Developing Cybersecurity in an Industrial Environment by Using a Testbed Environment

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

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

Abstract: Critical infrastructure protection requires a testing environment that allows the testing of different kinds of equipment, software, networks, and tools to develop vital functions of the critical industrial environment. Used electrical equipment must be reliable, capable and maintain a stable critical industrial ecosystem. An industrial business needs to develop cybersecurity capabilities that detect and prevent IT/ICT and OT/ICS threats in an industrial environment. The emerging trend has been to create security operations center (SOC) services to detect ICS-related threats in enterprise networks. The energy supply sector must consist of crucial elements for safe business continuity and supply chain management in the industrial sector. Threats have changed into a combination of threat types. Hybrid threats may prevent everyday industrial activities, processes, and procedures so that supply chain problems may become long-lasting and affects business continuity management.

The project CSG belongs to the (Cybersecurity governance of operational technology in the sector connected smart energy) research project consortium of Business Finland's Digital Trust Programme.

The first research paper regarding the CSG (Cyber Security Governance) project concentrates on the applied theory background of this project. The research provides a research approach for investigating cyber security at the operational and technical levels. It answers the questions of where to concentrate on OT-related cyber security research and how we aim to deploy a testbed to develop a governance model in the CSG project. The study's primary purpose is to describe the operating OT-SOC environment and analyze system requirements for optimizing situational awareness in the testbed environment.

Keywords: Cybersecurity, Operational Technology, Security Operations Center, Governance Model, Testbed

1. Introduction

Business Finland-funded CSG project will develop a cybersecurity system integrated reference model to cover the common cybersecurity solutions, processes, and architecture for operational technology environments (CSG consortium). The model will be validated in several experimental implementations. The model will enable the establishment of common and standardized capabilities towards creating a competitive advantage in the global business in securing industrial automation. The University of Jyväskylä (JYU) and Turku University of Applied Sciences (TUAS) are research partners. The University of Jyväskylä coordinates the project.

CSG (Cybersecurity governance of operational technology in sector-connected smart energy networks) Significantly increases the effectiveness and efficiency of cybersecurity of smart energy networks and other operational technology. The project aims at considerable cost savings and scalability through enhanced incident management, data gathering, and Artificial Intelligence based automation. The rapid escalation of cybersecurity threats has given rise to operations centers dedicated to handling them. The SOCs – Security Operations Centers are generally considered to be best provided as a service, especially for those wishing to concentrate on their actual business rather than mastering the multifaceted attributes of cybersecurity. Cybersecurity of operational technology (OT), also called industrial control and automation systems (ICS), has been brought into the spotlight. Maersk, Norsk Hydro, and SolarWinds are recent examples of attacks with dramatic consequences (MITRE, 2022).

The unstable and insecure situation in Europe has caused a reaction that the Western world to prepare for a more effectively changing security environment. Protecting critical infrastructure, such as the electrical grid, against hybrid threats is more important than ever in history (Idaho National Laboratory, 2018). Past decades have been relatively peaceful, but nobody knows what may happen next year. European Commission set new kinds of regulatory requirements for the EU member states. In addition, trade between Western states and Russia has almost stopped caused by sanctions.

This paper provides a research approach for investigating cyber security at the operational level and answers the question of where to concentrate on OT environment cyber security research and how we aim to deploy a

testbed to develop a governance/reference model in the CSG project. The paper emphasizes the importation of a testing platform for the CSQ project at the beginning of the research project. After the first research paper, the research will be able to continue to identify and specify the comprehensive cyber security requirements and aspects for the development of OT reference model architecture, like threat and vulnerability investigations, risk assessment, and cyber security measures in an operational environment. The project's main goal Is to develop a governance and reference model for the industry stakeholders.

2. The research objectives and background in the CSG project

2.1 Essential cybersecurity requirements

European Union Agency for Cybersecurity (ENISA) is the agency that works under the European Union purposed to achieve a high common level of Cybersecurity across Europe. ENISA contributes to EU cyber policy, aims to enhance the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes, and cooperates intensively with the Member States (ENISA, 2023).

For example, Directive (EU) 2022/2555 (known as NIS2) entered into force, replacing Directive (EU) 2016/1148. The directive aims to improve the existing cyber security status across the EU in different ways by:

- Creating the cyber crisis management structure (CyCLONe). The European Cyber Crises Liaison Organisation Network, EU-CyCLONe, will support the coordinated management of large-scale cybersecurity incidents.
- Increasing the level of harmonization regarding security requirements and reporting obligations
- Encouraging Members States to introduce new areas of interest such as supply chain, vulnerability management, core internet, and cyber hygiene in their national cybersecurity strategies.
- Bringing novel ideas such as peer reviews for enhancing collaboration and knowledge sharing amongst the Member States
- Covering a larger share of the economy and society by including more sectors (more entities are obliged to take measures to increase their level of cybersecurity) (EC, 2022).

2.2 Definition of IT and OT environment in the research

Information technology (IT) and operational technology (OT) have their stories. Typically, OT is used in production environments consisting of hardware and software systems that monitor and control physical equipment and processes. The stakeholders need to know more about how operational technology-related cybersecurity should be managed from a connectivity viewpoint in their system.

There is a growing need to increase the effectiveness, efficiency, and scalability of cybersecurity of OT, leading to the adaptation of capabilities of IT cybersecurity and integration of IT and OT.

Automation and using Artificial Intelligence and Machine Learning (AI/ML) will bring a competitive advantage in answering, especially scalability. In energy solutions, sector integration means integrating various energy sectors into electricity transfer networks that increase the overall complexity of the electricity networks. Still, it also enables them to balance out each other's peaks in consumption and generation, with benefits toward carbon-neutral and flexible energy systems. Compared with legacy power systems, the smart energy networks (SEN) are envisioned to fully integrate energy distribution and high-speed and two-way communication technologies into real estate, industrial factories, smart buildings, households, and millions of power equipment to establish a dynamic and interactive infrastructure with new energy management capabilities, such as demand response. It is expected that CSG will enhance the partners' capabilities and develop common capabilities, making significant steps forward in increasing competitive advantage.

2.3 Central terms

2.3.1 C2 and Service Operational Center (SOC)

Background about the term Command and Control center often refers to operative control processes and procedures of military actions. The Security Operations Center often operates 24/7, and key functions may consist of monitoring and managing customer´s security entity, developing and implementing procedures, responding to security events, analyzing customers' network traffic, providing threat intelligence reports, and implementing other security plans targets (Vielberth et al., 2020).

2.3.2 Critical Infrastructure (CI)

The systems and assets, whether physical or virtual, are so vital to society that the incapacity or destruction of such may have a debilitating impact on security, economy, public health, safety, environment, or any combination of these matters (NIST, 2018a).

2.3.3 Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS)

ICS consists of supervisory control and data acquisition (SCADA) systems that control assets and distributed control systems in different places geographically. Industrial control system (ICS) means several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (e.g., manufacturing, transportation of matter or energy) (Stouffer K., Falco J., Scarfone K., 2011). Many Cyber-Physical System applications can cause irreparable harm to the physical system under control and the people who depend on it. In particular, protecting our Critical Infrastructures that rely on CPS, such as electric power transmission and distribution, Industrial Control Systems (ICS), oil and natural gas systems, water and wastewater treatment plants, health-care devices, and transportation networks, play a fundamental role in our society. Their disruption can have a significant impact on individuals and nations at large. Cyber-Physical Systems are often operated under automated controls, and a sophisticated cyberattack can exploit weaknesses to its advantage (Hevner & Chatterjee, 2010).

2.3.4 IIoT

A smart grid system may consist of IT, a discrete system of electronic information resources organized for collecting, processing, maintaining, using, sharing, disseminating, or disposing of information. The Industrial Internet of Things (IIoT) collects data from connected devices (for example, smart connected devices and machines) in the field or plant. Then it processes these data using sophisticated software and networking tools. The entire IIoT requires a collection of hardware, software, communications, and networking technologies (Electronical Technologies, 2016)

2.4 The testbed environment of the project

CSG project aims to advance considerably in raising the cybersecurity effectiveness, efficiency, scalability, and automation of OT environments, developing novel AI/ML techniques, proactive security assurance, data gathering and filtering, and a decision support approach.

A reference model will be developed to address cybersecurity system integration, consisting of a secure smart energy sector integration governance model and an OT governance model. The goal of this model and the above-mentioned novel cybersecurity approaches together is to form a comprehensive and pioneering ecosystem for OT cybersecurity with significant business potential in international industrial automation and smart energy markets. Use cases applied in an authentic environment make it possible to test solutions and create best practices for the stakeholders. Crucial cybersecurity elements in the project consist of a) Proactive security assurance and cognitive support. b) Data gathering and decision support automation. c) Reference model consisting of governance model (including sector integration and OT cybersecurity).

This paper provides a research approach for investigating cyber security at the operational and technical levels. It answers the question of 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. The study's primary purpose is to describe the operating OT-SOC environment and analyze system requirements for optimizing situational awareness in the testbed environment.

The research approach consists of two pillars. Firstly, we have a testbed and platform to test electrical equipment such as relays and software representing critical network elements in an energy and electricity environment. The equipment we will get from stakeholders from the industry and IT sector. We have a network traffic “manipulator” that allows us to manipulate the quality of the traffic and make it possible to make delays on those. The tested equipment is crucial for stable business continuity and enables functionalities of workable industrial electric networks and ICT networks. The software that we use comprises two main categories. Open-Source-based OT-SOC software will monitor the operations and transfer relevant information to the OT-SOC of the University of Jyväskylä. Another software class belongs to industrial equipment such as IPS devices.

The built OT-SOC (Operational Technology-Security Operational Center) environment will reflect the real-life SOC environment. Testbed -work in the Jyväskylä testing laboratory will be parallel and develop the upper-level reference model. The model will be based on the results of use cases and inner and outer level-specific requirements that are considered. The Use-case inputs from testbed work in a simultaneous environment and analysis of threat assessment-based risk scenarios will create outputs for the first proposal of the governance framework.

2.4.1 Space and Configuration

There are some requirements for the designing process of creating a testbed environment.

a. The testing environment should be situated in a quiet space where different equipment combinations are possible to test, and it should have several electrical and network connection possibilities, such as sockets. Technical and electrical requirements are crucial. There must not be any extra factors causing interference. It must be a secure space where only a few selected researchers have access rights.
b. Servers, routers, tools, computers, testing components, and equipment comprise physical elements of the testbed in the SOC.
c. Monitoring software such as intrusion detection software comprises a monitoring platform for tests. In addition, the tested electrical equipment has different kinds of software and procedure to update the firmware, for example, by using a mobile.
d. Electrical networks and wired or wireless data and telecommunication network types establish the capacity to communicate, monitor traffic flow, and share information between the devices in different ways. Communication channels such as cables, Wi-Fi, LTE, and ethernet links create Information sharing entity.

The project aims to develop capabilities to monitor, detect, mitigate, and respond to OT-related cyber-physical threats and prevent and predict possible cyber-attacks. Preventative and predictive capabilities require artificial intelligence-based features. The features of the testbed-SOC concentrate on analyzing abnormal events in equipment, such as OT devices, but also abnormal traffic between them by using SOC software and IDS-tool. It also tests the features of the OT devices.

Figure 1 shows the configuration of the test environment.

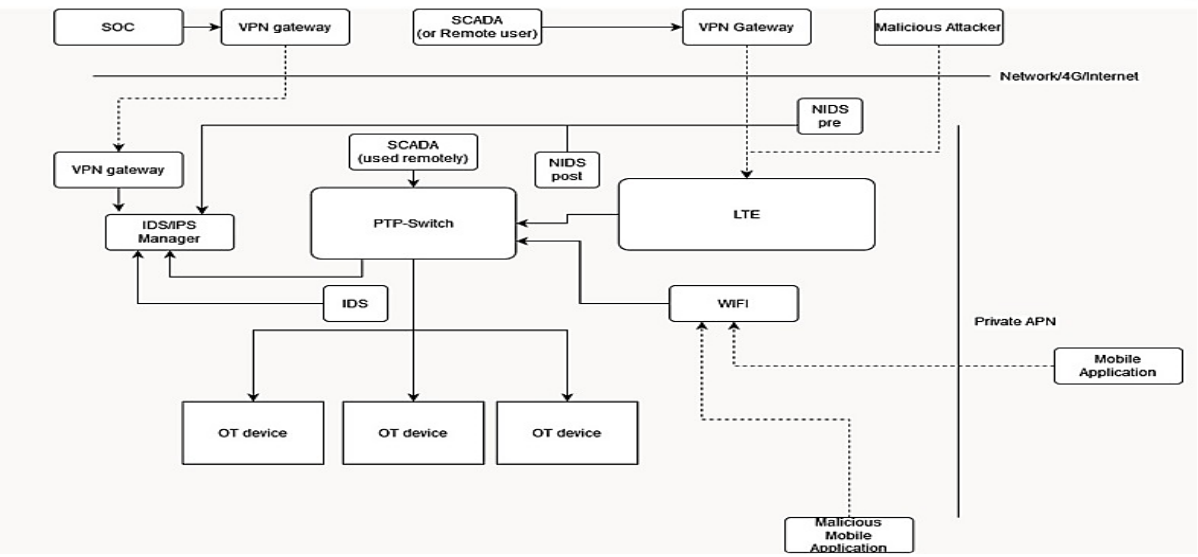

Figure 1: The testbed environment

Although the testing environment is not comprehensive, it is possible to create simulation models that demonstrate critical infrastructure-related group-based risks and scenarios that are a reality in production lines in an industrial atmosphere. It is not reasonable to test hundreds of solutions and operational technologies-based equipment combinations, but it is possible to create upper classes where to place tested use cases. The goal of the project defines the requirements for the testbed environment. There is also an “a-by project” target to produce data for the new OT-related cybersecurity standards at the industry level.

2.5 Typical OT-related Industrial threats

As Bodeau, McCollum & Fox (2018) wrote, the word threat refers to the adversary or the attack, depending on the context.

2.5.1 Industroyer

Industroyer is a sophisticated malware framework designed to causing impact the working processes of Industrial Control Systems (ICS), specifically components used in electrical substations. The industry is the first widely known malware specifically designed to target and impact operations in the electric grid (MITRE, 2022).

2.5.2 Data Destruction

Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt the availability of systems, services, and network resources. Data destruction will likely render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives. Common operating system file deletion commands such as del and rm often only remove pointers to files without wiping the contents of the files themselves, making the files recoverable by proper forensic methodology. This behavior is distinct from Disk Content Wipe and Disk Structure Wipe because individual files are destroyed rather than sections of a storage disk or the disk's logical structure (MITRE, 2022).

2.5.3 Manipulation of Control

Adversaries may manipulate physical process control within the industrial environment. Control manipulation methods can include changes to set point values, tags, or other parameters. Adversaries may manipulate control systems devices or possibly leverage their own to communicate with and command physical control processes. The duration of manipulation may be temporary or longer sustained, depending on operator detection (MITRE, 2022).

3. Research methodological approach

The aim is to utilize several cybersecurity frameworks to define the IT and OT ecosystem in the industrial environment.

NIST framework for the Critical Infrastructure (NIST, 2018a) is a crucial general tool for the initial research. The five simple core functions of the framework are as follows a) Identify, b) Protect, c) Detect, d) Respond, and e) Recover (NIST 2018a; NIST 2022). SP 800-37 rev2. The risk management framework for information systems and organizations with the cybersecurity framework of NIST (2018b) create more detailed issues for overall risk management. NIST Special Publication 800-150 (2016) guides how to share cyber threat information.

We have used for the initial analyses cybersecurity tools of MITRE ATTA&CK (2022a, 2022b, and 2022c), 800-53rev.5 (Security and Privacy Controls for Information Systems) (NIST, 2020) and Special Publication 800-1612rev.1) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations NIST (2022). Publication 1500-201 from NIST in Volume 2 provides an overview of the timing awareness in system elements and latency in CPS and describes special security issues concerning timing" (NIST, 2017).

MITRE's ATT&CK describe the actual attackers and their actions behind archetypes. The database provides an updatable list of detected techniques, tools, and groups. (Strom et al., 2018). ICS-related threats, actions, and tactics are also described. The database helps to form potential scenarios and consequences.

The Delphi method is suitable for conducting a relevant testbed environment analysis. The members that have been involved in this analysis process are researchers and also research methods. "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).

According to Yin (2014), the case study illustrates the attempt to produce detailed information about the object being researched. The materials collected for this case study are based on technical publications, official reports, and scientific literature.

4. Results

4.1 Where to focus cybersecurity assessment and development?

How the cyber security framework/frameworks will be used in this research project is based on an agreement with the project collaborators. The framework core provides a set of activities to achieve specific cybersecurity outcomes and references examples of guidance to achieve those outcomes. It must present key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk (NIST, 2022).

We have used MITRE ATTA@CK frameworks and matrix for the threat and risk analysis work in the ICS environment (MITRE, 2020a, 2020b, 2020c). Table 1 illustrates the adversary's tactical goal in the ICS environment. Even though IT and OT environments are linked more often to each other's, they differ fundamentally from adversaries' views. Reputation and increased costs affect business continuity for all enterprises, small or big (Idaho National Laboratory, 2018). Affected OT systems are not so easy to detect. The initial research indicates that crucial vulnerabilities are related to human-based activities.

Table 1: Adversaries' tactics (Mitre 2022b)

ID	Name	Description
TA0108	Initial Access	The adversary is trying to get into the ICS environment.
TA0104	Execution	The adversary tries to run code or unauthorizedly manipulate system functions, parameters, and data.
TA0110	Persistence	The adversary is trying to maintain their foothold in the ICS environment.
TA0111	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0103	Evasion	The adversary is trying to avoid security defenses.
TA0102	Discovery	The adversary is locating information to assess and identify their targets in the ICS environment.
TA0109	Lateral Movement	The adversary is trying to move through the ICS environment.
TA0100	Collection	The adversary tries to gather interest and domain knowledge data on the ICS environment to inform their goal.
TA0101	Command and Control	The adversary tries to communicate with and control compromised systems, controllers, and platforms with access to the ICS environment.
TA0107	Inhibit Response Function	The adversary tries to prevent safety, protection, quality assurance, and operator intervention functions from responding to a failure, hazard, or unsafe state.
TA0106	Impair Process Control	The adversary tries to manipulate, disable, or damage physical control processes.
TA105	Impact	The adversary tries to manipulate, interrupt, or destroy the ICS systems, data, and their surrounding environment.

Table 2. below indicates threat events that may affect in several ways to the OT-environment. From the view of the supply chain, the higher-level threats are more complex to govern than lower-level threats, and the consequences affect expansively.

Table 2: Examples of initial risk scenarios

Manmade events or Natural disasters	Potential consequences	Governance model scenario for Security operations (People, process, technology)
Power surges, frequency fluctuations,	Unstable operations, loss of situational awareness, production interruption, loss of reputation, cost increase	Information about frequency variation and effects, detection, mitigation, prevention, protection, repair, and information sharing with stakeholders
Electrical voltage fluctuations	Unstable operations, loss of situational awareness, production interruption, loss of reputation, cost increase	Voltage information management – detection, mitigation, prevention, protection, repair, and information sharing with stakeholders.
Structural or hostile events (physical sabotage)	Unstable operations, production interruption, loss of reputation, cost increase	Information about power supply problems, detection, mitigation, prevention, protection, repair, and information sharing with stakeholders
(cyber-attacks, man-in-the-middle, jamming, cyber-physical attack)	Unstable operations, production interruption, loss of reputation, cost increase	Information about abnormal cyber-physical events, detection, mitigation, prevention, protection, repair, and information sharing with stakeholders.
Configuration manipulation	Unstable operations, loss of situational awareness, production interruption	Information about abnormal events, detection, mitigation, prevention, protection, and information sharing with stakeholders.

Manmade events or Natural disasters	Potential consequences	Governance model scenario for Security operations (People, process, technology)
Third-party software or equipment.	Information sharing for unknown actors-unstable operation, loss of situational awareness, loss of reputation, loss of service reliability	Information about abnormal events, detection, mitigation, prevention, protection, and information sharing with stakeholders.
Environment (flooding, lightning, storm, earthquake)	interrupted production processes, and continuity management problems. two-way effects	Information about abnormal cyber-physical events, detection, mitigation, prevention, protection, and information sharing with stakeholders.
Remote update	parameters changes, unstable operations, loss of situational awareness, interrupted production processes	Information about abnormal events, detection, mitigation, prevention, protection, and information sharing with stakeholders.

The NIST (2015) specifies relevant key factors and requirements that drive design decisions regarding the control, communication, reliability, and redundancy properties at the ICS system level as follows: Control timing requirements, geographical distribution, the hierarchy of supervisory control, control complexity, the system's availability (reliability) requirements, the impact of a failure of control, the system's safety requirements.

4.2 Risk Management and Governance

There are many possibilities to understand the term governance or governance model. The primary function of a governance model is to organize the strategic, operational, and tactical/ technical level cybersecurity functionalities based on regulations, policies, guidelines, standards, and protocols. The cybersecurity governance model must consider the workplace culture, financial factors, risk and threat management, other security plans, and reporting processes that already exist in a company so that the board receives all the information it needs to put the goal of governance into practice.

The cybersecurity governance model must answer the question, how does an organization control and manages its security? Defining the risk-taking level, establishing responsibility frameworks, and determining responsibility for decision-making are essential parts of designing a governance model. The initial research indicates that the designing process of the governance model cannot be a separate part of the testbed results. There should be limitations, parameters, procedures, processes, how to deal with the different kinds of information-sharing situations, and how to share the data in a form by using a procedure that everyone understands and can work by using the same methods and procedures, and processes as other stakeholders (NIST, 2016).

There should also be an information-sharing connection between security operations centers and domain-based sectors. Information-sharing entities where to share and obtain information create added value for cybersecurity risk management. If the information-sharing method and process for the public safety authorities are not established, the threat information does not flow as required by the national and EU-level regulations. The national cybersecurity authority is the relevant actor in this case.

The research indicates that every industrial component and equipment combination is not impossible to simulate. Stakeholders have hundreds of different kinds of operational lines in their plants. That does not mean the tested combination of components and equipment does not reflect the crucial problems of the industrial environment. Creating higher-level classes and types of OT-related vulnerabilities, threats, and risks is possible. In addition, separate business units located in different locations must be standardized with each other within the business sector. The research indicates that IT- and OT-SOC -functions should be combined in the same security operations centers functionalities. Keeping those threat detection capabilities under different supervision operations makes no sense. It is meaningful to use the term SOC which consists of controlling, monitoring, detecting, possible counterattacking, and mitigation features. There is a fundamental need to reach initial threat signals from the OT factory environment that may inform SOC personnel about the potential risks that are not recognized. If the enterprise uses an operational control or supervision room in the factory, there has to have a 24/7 monitored information-sharing connection to the SOC. The SOC may also work as a filter that informs and changes the entity where the component and equipment are. Predictive features slow down operations before any serious harm happens.

4.3 Industrial sector operations and cyber security governance

People, processes, and technology are the key capabilities in the OT environment, but at the same time, they include vulnerabilities. All these parts should be covered to have high-level situational awareness of relevant threats, vulnerabilities, risks, and cyber security measures. ISO/IEC 27001:2013 (ISO27001) is the international standard for information security that specifies an information security management system (ISMS). The ISMS

assists organizations in managing their information security by addressing the people, processes, and technology (International Organization for Standardization, (ISO, 2013). NIST produces a voluntary set of guidelines for cybersecurity risk management. NIST Cybersecurity Framework (CSF) supports all other essential guidelines and standards (NIST, 2018a; NIST, 2022).

4.3.1 People: Stakeholders

A new cyber security model for governance driven by knowledge of vulnerabilities, threats, assets, potential attack impacts, and the motives and targets of potential adversaries is required. Securing the cyber aspects of an interconnected system of industrial environment hosted by multiple stakeholders requires a system-of-systems view in cyber security to analyze the whole operating environment. The organizations' stakeholders should have strategic, operational, and tactical/technical views of the cyber structure of their operational environment (Simola & Pöyhönen 2022).

At the strategic level, choices are primarily related to the organization's social responsibility, reputation, and business continuity (Finnish Standards Association SFS, 2016). The measures at the operational level promote the strategic goals, and thus, comprehensive measures will increase situational awareness for holistic cyber security management. It must be based on risk assessment and analyses of the measures based on the assessment. Maintaining cyber situational awareness concerning the organization's processes makes it possible to monitor and react efficiently to risks that constitute a threat within the organization's operating environment (Simola & Pöyhönen, 2022).

Consistent and predictable results are achieved more efficiently when operations are handled and managed as interrelated processes that function as a coherent system (Finnish Standards Association SFS, 2016). Cyber security threats and risks set special requirements for these processes and the need for situation awareness at this level in addition to other operational requirements. The targets can be achieved by defining the processes to be protected, choosing process control mechanisms successfully, and by using expedient technological solutions and services to protect the processes in the cyber environment (Stouffer et al., 2011).

4.3.2 Processes of industrial operations

Processes are key to the implementation of an effective cybersecurity strategy. Processes are crucial in defining how the organization's activities, such as governance, roles, and documentation, are used to mitigate the risks to the organization's information. Processes also need to be continually reviewed: cyber threats change quickly, and processes must adapt. People have to follow them correctly (Dutton, 2017).

4.3.3 Technology: Industrial systems

Technology is a crucial factor in the operational processes in an industrial environment. By identifying the cyber risks that an organization faces, start to look at what controls to put in place and what technologies you'll need to do this. Technology can be deployed to prevent or reduce the impact of cyber risks, depending on your risk assessment and what you deem an acceptable level of risk (Dutton, 2017).

Protecting systems, working methods, and procedures at strategic, operational, and tactical levels, security functions, and defense-in-depth strategy elements of stakeholders have to identify correctly. (Homeland Security, 2016). Effective working environments require effective cyber threat prevention mechanisms, but in addition to this, security operations must be able to eliminate combined cyber-physical threats.

5. Discussion and Conclusions

Firstly, this paper presents a research framework for the testbed work of cyber security in industrial operations and processes. It has two pillars and several research tasks. Testing platforms concentrate on practical tests, and the abstract base of research supports constructive development work. The Workable ICT and ICS systems are crucial factors for stable business continuity and risk management of the operational processes. Stakeholders must have strategic, operational, and tactical/technical level standardized security plans and guidelines consisting of cybersecurity sections to perform their daily working routines as securely as possible. Companies' coherent decision-making requires a common understanding of situational awareness about the situation from the industrial environment. Built testbed environment makes designing a cybersecurity structure for the repeatable and transferrable reference model possible. The Applied testbed environment supports to development of holistic cyber security architecture for the OT environment by using the guidelines mentioned

earlier in this paper. The proposed testbed solution is suitable for reflecting real-life operations from a real industrial environment.

Security elements like people, processes, and technology are the key capabilities in the cyber environment, but at the same time, these capabilities also include vulnerabilities. Vulnerabilities and threats can be divided into internal and external sources. Situation information from industrial production processes, relevant stakeholders, and technologies behind equipment, like machines and logistic systems, are needed to cover risk assessment in an industrial environment. This procedure is essential for monitoring IT and OT systems and sub-systems' health. The SOC that handles cyber-physical threats from the industrial control ecosystem is needed in the industrial environment and industry sector.

Technological development will challenge traditional physical monitoring systems and information-sharing methods. In the future, more than the human capacity-based ability to follow the flow of threat information or abnormal events from simple screens are required. Automated artificial intelligence-aided constitutes an opportunity to maintain supply chain and continuity management in control.

Requirements for threat visibility require gathering and analyzing data from the industrial environment and potential threats from outside. Standardized OT environments for digitalized systems and processes, procedures, data storing, data handling, etc., are needed in the near future. Efficient strategical, operational, and tactical situational understanding require SOC functionalities covering all system enterprises. Threats and vulnerabilities have to tackle before they affect a production line at the factory. All these issues made it possible to answer the research questions: where to concentrate on OT -related cyber security research and how we aim to deploy a testbed to develop a governance model in the CSG project.

References

Bodeau, D. J. & McCollum, C. D. (2018) System-of-systems threat model. The Homeland Security Systems Engineering and Development Institute (HSSEDI) MITRE: Bedford, MA, USA

ENISA, (2023. About Enisa. https://www.enisa.europa.eu/about-enisa

European Commission (2022) Directive (EU) 2022/2555. https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

Department of Defense. (2011) DoD Dictionary of Defense of Military and Associated Terms.

Dutton, J. (2017) Three pillars of cyber security. -09-26T10:00:51+00:00, [viewed April 2, 2023]. Available from: https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security.

Electrical Technology. (2016) Internet of things (IoT) and its applications in the electrical power industry http://www.electricaltechnology.org/2016/07/internet-of-things-iot-and-its-applications-in-electrical-power-industry.html.

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 25.4.2023

Finnish Standards Association SFS (2016) Johdanto laadunhallinnan ISO 9000 -standardeihin. Available on 3 April 2023: slideplayer.fi/slide/11133323/

Hevner, A., & Chatterjee, S (2010) Design research in information systems: Theory and practice. Springer Science and Business.

Homeland Security (2016) Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team.

Idaho National Laboratory (2018) Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector

International Organization for Standardization (ISO) (2013) ISO/IEC 27002:2013 Security techniques — Code of practice for information security controls. ISO. Available from: https://www.iso.org/standard/54533.html.

MITRE (2022a) "ATT&CK®for Industrial Control Systems"[online], https://attack.mitre.org/matrices/ics/

MITRE (2022b) "tactics," [online], https://attack.mitre.org/tactics/enterpise

MITRE (2022c) "ATT&CK Matrix for Enterprise," [online], https://attack.mitre.org/.

NIST (2015) SP800-82 Guide to Industrial Control Systems (ICS) Security

NIST (2016) SP 800-150 (2016) Guide to Cyber Threat Information Sharing

NIST (2017) SP 1500-201 Framework for Cyber-Physical Systems: Volume 1, Overview

NIST (2018a) Framework for Improving Critical Infrastructure Cybersecurity

NIST (2018b) SP 800-37 rev2. (The risk management framework for information systems and organizations with the cybersecurity framework)

NIST (2020) 800-53rev.5 (Security and Privacy Controls for Information Systems)

NIST (2022) NIST SP 800-1612rev.1) Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Simola, J., and Pöyhönen, J. (2022) Emerging Cyber Risk Challenges in Maritime Transportation. In R. P. Griffin, U. Tatarand, & B. Yankson (Eds.), ICCWS 2022: Proceedings of the 17th International Conference on Cyber Warfare and Security

(pp. 306-314). Academic Conferences International. The proceedings of the international conference on cyber warfare and security.

Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G. and Thomas, C.B. (2018) “Mitre Att&ck: Design and Philosophy”, Technical report.

Stouffer K., Falco J., Scarfone K. (2011) NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce. Available on 3 December 2021: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

Vielberth M., Böhm, F., Fichtinger I. and Pernul G. (2020) "Security Operations Center: A Systematic Study and Open Challenges," in IEEE Access, vol. 8, pp. 227756-227779, doi: 10.1109/ACCESS.2020.3045514.

Yin, R.K. (2014) Case Study Research, Design and Methods. 5th ed. Thousand Oaks: Sage Publications.