Impact of Cyber Security Operations on Hardware Requirements for Stable and Workable Industrial Environments

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: Securing electricity distribution is one of the most important principles of the EU cyber security strategy. For example, European cyber security regulations, such as NIS2 (Network and Information Security Directive), CER (Critical Entities Resilience Directive), and Cyber Resilience Act (CRA) together aim to create a foundation and guidelines for international standards in various industries and the operation of critical infrastructure. Securing critical infrastructure is a common goal for Western operators. The new European Union (EU) directives bring new requirements to critical infrastructure administrators, device manufacturers and operators. Previously, member states have had responsibility for compliance with the directives, but they have been given freedom in the method by which they approach the requirements. Currently, member states' solutions are not always uniform, which has led to increased difficulties in coordination on a multi-national level. This, in turn, may lead to difficulties in coordination when responding to cybersecurity threats and attacks on critical infrastructure. The new regulation focuses on unifying the reporting between member states, reporting requirements of severe critical infrastructure events, and creating cybersecurity risk management procedures. In this study, we will provide a novel solution on how critical infrastructure administrators, device manufacturers, and operators may respond and become compliant with the new EU directives. To reach compliance and to enable the responsibilities that are required by the directive, the critical infrastructure devices and environment must have the capability to enable the responsible parties to identify, protect, detect, respond, and report. This sequence of actions is cyclical in nature since the identification of threats and vulnerabilities requires reports, which in turn requires data and detection. Our study focuses on the hardware requirements this causes on the manufacturing specifications, such as data collection and detection capabilities. The research belongs to the CSG project, and the purpose is to develop a governance model to minimize Operational Technology related risks and create a new standardized operating environment for the seamless utilization of energy solutions and industrial environment. The results of the study will be used in the analysis of requirements definitions in the OT environment.

Keywords: Operational technology, Security operations, Cyber resilience, Governance model

1. Introduction

The first research of the CSG (Cyber security governance of operational technology in sector-connected smart energy networks) project handled a research approach for investigating cyber security at the operational and technical levels. It focused on where to concentrate on OT-SOC-related cyber security research and how we aim to deploy a testbed to develop a governance model in the CSG project. This is the second research paper regarding the CSG project, and it concentrates on the cybersecurity-related strategic requirements, which reflect the measure of the security operational centers and the operational industry level.

The research belongs to the CSG project, where the purpose is to develop a governance model to minimize Operational Technology related risks and create a new standardized operating environment for the seamless utilization of energy solutions and industrial environment. The results of the study will be used in the analysis of requirements and new design process definitions in the OT-SOC environment where the Industrial Control Systems (ICS) are crucial operative factors in an industrial environment. The key results create the basis for standardization work and create essential development needs for industrial business operations to develop cyber security.

The purpose of the research is to find out and compare international and national level requirements for the management of future industrial cyber security in industrial companies and compare how the initial use case findings and observations from the testbed platform help define new operational technology functionalities.

As the energy sector is the biggest contributing factor in achieving the EU's climate goal of reducing emissions by at least 55% by 2030, the Commission proposes to act on the Plan for the accelerated digitization of the sector, which is necessary to ensure that the transition to renewable energy sources, networked mobility, smart

buildings, and a more integrated energy system, at the heart of which are consumers. (European Council of the European Union, 2023)

Extensive energy disruptions in the US and EU over the past years have shown the need for resilient and cyber-secure energy.

What European Union-level legislation demands from national actors on a strategic level is noteworthy. We must compare what new threats and risks can arise if the legislation is implemented or is not implemented at the national level and followed at the company level. Based on this preliminary assessment, a deeper threat and vulnerability assessment can be made at different levels.

The main research question concerns the formulation of hardware requirements for cyber security operations such as information sharing. Cybersecurity requirements that we have in different kinds of Security Operations Centers set challenges to different kinds of digital-based operations. The past and present Command and control functions that we have for example, in SCADA systems differ. Therefore, it is crucial in the OT environment to analyze crucial needs of data and information content. How can we get proper and useful information from the industrial environment, and what information is needed? The test-bed environment or laboratory is built to answer questions such as those. The laboratory will help design the process of the cybersecurity governance model for the industrial environment.

2. Challenges in Standardizing the Elements of the OT Environment

To achieve the cyber security requirements of the European Union, member states must create or re-organize the authorities responsible for supervisory tasks. The large EU-level aim is that the European cyber defense strategy must be implemented within the EU member countries to achieve common situational awareness (European Commission, 2020a).

According to the European Commission (2022b), EU Member States must, by using a risk assessment, identify critical entities that provide essential services for the maintenance of functions vital to society, economic activities, public health, and safety or the environment, and identify cases in which an incident would have significant disruptive effects on these essential services or when it would affect the national systems that safeguard the rule of law. To ensure the proper functioning of the internal market, two main goals were defined related to the Cyber Resilience Act (CRA) (European Commission, 2022): Create the conditions for the development of secure products with digital elements by ensuring that hardware and software products are brought to market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout the product's life cycle; and create conditions in which users can take cybersecurity into account when choosing and using products with digital elements.

The following goals were set at the initial regulation meeting: To ensure manufacturers improve the safety of products containing digital elements from the design and development stage and throughout the entire life cycle. To ensure a consistent cybersecurity framework to facilitate compliance by hardware and software manufacturers. To increase the transparency of the security features of products containing digital elements and enable companies and consumers to use products containing digital elements safely (European Commission, 2022). The regulation set new requirements for cybersecurity in the industry environment. How does that affect the three selected/strategic, operational, and technical levels?

According to the (EU) 2022/2555 directive, we don't have cross-administrative authority that may perform supervisory activities between the different sectors. Reporting mechanisms have been organized mainly by sectors (European Parliament, 2022). Political governance is seen as the highest level of governance. The political level focuses on establishing processes, roles, and responsibilities for implementing the National Cyber Security strategies in their related policies. Dedicated cybersecurity agencies or departments within ministries are leading the political level (ENISA, 2022a)

2.1 Strategical Cybersecurity Requirements to the Industrial Stakeholders

According to the European Parliament (2022), companies must be divided into industry specific categories. Entities would be classified based on their importance. There will be two main categories, the essential and important entities. The directive requires companies to implement cybersecurity management as part of the other management strategies. The high-level critical sectors were Health, Transportation, Banking and financial market, Digital infrastructure, Water supply (Waste water), Energy, ICT service management, Public Administration, Space, and Digital service providers.

2.2 Operational Requirements - Continuity Management

Operational requirements are connected to business continuity management. Companies must conform in a manner where operational continuity management is verified as required by cyber security regulations. (European Commission, 2022; PECB, 2023) So-called national ISAC´s (Information Sharing and Analysis Centre) are communities that share information among their sector-based groups by using, for example TLP (Traffic Light Protocol) -mechanism, but it does not have joint cybersecurity elements to inform about cyber threats and vulnerabilities. However, the viable mechanism is under development (ENISA, 2023b).

2.3 Technical Requirements

NIS2 directive will set the cybersecurity-related requirements for critical cyber functions. Therefore, every organization must organize its core functions in a cyber-resilient way. Especially Cyber Resilience Act (CRA) sets new standards for industrial organizations at the technical level (European Commission, 2022).

3. Central Concepts

CSG (Cybersecurity Governance of operational technologies in the sector connected smart energy)

The main aim of the Business Finland-funded CSG consortium is to create a replicable governance model for the energy and industrial sector. Co-operative development work with business stakeholders and research organizations makes it possible to understand different industries better. The built test laboratory environment supports the main aim of the project.

The project consists of a cybersecurity governance model covering the industry operations, selected digitalized devices, used equipment, training employees, managing procedures, and information sharing process for operational technology that belongs on it. There will be three main governance levels: Strategic, Operational, and Tactical.

SOC & C2

In US basic military terminology, Command and Control (C2) is also described as the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission (Department of Defense, 2021). Command and control systems are the facilities, equipment, communications, procedures, and personnel essential for a commander to plan, direct, and control operations of forces pursuant to the missions assigned (Department of Defense, 2021).

The origin of this practice is in military operations, but it has evolved and spread across multiple industries, which has led it to be sometimes called “universal C2”, due to the similarity of sub-functions. A well-known implementation of this is NASA mission control, due to the complexity of the missions (Maykish P.,2014) As network infrastructure developed, the apparent need for C2 in complex networked environments became apparent, and network-centric warfare’s prominence led to military operations employing C2 in the form of Network Operation Centers (NOC) (Kaliyaperumal L., 2021). As networked environments evolved, so did the need for its protection, which led to NOC monitoring evolving into Security Operation Centers (SOC), with the capability of intrusion detection and response through reactive monitoring. Currently, sophisticated SOCs can proactively monitor with automation Kaliyaperumal L., (2021), but implementing SOC at this level into OT environments is challenging due to environments’ differences.

Cyber resilience

Cyber resilience is a fundamental feature in the OT environment when the main pursuit is to develop a safe and stable supply chain. Business processes belong to business continuity management (PECB, 2023). Operational industrial environments need standardization because workable, seamless industrial processes make it possible to enhance business processes. Standardized process management by Business Continuity Management (BCM, 2023) and also cybersecurity-guided development of devices are crucial factors when the purpose is to maintain fluent supply chain operations.

The white house (2013) defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes withstanding and recovering from deliberate attacks, accidents, or naturally occurring threats or incidents. Achieving resilience requires accurate information and analysis of risks. “Resilient infrastructure assets, systems, and networks must also be robust, agile, and adaptable. Mitigation, response, and recovery activities contribute to strengthening critical infrastructure resilience” (The White House, 2013).

Governance

Governance describes a complex system, defining roles, responsibilities, processes, and relationships. Governance includes stakeholders from and covers the private sector, the public administration as well as civil society and spans different topics such as economic, social, and political priorities (ENISA, 2023a). Cyber Governance is the operation of decision-making processes that enhance and ensure "participation, transparency, and accountability in taking measures related to cyberspace together with the mechanism of international agreements, strategies, laws, measures, regulations, and standards that interlock in the best way" (Efe, A. & Bensghir, K. T., 2019).

Threat Information Sharing

Cyber threat information helps organizations identify, assess, monitor, and respond to cyber threats. Cyber threat information may consist of indicators of compromise, tactics, techniques, and procedures used by threat actors, suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents (NIST, 2020).

Indicators are technical artifacts or observables that suggest an attack is imminent or is currently underway or that a compromise may have already occurred. Indicators can be used to detect and defend against potential threats. Examples of indicators may include the Internet Protocol (IP) address of a suspected command and control server, a suspicious Domain Name System (DNS) domain name, a Uniform Resource Locator (URL) that references malicious content, a file hash for a malicious executable, or the subject line text of a malicious email message (NIST, 2016).

Threat Reports describe tactics, techniques, and procedures, actors, types of systems, and information such as threat-related information that provides more accurate decision support and situational awareness to an organization. Threat intelligence consists of threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide an important context for decision-making processes (NIST, 2016).

Tactics, techniques, and procedures (TTPs) describe an actor's behavior. Tactics are high-level descriptions of behavior, techniques are detailed descriptions of behavior in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique. TTPs could describe an actor´s tendency to use a specific malware variant, order of operations, attack tool, delivery mechanism (e.g., phishing or watering hole attack), or exploit. (NIST, 2016).

Regulation

As we have seen in Europe, stable development of the security environment is not the same anymore. The eastern neighbor of Finland has started a war that affects all over the world. Therefore, we must take a couple of steps in advance to achieve a more secure state or situation where we want to live in the future. It is not possible to achieve a fully secured future, but we can do things and measures that allow us to develop better overall situational awareness including cyber situational awareness. Therefore, European-level security agencies and public safety actors have created cyber security strategies that must be implemented with European-level cyber security strategies in order to achieve joint overall security. Most European Union member states also have full membership in NATO, which secures our living in a changing security environment.

Digitalized transformation of traditional infrastructures in the world requires preventive actions against cyber threat events. Nowadays, hybrid threats are more common than ever. Cyber-physical threats set challenges because we must detect weak threats and signals much earlier than in basic or simple threat atmospheres. The new European-level legislation set new requirements for the European Union member countries, its enterprises, companies, and individuals, including management level and in-practice level workers (European Commission, 2022). For example, the manufacturing process and used components of the digitalized equipment and devices will be more standardized. NIS2 Networking and Information Systems directive sets requirements for the companies and their strategic, operational, and technical functions. On the other hand, the Cyber Resilience Act (CRA) supports the goals of the NIS2, and NIS2 supports the aims of the CER Cyber Resilience directive. CRA sets 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, 2023c). The aim is to create common industry-specific cybersecurity requirements for the global business environment. The detected cyber incidents must be reported to the national cybersecurity agency and the national cybersecurity agency has to resend those vulnerabilities information to the European level security agencies. It is also crucial that the information will be shared to other EU member states and sector-specific actors.

3.1 Laboratory Environment

The developed testbed implements high-end OT hardware and software solutions commonly used in critical infrastructure that are connected to an IT network, which enables it to be operated, maintained, and surveilled remotely. Developed testbed enables cybersecurity-related use cases that target each component, their connecting interfaces, and specifically the addition of IT solutions in OT environments. Current IT related cybersecurity research highlights the importance of both host and network detection solution, which is tested in practice with use cases. For this, a SOC will be implemented, with sensors at different levels of intrusion, to demonstrate the required depth of access the detection sensors may require, to provide the protection against malicious activity required by the regulations. For example, a sensor at the network layer might notify SOC that the OT device is attempting to exfiltrate information outside of the allowed operating region, but it would not provide any information about the malicious internal activity of the OT device. In addition to this, the SOC will be further developed with machine learning solutions to detect more sophisticated attack patterns, which enables more sophisticated use cases. The developed testbed will in this way provide data to support the development of maturity levels and highlight the possible risks that different levels of maturity have when it comes to the implementation of IT in an OT environment.

4. Research Methods

The built testbed in a laboratory environment allows to research scenarios in a way that the created threat scenarios are possible to execute in practice. The devices, equipment, and software that we have gotten from stakeholders enable us to do tasks as we have planned.

Initial laboratory tasks will produce new data for the governance model and help to develop features and functionalities of the security operations center. It will bring added value to the IT-SOC features because there are missing signal-processing elements that enhance the formation of situational awareness functionalities. It is crucial to gather data such as weak signals from the industrial environment where the old-fashioned machines are. The critical is to identify the emergency point, where SOC and detection features must react. In Industrial Control Systems such as Scada, intrusion prevention or detection tools are relevant machines that we must have under the secured control of operations. We will apply a widely used design science research methodology used traditionally in software and system development. As Hevner (2004) has explained in Figure 1, design science research methodology is based on three iteration cycles that support each other's. On the left side, there is an environment where problem formulation has been done. We must understand the environment where we are doing our study (people, organizations, technology).

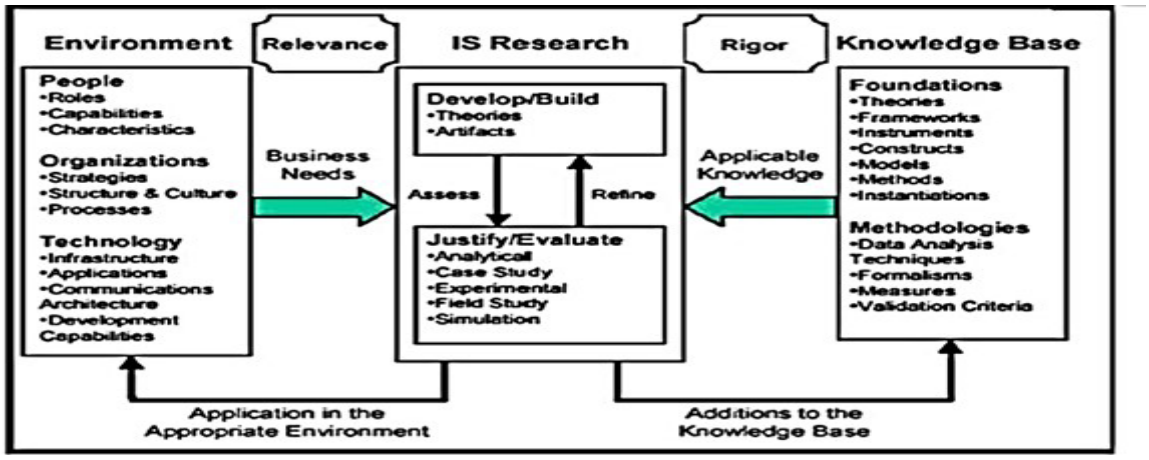

Figure 1: Information Systems Research Framework (Hevner et al. 2004)

Operations of the Design science research form by requirements from test environment that we have created. Case study research basement by Yin (2004) and the present knowledge base creates a core framework for the artifact and creates an added knowledge base. This output of the iterative process must be different than present system. The added value of the designed system must be in line with the original aim of the research.

As Yin (2004) states case studies solve real-life problems from real life. Exactly formed research questions such as "How does a hawk catch a mouse?" form the basis of the case study strategy. The research problem must be clearly defined. Why and when words are commonly used in research questions.

Nunamaker & al. (1991) argued that the systems development framework consists of five main stages: conceptual design, constructing the architecture of the system, analyzing the design, prototyping (may include product development), and evaluation.

We have also used The Delphi method which is suitable to make a relevant analysis of the testbed environment. "The Delphi method is an iterative process to increase consensus-building and, in the end, to have consensus among experts from an examined case." (Garson, 2012).

5. Results

Firstly, the systematic analysis of the study indicates the following things: There must be common overall situational awareness based on correct information as well as in the smallest industrial units and among the upper-level decision-makers. Horizontal and vertical situational awareness must be based on a common mental model and understanding of the current state of the overall security at the strategic, managing, operational, and tactical levels. That understanding or awareness should come for example, from the operational environment where industrial devices and components have crucial roles according to the continuity management and supply chain (NIST, 2022; United States Government Accountability Office, 2015).

If communication is not possible or if the information does not flow between the decision-maker level and the operational environment, potential obstacles prevent tackling cybersecurity threats. Fundamental problems in security management implementation processes set new challenges to implement and apply new cybersecurity technologies and tools (Simola, J., & Lehto, M. 2020).

Implementation processes at the technology/ technical level in practice set new challenges, and it must follow strategic cybersecurity goals at the national level and companies' business strategies. To achieve cyber resilience, it is important to find crucial factors that affect the whole supply chain in the plant's production line.

The testbed environment will show the weakest points that may generate vulnerable setpoints in the supply chain and information sharing. The testbed environment has been built for development work by using the idea of the DSR methodology, and we have opportunities to demonstrate real-life problems that occur in ICS environments.

The knowledge base Matrix developed by MITRE (2023) proves that ICS-related vulnerabilities are linked to the IT -environment in many ways. We are going to apply Use cases because one of the main aims is to design combined IT/OT Soc that make it possible to use proactive features in threat detection functions.

The Soc maturity is crucial in efficient proactive and prevention mechanisms. The threat scenario analysis illustrates that it is crucial to harmonize different kinds of soc features within the sector-based information-sharing groups. If there are different soc maturities in one sector-based (E.g., energy sector) sharing group, the weakest link governs the procedures. It is crucial and critical to set maturity assessment in a way that has been meant in cybersecurity scenarios state. If there is a cap on the activities of national authorities, it will create more vulnerabilities in industrial basements where hardware and software are connected to each other, and cyber threats are not detected in the way they had been.

Setting soc maturity at a common standard level also helps other countries and organizations to implement the operational systems and procedures to the required situation. Getting the required needs, in reality, is possible if sensor technology has been applied to all required cybersecurity stages.

5.1 Challenges Concerning Information Sharing in SOCs

In Europe, unlike in the US, Security Operation Centers are traditionally sold as a service from the private sector. To ensure the continuity of critical cybersecurity services, sharing sensitive information on higher levels of critical infrastructure and government level would benefit from SOCs not being established through competitive tendering as Figure 2 illustrates. Additionally, the government-affiliated SOCs would lower the threshold for private companies in critical infrastructure to share their vulnerable data, which helps develop more mature situational awareness (situational picture) as the data is collected to (higher levels) for further analysis. There should be horizontal and vertical possibilities to exchange data or information that is processed understandably.

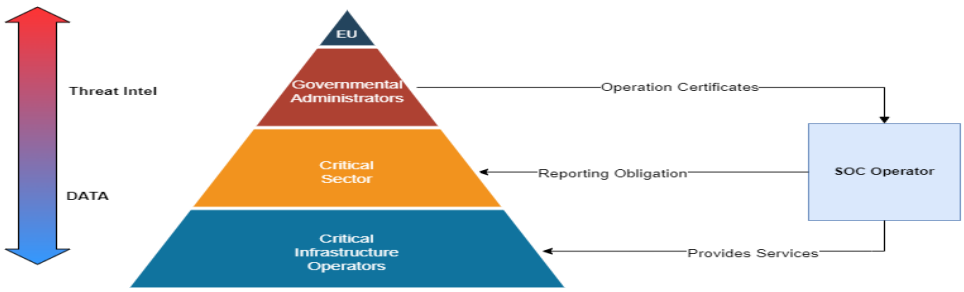

Figure 2: Information sharing pyramid

Since SOC as a service in the private sector is an established model, it can be used on the lower level of the framework as long as it is organized based on maturity and capability. This enables the SOC to report their findings informally and with the required depth and route based on the NIS2 directive.

5.2 Logic of Information Sharing Activities

In this sense, a SOC operator could provide their services to multiple critical infrastructure operators but would have to be affiliated to their operation sector for reporting purposes. To ensure continuity, the sector-based SOCs are specifically designed and built for that purpose rather than through competitive tendering. This additionally helps with competitive integrity, where a private SOC operator could provide services for sector SOC operations and operators within that sector, as Figure 2 illustrates. The collected data is analyzed, and overall countermeasures are provided to the sector-specific database, which helps sector operators through preventive countermeasures based on previous reports. Sector-specific reports are further reported to higher administrative level, which helps create a mature overall picture of situations between sectors and develop a unified countermeasure database, where other critical infrastructure sectors may search for possible preventive actions based on previous reports.

To draw a similarity to a well-known case with a malicious attack, while host device logs and network logs may have provided cohesive and matching data, additional sensors that are completely separated from its functional operating system could have showcased an anomaly. There is an advantage in the OT environment compared to the IT environment to use different kinds of sensor technology as Figure 3 demonstrates.

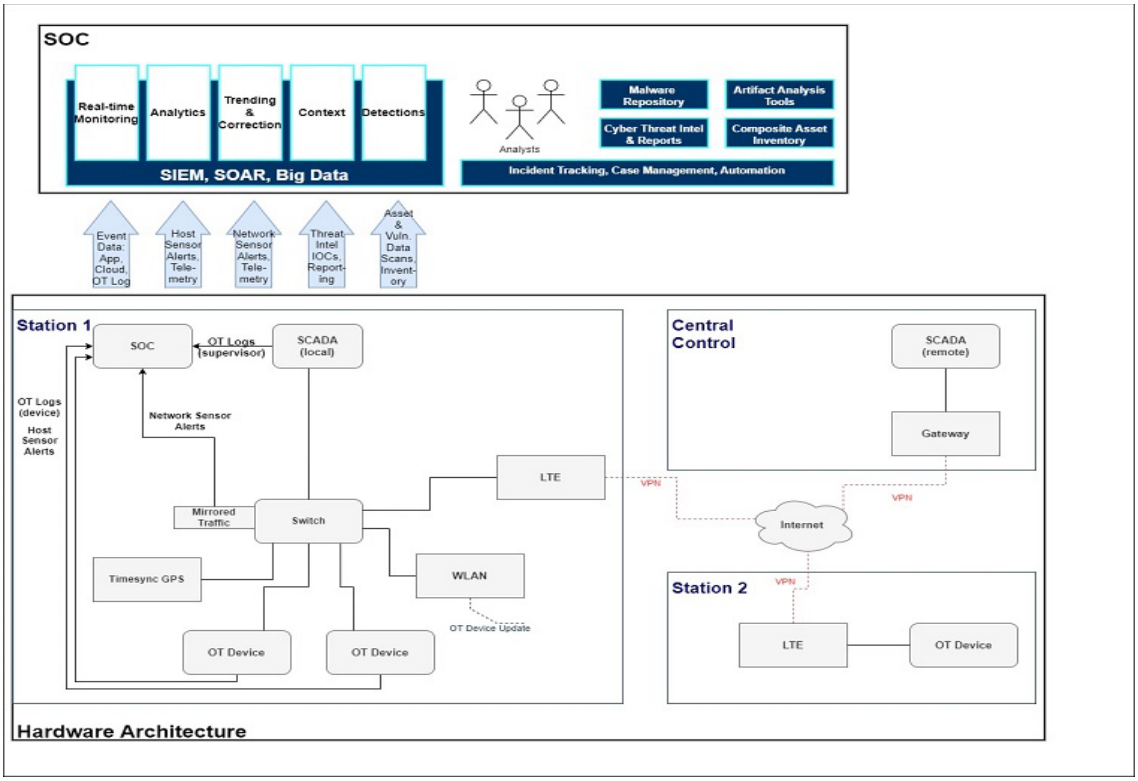

Figure 3: Hardware architecture and Soc environment (Modified from Knerler, K & al.2022)

Figure 3 demonstrates how developed testbed collects event data in the form of OT logs from OT devices and SCADA software, host sensor data from OT devices, and network sensor alerts based on the mirrored network traffic occurring through the switch. Alerts occurring from the data are audited for reporting and threat intel IOC purposes, which functions as an interface for the overarching reporting in the NIS2 directive. OT environment is unique compared to the IT environment, where asset and vulnerability data scans are seen as too disruptive, which is why only inventory documentation is seen as a possible solution. Deep scans are too harmful to the system. Scanning open ports doesn´t load that much. One important thing to measure will be how heavy scanning can be done. Twinned systems might be a solution for scanning, but they would require expensive hardware duplication. Twinned system would additionally help with critical system updates.

The multi-sensor system allows internal network traffic to be analyzed throughout its travel, allowing the SOC to alert of possible tampering midway through the operation. This leads to malware needing multiple devices, if not the whole system, under control to remain hidden while tampering.

Traffic mirroring is the initial step in network sensors. However, SOC is, in this case, connected to the internal network, and the attacker that controls the switch may notice the monitoring. Additionally, it only monitors the internal network from the switch's point of view, whereas advanced monitoring would be through data diodes, so the monitoring remains undetected, and possible signal or packet tampering between device connections may also be monitored.

The problem is that SOC operators can also be critical infrastructure operators. Threat reports must be in a concise and comprehensive format so that the information is not lost on the way. For example, if the IP is different for the attacker in different sectors, but the attack chain remains the same. The critical sectors must have their own cyber security capability to handle comprehensive and concise threat reports. National cybersecurity authority should transfer relevant information to different sectors. The energy sector does not know what devices other sectors have, so it is not possible to know if any IT/OT information is relevant to other sectors. Figure 4 demonstrates the problem formulation of different kinds of maturity levels in SOC´s.

Important things to note: On what scale are horizontal and vertical operations in terms of reporting? Where is any level of cyber security capability located? In other words, overlapping activities must be reduced and critical information threatening vital functions must be shared with the authorities regardless of the level of maturity.

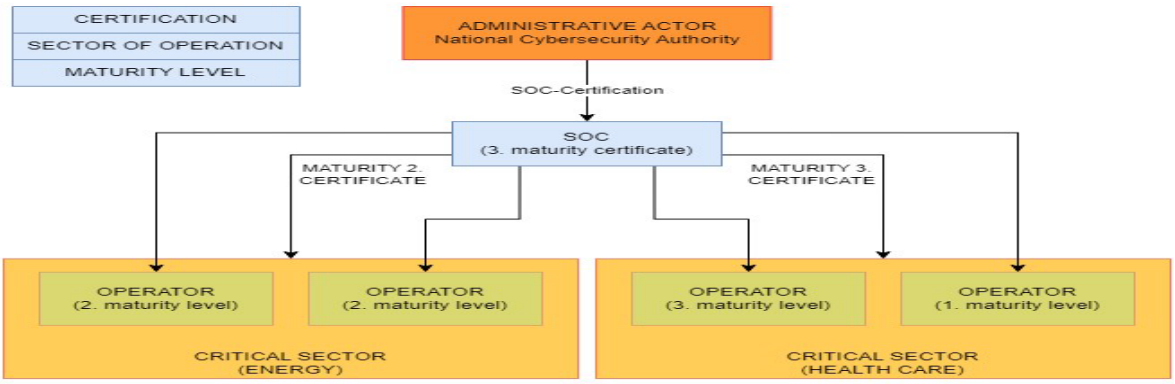

Figure 4: Maturity of the SOC´s

If the SOC activity is locked behind certificates on a sector-by-sector basis, a reporting system can be created. At the same time, a classification of SOC abilities is created, and operators are divided into different ability levels. For example, SOC has the 4th maturity for operations, but its know-how in the energy sector is only the 3rd maturity. In this case, operators in the energy sector can only buy protection of 1-3 maturities from SOC.

Cooperation between operators can be managed through their maturity levels. This enhances situational awareness and governance within a sector since a lower-maturity cybersecurity solution could undermine the network as a whole.

Additionally, there are differences between the countries; protection level may set soc operators in unequal situations from each other. Secure Continuity management sets its own requirements for a situation when operations are sold abroad.

For example, the SOC always reports the operator's problems to the operator's sector (e.g., X IP address is bad), from which the sector's other SOC operators or operators can obtain information for their own measures as

Figure 5 illustrates. Correspondingly, higher-level situational information must be kept, which is why the overall events of the sector are reported to the administrative operator.

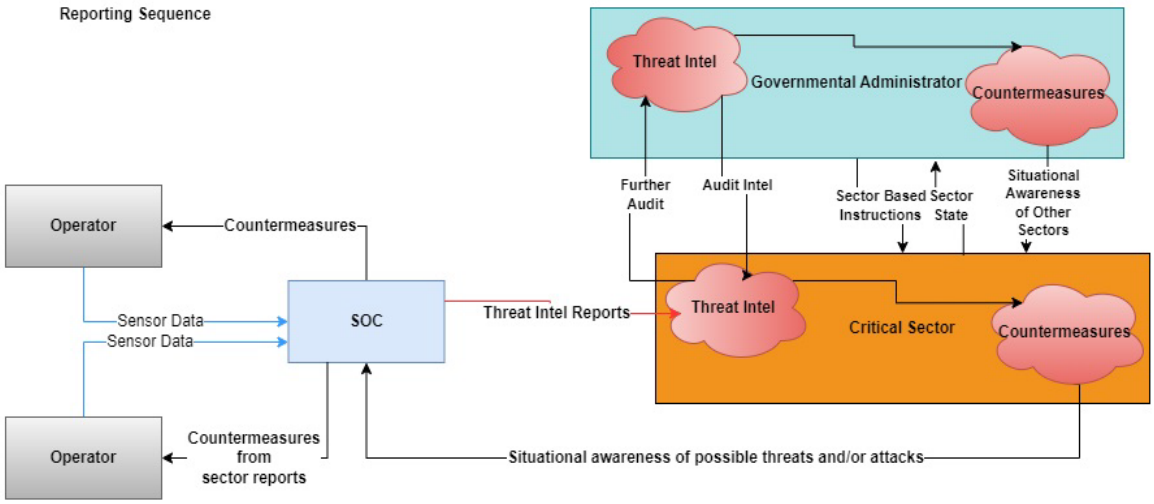

Figure 5: Reporting Sequence

The administrative actor also receives more extensive reports of cyber security events from SOCs to improve situational awareness.

6. Discussion and Conclusion

Ongoing implementation work of regulation is not a separate section from the development work of a joint strategic view of the Western cyber-attack prevention tendency. As we have seen, strategic aim and operational, tactical technology-based approach are not separate from each other. Designing a new governance model for the governance OT environment requires a coherent understanding of every awareness state. Political, strategic, operational, and technical/tactical levels must support each other to achieve common cyber situational awareness. Strategical level requirements face device-level requirements to notice deficiencies in equipment and justification for these. On the other hand, practical tests in a testbed environment produce requirements for future maturity aspects.

Standardized SOC features are crucial for the formation of joint situational awareness. Information-sharing mechanisms are crucial factors that affect supply chain management. Control processes must be formed in order to achieve real-time data from the factories. The information should be shared with other stakeholders by following standards and guidelines that are consistent with best practices. We must have at least two levels of information that industrial organizations of critical infrastructure should share within the sector-based groups. Overall cybersecurity maturity level is achievable only by implementing all required elements into the practice. That means the flow of information should achieve all required stakeholders at the time, information should be reported in an understandable way (consisting of relevant information) and it has to affect procedures and processes that are effective and efficient, preferably proactive. Shared information is not enough to achieve resilience in the cyber-physical ecosystem.

References

Department of Defense (2021). DOD Dictionary of Military and Associated Terms. U.S.

Efe, A. & Bensghir, K. T., (2022). cited in Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review.

European Commission, (2020a). 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, (2020b). Proposal for a directive of the European parliament and of the Council on the resilience of critical entities. COM (2020) 829 final. 2020/0365 (COD). Brussels, 16 December.

European Commission, (2022c). 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 Council of the European Union, (2023). European Green Deal https://www.consilium.europa.eu/en/policies/green-deal/

ENISA, (2023a). Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies.

ENISA, (2023b). Information Sharing and Analysis Centers, ISAC in a box. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing/isacs-toolkit/view#build/governance-structure

Garson, G. D. (2012). The Delphi method in quantitative research. Asheboro, NC: Statistical Associates Publishers. Available from: https://faculty.chass.ncsu.edu/garson/PA765/delphi.htm, retrieved 23.10.2023.

Hevner A., March, S.T., Park, J., and Ram, S. (2004) Design Science in Information Systems Research. MIS Quarterly.

Kaliyaperumal L.N. (2021). The Evolution of Security Operations and Strategies for Building an Effective SOC. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc

Knerler, K., Parker I., Zimmerman C. (2022). 11 Strategies of a World-Class Cybersecurity Operations Center. MITRE Corporation.

Maykish. P., (2014). C2 Rising: A Historical View of Our Critical Advantage in Air & Space Power Journal.

MITRE (2023). "ATT&CK Matrix for Enterprise," [online], https://attack.mitre.org/.

NIST (2016). Special Publication 800-150 Guide to Cyber Threat Information Sharing.

NIST (2022). SP 800-161 Rev. 1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

PECB, (2023). ISO/IEC 27001 vs, ISO 22301 vs. ISO 31000: What you need to know? https://pecb.com/past-webinars/isoiec-27001-vs-iso-22301-vs-iso-31000-what-you-need-to-know

Nunamaker, J., Minder Chen J. R. and Purdin T., "Systems Development in Information Systems Research," (3), pp. 89-106, 1991.

Simola, J., & Lehto, M. (2020). National cyber threat prevention mechanism as a part of the E-EWS.In B. K. Payne, & H. Wu (Eds.), ICCWS 2020 : Proceedings of the 15th International Conference on Cyber Warfare and Security (pp. 539–548). Academic Conferences International. https://doi.org/10.34190/ICCWS.20.106

United States Government Accountability Office, (2015) Critical Infrastructure Protection. Sector-Specific Agencies Need to Better Measure Cybersecurity Progress.

White House, (2013). Presidential Policy Directive/PPD-21 -- Critical Infrastructure Security and Resilience

Yin, R.K. (1994). Case Study Research: Design and Methods, 2nd edn. Sage Publishing, Thousand Oaks.