA) triad is a form of representation of the fundamental elements of security objectives in information systems (NIST, 2020a,2020b). Confidentiality is focused on the restrictions on the use and storage of data, which may be lost in cases such as during insecure data transmission or access control (Kar &et.a., 2021) On the other hand, integrity offers guarantees that data has not been tampered with. One way to attempt to secure data during transmission is to use checksums to validate the integrity of the transferred data between the sender and the receiver (Kar and Zolkipli, 2021). Availability in information systems ensures that the authorized users have timely and uninterrupted access to necessary information, resources, and components. In OT environment, availability includes being able to use the devices that are part of the system, which could be crucial for the environment they're in (Kar and Zolkipli, 2021). The impact of availability is exacerbated in critical infrastructure, where the loss of availability would have cascading impact on society.

Although CIA triad implements heavy focus on technical security controls, when socio-technical elements are important in system security, it is a valuable and straightforward way to understand and solve issues that are relevant in information security (Samonas and Coss, 2014). For example, it is especially relevant in Common Vulnerability Scoring System (CVSS) scoring when system impact of a vulnerability is estimated, which are used in estimating severity of Common Vulnerabilities and Exposures (CVE) events. CIA triad has its roots in military security mindset, where the protection is perimeter focused against external threats (Samonas and Coss, 2014). Additionally, loss of CIA of information or information systems is used as basis in development of relevant security controls (NIST, 2020)b.

3.1.2 On the Aspects of CIA/AIC Triad in IT/OT

CIA triad originates from IT domain, where the security features aim to provide safety by protecting itself against cyberattacks. Traditional OT domain's safety aims to ensure functional resilience and safety to protect the environment and humans against unwanted operations that could lead to physical damage or injuries (Hollerer & et.al, 2022). Additionally, priorities considering the CIA triad are inverse between traditional IT and OT environments, where IT environments prioritise confidentiality first (CIA) and OT environments availability first (AIC)5. With the OT 4.0 shift of integrating IT capabilities and interfacing OT devices into IT infrastructure, the difference between IT and OT is diminished, since it opens OT environments as targets against cyberattacks. For

example, cyberattacks may target OT environments to prevent the availability of safety function of an OT device, which may lead to undermined safety of the environment. However, while loss of availability might be the major threat in OT environments, loss of confidentiality and integrity may be used to cause loss of availability with cyberattacks. In an automated system, the loss of integrity can lead to a higher loss of availability. This is due to the potential for system shutdown triggered by cascading adjustments. These adjustments are based on the falsified data and are intended to steer the system towards correct function. For example, if data routes have their integrity lost (manipulated device status report), the automated safety system shutdown may be used as the attack vector to damage the equipment, leading to loss of availability, which in turn impacts the security (Dentlzer&et.al,.2021). Similarly, loss of confidentiality on higher privileges and device data may lead to them being used to aid in attacks against the OT environment's availability. Therefore, while availability is the most important target to defend, confidentiality and integrity are inherently connected to overall availability in OT 4.0 environments. This leads to the need to balance all aspects of the CIA triad to ensure safety when designing system controls rather than prioritizing confidentiality first.

4. Background Theory

We have applied a design science research methodology, which is used traditionally in system development (Hevner & et.al., 2004). As part of the design science process, the multiple case study research-based strategy by Yin (2004) and the knowledge base of the case studies create a core framework for the governance model and generate an added knowledge base. This iterative design science process output must be different from the present system. The MITRE Att&ck (2023) framework has formed the common base for analyzing cyber-attacks, tactics, and scenarios. It has its own weaknesses related to industry-based threat classification, but it is very suitable to apply to almost all kinds of companies. Operational Technology-based vulnerabilities are nowadays the main target when the aim is to develop a coherent cyber security environment. The MITRE Attack framework (2023) is an important element of the testing process. We have used data from it in several cases.

The paper concentrates on data integrity validation and its process. The process will be validated using data from various points during execution. Another research focus concentrates on enhancing the visibility of sector-based threat information. Two main aspects must be considered:

- Data integrity validation may be done with data sensors at various points, where the values of the data may be compared to ensure their correctness. The various data sensors may also be used to track process steps throughout the system. This way the process integrity may be a target for validation instead, to ensure it has not been tampered with. For example, with various data sensors, the system warden may see that the command sequence is manipulated halfway through the process, leading to a different outcome than initially requested. This may be included with additional system-specific information, such as software versions, hardware equipment, and network protocols.
- When a system vulnerability or malicious attack is detected, the additional system information aids in threat intel and security breach reporting to the relevant stakeholders. These companies may work in similar or adjacent sectors, where identical hardware or software is used. In summary, the process validation may be used to provide context to threat intel. Additionally, the NIS2 (2022) directive mandates sector-based threat intel reporting, where companies are obligated to report to the relevant government body about possible security breaches. Using various data sensors for process validation improves the visibility of the security processes, which in turn aids in providing information to governmental bodies. This, in turn, proves that the company is upholding its obligations.

4.1 Point of Process Monitoring

Monitoring a process and its data traffic in OT environments aids in creating a holistic situational awareness, in addition to process awareness, which includes elements such as steps taken, transferred data, used devices, and software versions. If a cyberattack uses specific process as an attack vector, process-based monitoring aids in forensics due to documented and monitored content. Additionally, monitoring a singular process through various data sensors aids in auditing process function events. For example, if a cyberattack manipulates data at a particular step of a process, such as during a log request or SCADA command, it may be analysed in forensics towards a specific section in internet infrastructure where the step would occur. This provides additional information, which may be used in further forensics, such as the devices (e.g., switch and IED) used in this specific step, their software versions, and protocols used in communication. This additional information needs to be manually managed in cases where the monitoring focuses on specific data values without including process as a

framework for context. Additionally, process monitoring enables analysis of causal relationship between steps and other processes. If a data value doesn't change as expected after a certain process step is performed, it could signal a potential compromise.

4.2 Testbed Environment

The testbed environment developed by the University of Jyväskylä is a unique platform for testing different kinds of vulnerabilities and threat scenarios. Testing separate software, devices, and network combinations in many ways is possible. Collaboration with business companies is essential and generates new data for protecting critical infrastructure.

We have tested how to detect and see threat data at different points. The used laboratory environment consists of a process plant with its OT devices and the control and monitoring network, as Figure 1 illustrates. The plant can be controlled with local and remote SCADA system. Remote control is implemented with an LTE connection. A separate monitoring network is connected to the process plant. Monitoring is implemented by mirroring the network traffic from the central switch and OT device log information from the central logging points of the process plant and the control center (Office).

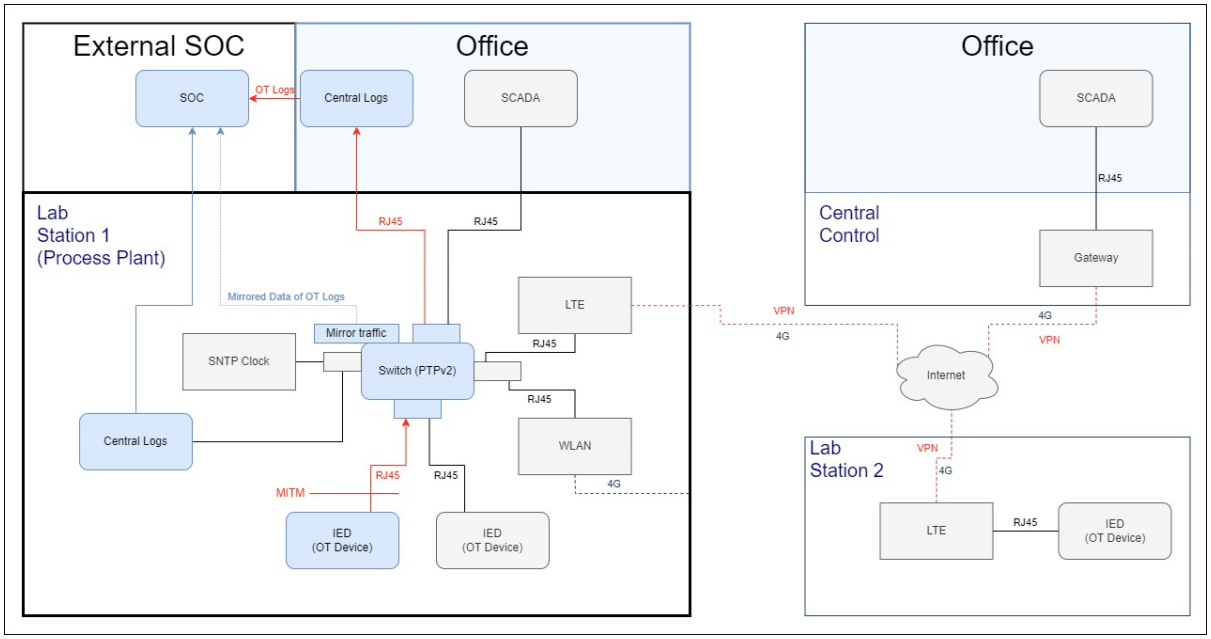

Figure 1*:* Testbed environment

The Man-In-The-Middle (MITM, man = person, device) scenario is indicated in red, which is used to validate the process-based data integrity verification method. PITM data compromise is carried out with an additional device which is added to the connection between the process plant and the office. Compromised OT logs are also highlighted in red. The devices utilized in the scenario are highlighted in blue.

4.3 Use Case

4.3.1 Environment and Scenario

As Figure 2 illustrates, the use case is depicted with a real-world counterpart. Separate office space contains the plant's control system, which is connected to the plant's internal switch. The data transfer between the production plant and the office space is remotely monitored with a separate SOC. Furthermore, one distinct isolated network is employed for the surveillance of OT device logs, while a different network is used to directly request OT device logs from the device itself.

In this scenario, the attacker has access (physical or network) to the process plant control network. The attacker modifies the data transferred between the OT device and the central switch. By modifying this data, the attacker can compromise the situational awareness of the control system and SOC, evade installed defense mechanisms, and disguise footprints left in the system. MITRE ATT&CK (2023) classifies the attack as a Man-In-The-Middle (MITM, Person-In-The-Middle) technique and a defense evasion tactic.

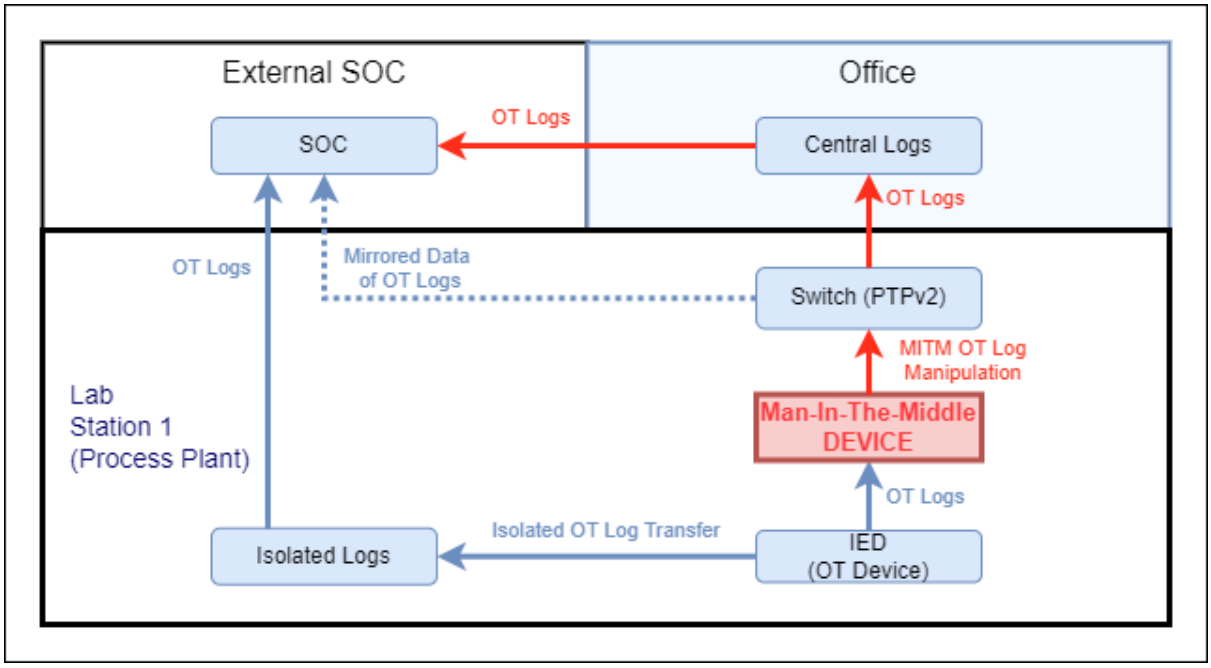

Figure 2*:* Description of the use case

4.3.2 Performed Use Case

During the executed log request process, monitoring occurs via data links at the central logging device, switch, and IED. The IED reports within the internal network through the switch to the logging device, while external reporting is done via an isolated cable. Specifically, the process involves a log request from the central logging device to the IED through the switch, supported by an additional external request from the SOC.

The MITM attack undermines the integrity of the response to the central logging by manipulating the sent data. This leads to central logging and switch data links to report incorrect status. From the SOCs perspective, there is a discrepancy in the status logs returned in response to the event log request: the switch and central logging indicate a 'local control' status, while the IED reports a 'remote control' status. This deviation is an anomaly, prompting further investigation to identify potential malfunctions or Indicators of Compromise (IoCs). By analyzing the causal relationships of process steps and examining historical logs, we can determine whether this IED should be in a 'remote control' or 'local control' state based on previous state-change commands. This verification process helps pinpoint the location of potential IoCs within the internet infrastructure.

5. Findings

The upcoming NIS 2 directive requires critical infrastructure operators to monitor their systems for cyber-threats. Operators must be able to report any potential threats and interpret the reports of other operators. To make the most effective use of potential threat reports, they must also include information on the cause-and-effect relationship to which the threat is related.

The capability to monitor, log, and report one's own behavior is vital to the OT device. Additionally, centralized monitoring is crucial to ensure the correct functionality of the entire system. However, in OT environments, there are hardware limitations to monitoring the integrity of the command-and-control process. For this reason, it is possible to add a separate monitoring network to the old systems. The monitoring network monitors possible IT threats to the OT network, as well as threats related to the integrity of the OT process. The threat information about OT systems must especially be able to be shared with operators in the same sector.

At the heart of the monitoring network is a SOC, where IT and OT data from the network are collected. The SOC must be able to handle traditional IT-related cyber threats and OT-related threats. These also include threats related to the integrity of the OT process. Therefore, when collecting and sharing threat information from OT systems, it is essential to include information about the environment in which the threat was detected, including devices and protocols. The information must be structured so that an operator in the same sector can use the threat information in their own system. Also, Potential confidential business secrets must be considered when

threat information is shared. The specific information to be shared must be agreed upon separately, as the detailed analysis of it could potentially expose these secrets.

The current situation in OT environments focuses on monitoring operating environments' performance and status to ensure safety and reliability. However, convergence of IT and OT has led to a situation where transferred data and operation functions may be maliciously manipulated through the IT interfacing elements. In OT one method to verify such manipulation is based upon checksums, but it originates from finding corrupted packets, not intentional manipulation. The majority of OT monitoring is therefore focused upon whether the machine or function is mechanically broken or that someone has unintentionally configured the device wrong.

According to process control, an isolated network and hardware are good for monitoring the process in a way that many sensors are used. It is important to divide what is monitored and in what context; in the case of the man-in-the-middle attack, the entire log reporting process is needed. Many checkpoints show where the process went wrong. It is important to analyze what this can mean for the entire system's operation. A cause-and-effect relationship can be found in the process data. We monitor processes; in practice, we monitor the operation of the electricity distribution network with certain devices. Sector-specific information is distributed upwards. The purpose is to share and receive data about potential threats identified in one's own sector.

6. Conclusion

There is a need to enhance the maturity level of monitoring events in the operational technology environment. Researched events from the IT and OT environments are crucial when the purpose is to produce coherent situational awareness of the industry environments. Without the ability to see the required things from the IT/OT environment, understanding the business situation may disappear.

The visibility of cyber security processes is critical to fulfilling the requirements of European Union regulations. Several OT-related standards and special publications are important in steering the supply chain. Validation is a set of actions regarding the system requirement, and it is important to ensure they are fulfilled.

NIS2 (European Parliament, 2022) requires collaboration between the industry sectors and within it. The information must flow, so the connection between the strategic, operational, and technical levels is a crucial factor that enhances the overall situational awareness within sector-based industries and at the enterprise level. As ENISA (2023) states and NIS2 suggest, there must be understandable mechanisms where operational technology-related events are transmitted and transformed into a form that generates added value for the decision-makers. It is not enough to achieve a report that indicates events. There should be information about the type of vulnerabilities and a description of the whole process, including the source of the threat and potential consequences. Because many attempts of the adversaries' attacks are being tried again, ja, unintentional events or incidents are often repeated. Decision-makers should be able to make decisions regarding business continuity and information-sharing capabilities depending on the security operation center's maturity to detect operational technology-related threats deep enough. That is impossible without gathering and combining different kinds of data from the physical and networked sensors. So, the framework of the process control mechanism that gathers data and shares data from the Operational Technology environment to the SOC is crucial to enhance operational technology cyber security at the ground level. The developed taxonomy has its own role in forming situational awareness (NIS Cooperation Group, 2018), but it must be kept up to date more efficiently because of the development of potential incidents.

The CSG project concentrates on developing the governance model for the OT environments. All research data from the testbed environment support the development process of the governance model.

Acknowledgments

The research was supported by Business Finland (grant number 10/31/2022) and the University of Jyväskylä.

References

CISA (2020) Critical Infrastructure Sectors. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Denzler P., Hollerer S., Frühwirth T., and Kastner W. (2021) Identification of security threats, safety hazards, and interdependencies in industrial edge computing. In The Sixth

ACM/IEEE Symposium on Edge Computing (SEC' 21), December 14–17, 2021, San Jose, CA, USA. ACM, New York, NY, USA.

Eto J. H., LaCommare K. H., Caswell H., Till D., (2017) Distribution system versus bulk power system: identifying the source of electric service interruptions in the US. The Institution of Engineering and Technology.
ENISA (2023) Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies.
European Commission, (2020) The EU's Cybersecurity Strategy for the Digital Decade. Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020JC0018
European Commission, (2022) Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.
European Parliament, (2022) Directive 2022/2555 Network and information security (NIS2).
European Parliament (2023) Directive (EU) 2023/2413 of the European Parliament and of the Council of 18 October 2023 amending Directive (EU) 2018/2001, Regulation (EU) 2018/1999 and Directive 98/70/EC as regards the promotion of energy from renewable sources, and repealing Council Directive (EU) 2015/652
GAO, (2018) Critical Infrastructure Protection Actions Needed to Address Significant
GAO (2024) Cybersecurity Supply Chain Risk Management (C-SCRM) Acquisition Guide
Hollerer, S., Sauter, T., Kastner, W., (2022) Risk Assessments Considering Safety, Security, and Their Interdependencies in OT Environments. In The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria. ACM, New York, NY, USA. https://doi.org/10.1145/3538969.3543814
Homeland Security (2016) Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Industrial Control Systems Cyber Emergency Response Team.
Hevner A., March, S.T., Park, J., and Ram, S. (2004) Design Science in Information Systems Research. MIS Quarterly.
IDAHO (2016) Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector
Kar Yee, C., & Zolkipli, M. F. (2021) Review on Confidentiality, Integrity and Availability in Information Security. Journal of ICT in Education, 8(2), 34–42. https://doi.org/10.37134/jictie.vol8.2.4.2021
MITRE (2023) "ATT&CK Matrix for Enterprise," [online], https://attack.mitre.org/.
NIS Cooperation Group (2018) Cybersecurity Incident Taxonomy CG Publication 04/2018
NIS Cooperation Group (2018) Reference document on security measures for Operators of Essential Services
CG Publication 01/2018
NIST (2020a) Special Publication 1800-26A Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events
NIST (2020b) Special Publication 800-53r.5. Security and Privacy Controls for Information Systems and Organizations
NIST (2023) Special Publication800-82r3. Guide to Operational Technology (OT) Security
Peerenboom J (2001) “Infrastructure Interdependencies: Overview of Concepts and Terminology.” (NSF/OSTP Workshop on Critical Infrastructure: Needs in Interdisciplinary Research and Graduate Training,
Washington, DC)
Rinaldi, S., Peerenboom, J., Kelly T., “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,” IEEE Control Systems Magazine, (December 2001), pp. 11-25, http://dx.doi.org/10.1109/37.969131
Samonas, S., Coss, D., (2014) The CIA strikes back: redefining confidentiality, integrity, and availability in security. USA.
U.S. Department of Energy (2021) Methodology for Cybersecurity in Operational Technology Environments.
Zetter, Kim, (2016) "Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid," Wired, www.wired.com.
Yin, R.K. (1994) Case Study Research: Design and Methods, 2nd edn. Sage Publishing, Thousand Oaks.