

HANNING ZHAO

Visualizing Operational Cybersecurity:
Enhancing Situational Awareness in
Industrial Environments

This and the following page will be replaced in the printing house.

The series, ISBN and ISSN numbers are added on this page in the library.

This and the preceding page will be replaced in the printing house.

Dedicated to those writing dedications.

Seriously, have FUN

with it.

PREFACE/ACKNOWLEDGEMENTS

Preface or acknowledgements here.

the skiff has passed ten thousand mountains

ABSTRACT

The integration of Information Technology (IT) and Operational Technology (OT) in the Industrial Internet of Things (IIoT) has transformed industrial operations, enhancing efficiency and intelligence across a range of critical infrastructures and IIoT sensors in Industry 4.0. However, such environments also introduce new cybersecurity challenges due to the increase in cyber attacks targeting industry. Consequently, effective security monitoring and management become crucial and demanding tasks for both field operators and cyber defenders. Therefore, the primary aim of this study is to develop novel cybersecurity visualisations for IIoT systems in three diverse industrial scenarios, including building automation, maritime industry, as well as smart mobile machines. The proposed security visualizations are designed to reinforce cyber situational awareness among multiple stakeholders roles and contribute to a collaborative cyber defense within these industrial environment.


This research explores the complexities inherent in the integration of IIoT and OT, focusing on the unique challenges that poses for effective security visualization. The primary objective is to develop advanced visualization tools to enhance cybersecurity situational awareness within diverse industrial environment. security visualization techniques and information sharing in operational environments has been as effective common tools and strategies for improving situational awareness of different users.

By Employing a multidisciplinary approach, this study integrates key principles from computer science, data visualization, cybersecurity and industrial engineering. The goal is to conceive innovative visualization solutions for cybersecurity management of IIoT systems. These developed security visualization will be tailored to three predetermined industrial scenarios. Furthermore, the research will investigate appropriate techniques for evaluating effectiveness and holistic usability of security visualizations in industrial environments.

TIIVISTELMÄ

Other abstract text here, e.g. in Finnish.

CONTENTS

1	Introduction	17
1.1	Security Visualization	17
1.2	Research Questions	18
1.3	Scope and Research Contribution.	19
1.4	Thesis Structure	22
2	Background/Related Work	25
2.1	OT/IT.	25
2.2	IoT devices and technologies	25
2.3	SIEM.	27
2.4	Cyber situational awareness	27
2.4.1	industrial CSA	30
2.5	data?	30
2.6	Existing work in CSA visualization	30
2.7	Other Security dashboards	33
3	Research Methodology	35
3.1	Design Science Research Methodology	35
3.2	Systematic Literature Review	37
3.3	User-Centered Design	38
4	Primary Stakeholder Roles	41
4.1	Cybersecurity stakeholders across industries	41
4.2	Key stakeholders in Maritime  building automation	43
4.3	Workflows	47
5	c5	51
5.1	Visualization Interfaces Design	51

5.2	Maritime	51
5.2.1	Building automation/security analysts	53
References	55
Appendix A	Appendix	65

List of Figures

List of Tables

1.1	Research questions addressed in six publications	19
2.1	Research questions addressed in six publications	33
4.1	Stakeholder roles supported by current visualization systems.. . . .	42
4.2	Stakeholder roles in two industrial sectors as studied in Publication 1 and Publication 3.	44

List of Programs and Algorithms

ABBREVIATIONS

3D	Three Dimensional
ADS	Anomaly Detection System
API	Application Programming Interface
AR	Augmented Reality
CBOR	Concise Binary Object Representation
CoAP	Constrained Application Protocol
CPS	Cyber-Physical System
CSA	Cyber Situational Awareness
e.g.	for example, from Latin <i>exempli gratia</i>
et al.	and others, from Latin <i>et alii</i>
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IODEF	Incident Object Description Exchange Format
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
JSON	JavaScript Object Notation
LWM2M	Lightweight Machine-to-Machine
MR	Mixed Reality

OMA	Open Mobile Alliance
OT	Operational Technology
REST	Representational State Transfer
SIEM	Security Information and Event Management
SOC	Security Operations Center
UCD	User Centered Design
UI	User Interface
UX	User Experience
VR	Virtual Reality
XML	Extensible Markup Language

Author's contribution

The contribution of Hanning Zhao to each of the publications listed aforementioned included in this dissertation as follows.

- | | |
|----------------|--|
| Publication I | The author is the primary contributor to this paper. The main contribution is to design security visualization platform for maritime industry. By analyzing identifying multiple stakeholder roles and their requirements, three security visualization systems have been developed for operational maritime cybersecurity. The design of those visualization platform is tailored by customized use interfaces and visualization widgets to support their own security operation. The visualization platform targeting to increase different stakeholders roles' situational awareness of cybersecurity status of a operational port and fairway area also facilitate collaboration in terms of incident exchange among multiple stakeholders. A scenario of collaborative cybersecurity defense is presented and has revealed how operational security visualization can helps in maritime industry. |
| Publication II | This publication focuses on designing visualization platforms for supporting incident exchange among different stakeholders in |

two industrial scenarios. The author defined and analysed various stakeholder roles and the workflow of incident exchange among these roles. The outlined workflows illustrate how the roles of each stakeholder are interconnected during both the operational phase and the flow of the supply chain. Additionally, different sample incident reports for common cyber attacks for IoT and industrial environments have been created and evaluated based on open standard using three data representations. The author is the first author of this publication.

Publication III This paper describes an building automation scenario where security visualization can be applied for increasing cybersecurity situational awareness. The author proposed a User-Centered design method for designing security dashboard for non-experts in smart building use case. The publication studies the Sigfox-based IoT systems and multiple stakeholder roles as well as their needs in terms of cybersecurity management. According to different stakeholders, three security dashboards have been developed and evaluated by different stakeholders. The author was also responsible for the design of usability testing and results analysis from user testings of developed dashboards.

Publication IV The publication proposed an approach of using LwM2M standard for cybersecurity monitoring and incident exchange among multiple stakeholder roles within industrial environments. The author implemented data models for security related data, and evaluated the effective of the proposed system in maritime scenario. The publication studied three differed data representation supported by proposed LwM2M system and measured the bytes of traffic data based on different formats in a collaborative cyber defense use case. Key resulted have been presented and analysed.

Publication V The author conducted a systematic literature review in existing cybersecurity visualization in industrial and operational environment. The publication aims to provide a holistic review of security visualization systems, previous survey related to cyber-

security visualization have been studied and analysis. The author proposed the taxonomy of surveyed papers and presented the key findings as well as research gaps. By analysing existing literature, visualization techniques and implementation methodologies have been summarised. Future directions of research on security visualization have been highlighted. The author is the primary contributor to this paper.

Publication VI Novel method for evaluating security visualization.

1 INTRODUCTION

1.1 Security Visualization

In the last decade, the cybersecurity visualization (VizSec) research community has been actively engaged in the exploration and examination of diverse visualization techniques and platforms tailored to support the endeavors of security professionals [11, 69]. Broadly speaking, cybersecurity visualization, also known as security visualization, encompasses a multifaceted domain that intersects big data, visualization, human perception and security [47]. Specifically, it has been grown as mature term as *"the creation of charts, graphs, and analogous visual representations derived from cybersecurity data within a well-defined context, as visual interfaces play a pivotal roles in amplifying cognitive activities of human operators."* [12, 66]. As increasing challenges in cybersecurity domains, especially recent cyber attacks has targeted to industrial sectors, aiming at critical infrastructure [33], security visualization becomes more significant for human operators. Some studies used the word of security visual analytic too [7, 77].

Industrial operational environments, such as manufacturing plants, utility services, and transportation systems, are essential to the functioning of society. They operate using a blend of legacy systems and cutting-edge technologies, making them uniquely challenging to protect. Traditional IT security solutions often fall short in addressing the specific needs of industrial systems, which require continuous operation and have stringent safety and reliability requirements. More specifically, in such environments, the convergence of Operational technology (OT) and IT has introduced new cybersecurity challenges, especially in light of the escalating cyber threats and attacks [4, 68]. Diverging from IT systems, OT encompasses both the hardware and software components responsible for monitoring devices, processes, and critical infrastructures within industrial environments [10]. Moreover, a growing multitude of Internet of Things (IoT) devices that are incorporated into OT networks also have

become the main victims in recent attacks. Current tools such as Security Operations Center (SOC) and Security Information and Event Management (SIEM) has been applied for threats initiation and situation awareness,, for supporting the human factors and effective information comprehension from machines, security visualization, has played a big role in the whole pictures [20, 17, 10]. .

Security visualization can increase cyber situational awareness by provide efficient and meaningful insights to overwhelming amounts of data, allowing decision makers to both explore and monitor the cyber status at various abstractions levels [20, 22]. However, there is still a notable deficiency of using such visual tools for industrial and operational environments, within which there is a growing demand for applying visualizations to enhance situational awareness [13, 33].

non-security expert users [72].

By leveraging the use of graphical elements to represent security data and leverages human visual perception to facilitate a quicker and more accurate understanding of security-related information. It enables the identification of patterns, detection of anomalies, and the comprehension of complex cyber threats and vulnerabilities, to arrive at informed decisions more effectively.

This doctoral thesis aims to address the critical gaps in using security visualization for increasing cyber situational awareness within integrated OT networks. By investigating the intricacies of IoT-OT integration and the challenges it poses for security visualization, this research endeavors to develop more effective methods and tools for assessing and communicating the security status across multiple stakeholders in industrial environments. Two industrial scenarios have been covered in this dissertation: building automation and maritime industry. Through an interdisciplinary approach that draws on concepts from computer science, data visualization, cybersecurity, and industrial engineering, this thesis seeks to contribute to the advancement of knowledge in the realm of cybersecurity situational awareness in industrial.

1.2 Research Questions

The main objective of this research is to strategically address the existing gap in security visualization for IoT devices within operational industrial environments. This goal poses the main research question of this dissertation as to "*how can security visualization being leveraged to increase cybersecurity situational awareness in op-*

erational environments". To thoroughly address this research issue, the study will include several focused sub-questions as follows:

- **Research Question 1:** Which types of security data from IoT devices and networks are essential to visualize for the operational environment?
- **Research Question 2:** How can visualization tools be adapted to reinforce the cybersecurity situational awareness among various stakeholder roles in industrial environments?
- **Research Question 3:** What are effective visualization techniques and how to evaluate these proposed visualization solutions?
- **Research Question 4:** How do different industrial contexts influence the design and functionality of security visualization tools, and what are the best practices for customization?

All these four formulated research questions aims to explore about using visualization in operational environment to support multiple stakeholders in terms of cybersecurity management and collaboration. Table 2.1 shows the publications focus on addressing different research questions.

Table 1.1 Research questions addressed in six publications

-	P1	P2	P3	P4	P5	P6
RQ 1	x				x	
RQ 2		x	x	x	x	x
RQ 3			✓			
RQ 4						

All four research questions are structured to address three focus areas: *Cybersecurity visualization*, *Cybersecurity management*, and *Design and evaluation*. The following section will elaborate on how each of the six publications correlates with these areas, offering a detailed mapping and discussion.

1.3 Scope and Research Contribution

This dissertation focuses on designing and developing novel cybersecurity visualizations in a multiple-stakeholder operational environments. The scope of the dissertation lies in designing cybersecurity visualization for increasing cybersecurity situa-

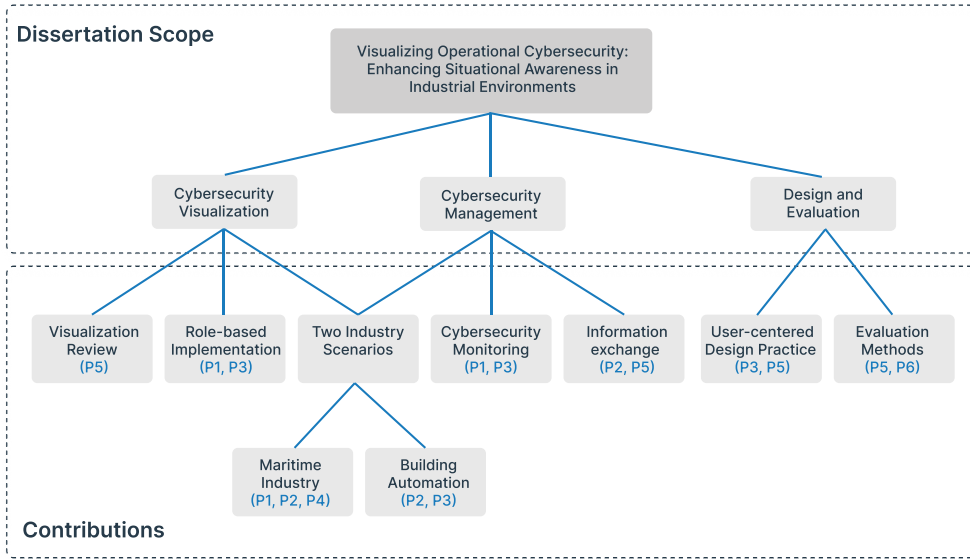


Figure 1.1 Dissertation scope and research contribution.

tional awareness across multiple stakeholders within two defined industrial scenarios and implement the effective and usable visualization for cybersecurity management as well as evaluation the developed systems. Figure 1.1 below illustrates the overview of research scope and contribution.

The research scope includes three focus areas when considering how cybersecurity situational awareness can be reinforced by visualization tools: *Cybersecurity visualization*, *Cybersecurity management*, and *Design and evaluation*. It primarily addresses how these practices can be leveraged to enhance situational awareness and operational efficiency against the backdrop of ever-evolving cybersecurity threats. The main contributions derive from those three areas and two defined industrial scenario has been defines: Building automation and maritime industry. Both industrial has been digitized equipment with IoT devices and sensors for facilitating operation and management efficiency. Building automation refers to smart buildings and apartments where different IoT sensors has been installed for physical and security monitoring. Maritime industry in this dissertation specifically addresses on the smart harbour and fairway area where smart devices have been installed for navigation and pilotage. Both two industrial have been considered as can be benefited from security visualization in terms of cybersecurity management and collaborations.

In addition to two industry scenarios, the first focus area - *Cybersecurity visualization*, includes the review as the foundation of this study and also exploration of visualization techniques design. The literature review of security visualization provides more insights and research gaps and directions for this study. Thus, a spectrum of different types of cybersecurity can be considered relevant as foundation for this dissertation, especially when designing in different industrial sectors. Main contribution are:

- Literature survey of existing operational security visualization in industrial scenarios, showing the landscape of security visualization systems.
- Identification and analysis of diverse stakeholder roles in two industrial sectors, as well as their security operations.
- Choosing effective and usable visualization techniques based on different stakeholders' profiles and needs. adaptive to support users to achieve context-specific comprehension and management of IoT devices and networks.
- Implementation role-based visualization systems within the maritime industry and building automation sectors, thereby supporting different stakeholders' roles with most suitable visualization techniques.

The main objective of developing effective security visualization to enhance the cybersecurity situational awareness, thus *Cybersecurity management* is a crucial goal for achieved. It covers two both cybersecurity monitoring and security-related information exchange, focusing on the strategies and frameworks for managing cybersecurity, particularly how visual tools can support decision-making processes and operational responses. Designing visualization for allowing the holistic security monitoring and collaboration among multiple stakeholders is the second focus areas in this dissertation and main contribution can be summarised as follows:

- An analysis of security collaboration among multiple stakeholders, including their own responsibilities, workflow in terms of incident handling in two industrial scenarios.
- Devising standard-based data models for modeling the cybersecurity health of devices and systems in industrial environments. analysis risks the threats in different use cases.

- Implementation of security visualization platform for supporting operational security monitoring and exchanging security issues and incidents in two industrial scenarios.
- Evaluation and Analysis of serialisation efficiency of exchanged messages with three data formats.

The last focus area is *Design and evaluation*, which aims to uncover the methodologies used in the design of security visualization within industrial environments and the strategies for evaluating developed visualization solutions in environments involving various stakeholders. This dissertation primarily explores user-centered design practices and introduces innovative evaluation techniques tailored to scenarios involving multiple stakeholders.

- Analysis the research gaps in employing UCD in security visualization development in industrial environments.
- Development of UCD method for security visualization in automation building automation scenario.
- AI based evaluation methods for helps in UCD evaluation, measuring the usability and effectiveness of developed security visualization platforms based on different stakeholder profiles.

1.4 Thesis Structure

The rest of the structure of this dissertation as follows. Chapter 2 explained the background work, starting with introduction of operational environment and techniques are involved, as well cybersecurity situational awareness with detailing its definition and taxonomies. this Chapter 2 also points out, introduces the Security information and event management (SIEM) solutions. Chapter 3 focus on the challenges and research methodologies have been used in this doctoral research. it mainly follows Design Science Research methodologies and a system literature review has been conducted for studying the existing security visualizations. Also User-Centered Design method is presented and discussed.

Chapter 4 present the security visualization design and techniques selected for adaptive visualization in two industrial scenarios. Chapter 5 shows cybersecurity management solutions, the implemented systems support both security monitoring

and information exchanges. Chapter ?? evaluation methods for usable visualization. Chapter ?? presents the discussion and results in light of the four research questions. Chapter ?? concludes the dissertation and provides future direction of the research.

2 BACKGROUND/RELATED WORK

2.1 OT/IT

What is operational environment?

IT/OT cobvernegncet referesto
digitisation,
the different of [25]

OT systems were designed to integrate data acquisition systems, data collection/-transmission systems and Human Machine Interface (HMI) systems to create a centralised control and monitoring solution. Thus, allowing an operator to visually interpret the state of the plant for control and monitoring purposes (Shahzad et al., 2015).

figure show steh diferent and also covernerncy,
when in industrail, avavaibility is the top poriroort of the enveionements.

operational environment in this dissertation refers to " *operational industrial environment*" and " *operational environments*" interchangeably in this paper, to refer to industrial environments encompassing all systems and networks that contain a diverse, heterogeneous array of running endpoints. These endpoints include critical Operational Technology (OT) and Information Technology (IT) systems, as well as connected Internet of Things (IoT) devices and networks. "

2.2 IoT devices and technologies

The Internet of Things (IoT) has allowed ubiquitous internet connection of smart devices and objects for sensing environment, process and transmit surrounding data. A growing number of devices and systems has been deployed in various industries domains, to enable both safety monitoring and efficient interaction between digital counterpart and physical world, where also address as a Cyber-Physical System

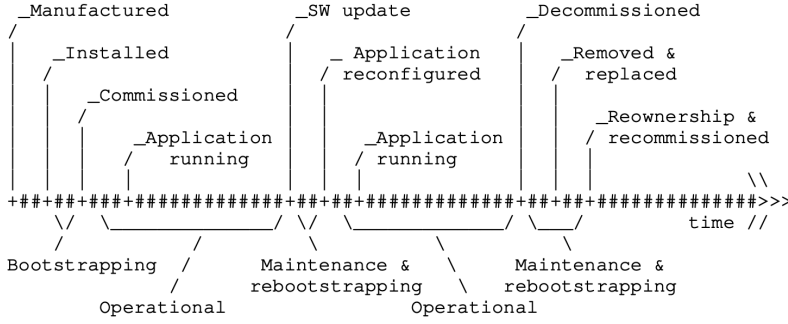


Figure 2.1 The lifecycle of a Thing in the IoT from [21, 26].

(CPS) [67]. Several definitions of IoT have been proposed. Working Group within the Internet Engineering Task Force (IETF) denotes IoT as "*the interconnection of highly heterogeneous networked entities and networks that follow a number of different communication patterns, such as: human-to-human (H2H), human-to-thing (H2T), thing-to-thing (T2T), or thing-to-things (T2Ts).*" in RFC 8576 [21]. While in RFC 7452 [71], the term "Internet of Things" (IoT) simply denotes as "*a trend where a large number of embedded devices employ communication services offered by Internet protocols.*" The definition from NIST [61] addresses the IoT as network of devices, but also contains the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.

While IoT typically covers consumer devices in retail and lifestyle, its subset Industrial Internet of Things (IIoT), focuses mainly on OT environments, including smart manufacturing process, smart logistics, and smart cities [70]. IIoT covers the the domains of machine-to-machine (M2M) and industrial communication technologies with automation applications. It paces the way for efficient and sustainable production and automation in a wide range of industrial sectors [67]. The Industrial Internet of Things (IIoT) refers to "*the application of instrumentation and connected sensors and other devices to machinery and vehicles in the transport, energy, and other critical infrastructure sectors.*" [48].

For both consumer IoT and industrial IoT, the lifecycle of devices is crucial both devices and security aspects. [26], proposed the lifecycle of an IoT devices and it is applicable to distinct applications and scenarios, it divides the lifecycle into three stage: Bootstrapping, Operational; Maintenance and Re-bootstrapping. RFC 8576 [21], also utilised the same lifecycle framework as shown in Figure 2.1. Each device

and its components can come from several different manufacturers before factory assembly. Assembled devices are transported to vendors or installers. Afterwards, they will be installed in various industrial environments such as a smart city, maritime harbour etc. Upon joining the network and becoming operational they provide end-user services. During this operational phase, the device is under the control of the system owner. For devices with lifetimes that span several years, occasional maintenance cycles may be required.

During each maintenance phase, the software on the device can be upgraded or applications running on the device can be reconfigured. The maintenance tasks can thereby be performed either locally or from a back-end system. The end of the bootstrapping phase is marked by the IoT device being able to connect and communicate on the network, in addition to having the location of the server and the correct security credentials to interact with the management server. Once the client is registered with a server for management, the IoT device enters into its operational state, where it can securely communicate with other devices and services. IIoT has been a crucial issues in operational environment, and they are also commonly cases for security vulnerability, work [75] shows a comprehensive architecture for showing the security based on lifecycle and highlighted the attack surfaces and common vulnerabilities of IoT devices. [70] have mentioned that the stricter safety and security requirements of IIoT and two commonly identified security requirements are the ability to monitor infrastructure.

2.3 SIEM

The difference of the our visualization and SIEM systems.

2.4 Cyber situational awareness

Situational Awareness (SA) has become well-studied subject with numerous definitions have been proposed. In the work of Jiang et al. [33], SA is defined as "*refers to the human cognitive capacity to analyze its environment and act accordingly.*" and have been acknowledged as a crucial element for effective decision-making across a wide variety of contexts. The other widely applicable definition provided by [15] is "*the perception of the elements in the environment within a volume of time and space, the com-*

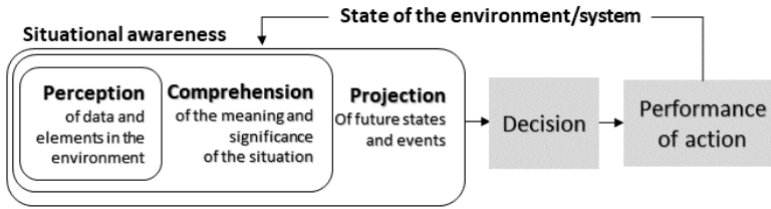


Figure 2.2 Three levels model of SA adapted from [33].

prehension of their meaning and the projection of their status in the near future". Endsley believes that SA is explicitly recognised as a construct separate from decision making and performance, holding with such believe, Endsley proposed the three hierarchical phases as illustrated in 2.2. This three-level model shows the primary components of the definition of SA while [55] extends it to the four levels:

- Level 1: *Perception* of the Elements in the Environment, The first step in achieving SA is to perceive the status, attributes, and dynamics of relevant elements in the environment.
- Level 2: *Comprehension* of the current Situation: different elements in the perception level. This allows users to go beyond simply being aware of the elements in the environment to comprehending the situation.
- Level 3: *Projection* of Future Status, This is achieved through knowledge of the status and dynamics of the elements and comprehension of the situation (both Level 1 and Level 2 SA).
- Level 4: *Resolution*, necessary actions that deal with controls to repair, recover, remedy and resolve the perceived situations [55].

Therefore, a successful decision-making is based on a good building of SA, especially comprehending and projecting future development, rather than a simply perception of the surroundings and environments. Based on SA of individual, the team SA is determined by each members' SA and shared knowledge, those overlaps forms team SA and help for making and performance of action. In team work, each member's SA will be shaped by their specific roles and responsibility. the quality of a overall team SA of shared knowledge may serve as an index of effectiveness of human-machine interface or team coordination [15].

In the context of a cyber environment, Cyber SA, has been identified a subset of overall SA, Jiang et al. [33] defines CSA "*refers to the gathering of information, along with the perception and comprehension of the cybersecurity posture of specific environments.*" In Franke et al. [20] 's work, CSA has two aspects: *technical aspect* and *cognitive aspect*. The authors believe that the *technical aspect* of SA involves data fusion, including data gathering, acquiring, compiling, processing, and analyzing data. The integration of information and data stands out as critical elements for supporting human assess present conditions and forecast future states. On the *cognitive aspect*, SA is concerned with an individual's mental awareness within a specific context, particularly a person's capacity to comprehend the technical implications and synthesize insights to facilitate decision-making and performance of action. The work of Collo et al. [10] also combined concepts of cybersecurity and information security SA, pointing out the goal of both concepts aims to increase the knowledge levels of employees regarding potential security threats, risks and vulnerabilities.

The three-model architecture along with the two aspects of SA have laid the groundwork for subsequent research on the development CSA architecture and taxonomy. More specifically, the architecture of CSA developed by [38] consists of four components: *Data fusion, Visualization; Humane machine interface and Information sharing*. The similar CSA taxonomy is developed in Evesti et al. [17] 's study, the author states the goal of Cybersecurity SA as "*to know what is going on in the networked systems, what is their current estimated security level, and what are the causal relations that realise any observed risks.*" the proposed Cybersecurity SA taxonomy includes three critical components: *Data gathering (operational and strategic); Analysis; Visualization*.

With highlighting the CSA as an essential part of cyber defense, later research work [29] has outlined improved version of CSA taxonomy that combines the three models of SA and developed CSA taxonomy in [17]. Figure 2.3 illustrates the taxonomy CSA components and tool based on three levels of SA. This work has pinpointed unique features of SA in the cyber environment from the three-level model perspective. The complementary CSA tools allows cybersecurity operators to cope with the complexity of cyber threats and landscapes [29].

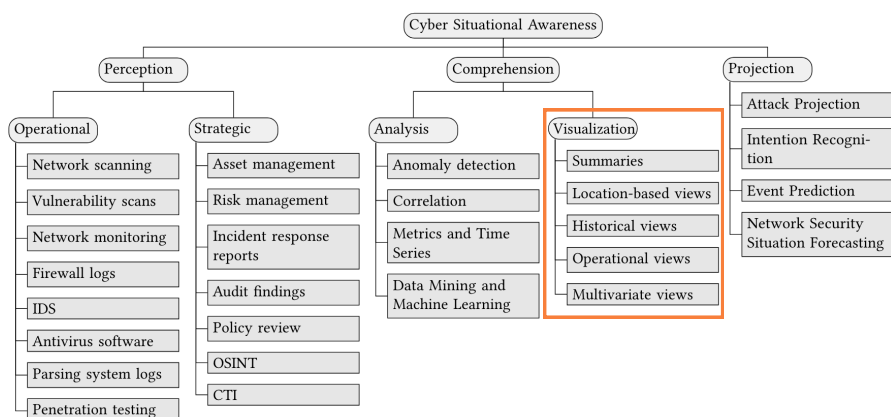


Figure 2.3 taxonomy of CSA and role of visualization in [29].

2.4.1 industrial CSA

ICS CSA [2]. Compared to the SA in the cyber environment, cybersecurity SA in the industry is also indicates the but also includes the SA of physical of devices team collaboration CSA [60]

2.5 data?

[9] how emplotree can work from the CSA to ehance and increase the for tehtr security oerston and the imiportantce for them to be aware of security risks and security issues "

security monitoring, data analysis [35].

Figure 2.4

The capability of a powerful SA system is highly related to the quality of data and collection processes such as automation, real-time data collection, or available datasets.?? [1]

2.6 Existing work in CSA visualization

Analysis and visualization can support for human operators' comprehension of cybersecurity status of the environments.

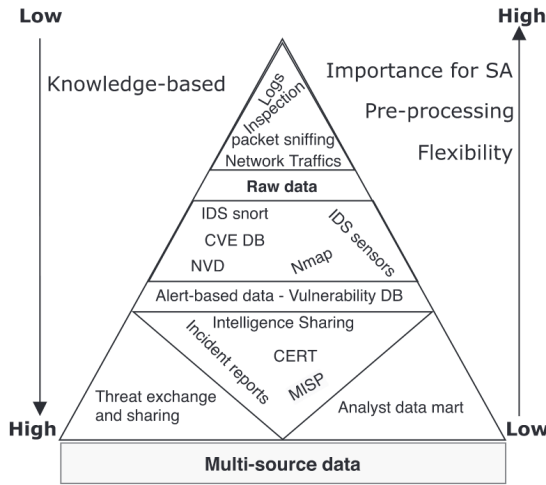


Figure 2.4 multiple data types in [1].

SOC can be the part of effective tools for increasing CSA.

in work of [72], the authors delimited SOC security operation center from other concept as Security Information and Event Management (SIEM): so SOC represents an organizational aspect of an enterprise's security strategy. It combines processes, technologies, and people to manage and enhance an organization's overall security posture. However, SIEM is an integral part of many SOC's to cover a large part of the technological requirements. It is responsible for collecting security-relevant data in a centralized manner [72].

[57] states that SIME is expensive and required alot time for learning and training, [44]

Visualization has been a critical component in CSA development and group into the tools for implementing comprehension level of CSA [17, 29, 38]. As it shown in Figure 2.3, data visualization has been categorized as four types according to their purposes and features: *Statistic summaries*; *Location-based views*; *Historical views*; *Operational views*; *multivariate views*. most current visualization systems are developed as security dashboard.

Security visualization has been a long standing research area [66, 58, 69]. Numerous of visualization systems have been developed for network security and anomaly in the cyber environment. Cyber defense involves human engagement and operations in a constantly dynamic and strategic environments, where CSA can helps

humane be area what is going on.

guideline for designing cybersecurity visualization [64]: visualization design is to provide the human cyber defender with efficient and effective perception, comprehension, and decision-making in an automated and real-time manner, monitor and thwart cyber attacks.

In the work of [66, 39], the author argued that Visual data analysis help to perceive patterns, trends, structures, and exceptions in even the most complex data sources. The study believed that the ultimate goal of a network security visualization is to provide a high-level view of security events to system analysts for more timely and informed decisions, and pointed out the future direction as *developing processes and algorithms that prioritize situations and project critical events*. Additionally, other security visualization reviews also have shows that one common goal of security visualization for increasing CSA, both Zhao et al. [77] and Zhang et al. [76] states that analysts are able to achieve by raising the overall awareness of network anomalous state through CSA integrated with data from various network devices.

While cybersecurity has became challenging in industrial environment that digitizing has been implemented. current focus has been shift from traditional IT system and computer network to operational environment, explore their visualization for increasing in CPS system [8] explore the security visualization for CPS system, a literature review has been developed for a smart grid case.

However, most existing security visualization are produced only for support the comprehension level of CSA, with realizing this research gap, [33] conducted a systematic literature review for security visualization gaining in-depth and holistic insights into the state-of-the-art CSA visualization. This review provides the analysis of three CSA levels that can be achieved through the proposed visualization systems.

Security visualization have been seen as critical part of SIEM while provide interfaces to human operators, for effortlessly comprehend the security situation and take swiftly responded to cyber threats or incidents. support the comprehension level of CSA, with realizing this research gap, [24] However, industrial environment,

visualziation techniques, and those ones for cybersecurityindustrail and environemnts so that information sharing other visualizations for information exchange, security incident exchange, collaboration,

most security visualization has been develop as dashboard. the design of dashboard and concepts [31, 19]: *A dashboard is a visual display of the most important*

information needed to achieve one or more objectives that has been consolidated in a single computer screen [or printed page] so it can be monitored at a glance. most are security dashboard and includes different views.

dashboard patterns [5] mentioned based on analytic dashboard and below tables shows some example of industrial visualization

Table of visualizations in industrial scenarios.

Table 2.1 Research questions addressed in six publications

-	P1	P2	P3	P4
ERTenr et al. [43]	monitoring and ninoly detcteon	water treat plants	Operators; Analyst	spiral chart

2.7 Other Security dashboards

[62], smart

visualization [53],

dfeinds it as three parts, ensure proetctcion of data and netwokrs, system,,

arasing knewldes and of security alers, security risks, provide knowdlegs and aware of cyber attcks

[9] how emplotree can work from the CSA to ehance and increase the for tehirs security oerstion and the imiportantce for them to be aware of security risks and security issues “

vsualziation conectes and how it works with the constcrurctu for this, [23]

both mentioned the data share, [17][10]

both mentioned the data share, [17][10]

wate vis [43], [29], [10], [evesti2017cybersecuity], [52], [50], [49], [74], [sethi2017expert], [46], [41], [39], [56], [46], [31], [63], [15], endsley’s model of three layers of security vsialzuations studied

[32], [6], [65], [3], visualization mostly related work, situational awareness

[41], [65], [8], [33], [58], [maddigan2023chat2vis],

3 RESEARCH METHODOLOGY

This chapter presents the main research methodologies have been applied in the dissertation. Design Science Research Methodology has been primitively used in the included publication, a systematic literature review have been followed by one publication while UCD method is being both used and studied in two publications for designing security visualization systems.

3.1 Design Science Research Methodology

This study undertaken for the dissertation falls into a category of research methodology known as Design Science Research Methodology (DSRM) [56]. DSRM is the predominant research methodology used for Information Science research. The principle of “Design science . . . creates and evaluates IT artifacts intended to solve identified organizational problems” [27]. It refers to a rigorous process to design artifacts to overcome observed problems, making research contributions and evaluating the designed artifacts, and communicating the research results to appropriate audiences [27]. It is envisioned as a process model that consists of six activities in a nominal sequence, namely:

1. Problem identification and motivation;
2. Definition of the objectives for a solution;
3. Design and development of a research artefact;
4. Demonstration;
5. Evaluation;
6. Communication.

DSRM has been seen as a potential methodology for ensuring the acceptance of Design Science research [56]. In this dissertation, all Publication 1 to 6 follows this

six activities in their research work and following section detailed in accordance with six steps in following section.

Problem identification and motivation:, one common challenge and problem lies in two distinct industrial scenarios is the low cybersecurity situational awareness. this results from IT/OT integration while multiple stakeholders' in such scenario complicates the cybersecurity monitoring and collaboration. Also recent work shows the shift focus from using security visualization in IT networks to operational industrial environments. The research problem have been clearly defined in all Publication 1-6. The motivation behind this study is from the surge numbers of attack in industrial recently, resulting in a high demand of visualizations for OT and CPS systems, with a solid expectation for using such tools can supports both security professional and non-experts mitigating cybersecurity threats and incidents.

Definition of the objectives for a solution: The objectives of the developed solutions should be based on the identified research problems. All Publications clarified the objective for developed solution. In both building automation and maritime industry, requirements and goals of cybersecurity visualization and back-end cybersecurity management system is clarified and documented.

Design and development of research artefact: Creation of the artefacts includes both functionality and architectures as solutions to overcome, resolve the identified research problems. Publication 1- 5 include development, wither its visualization systems or solution of cybersecurity data management. Two security visualization systems has been developed, severing for two different industrial scenarios - building automation and maritime industry. Publication III shows the designed visualization user interfaces of multiple stakeholders for different usage. In addition to user interface design, a lightweight solution of cybersecurity management and incident exchange system has been developed in Publication IV.

Demonstration: When proof-of-concept-level prototypes are developed, the artefacts are adapted to use and tested. Publication 1,2,3,5 include demonstration activities while both developed security visualization systems and platform for monitoring and incident exchange have been presented for diverse stakeholders in two industrial environments during project seminars and review meetings.

Evaluation: This activity includes an analysis of how well and effective the developed research artefact achieves the objectives of solutions. Publication 1,2,3,4 shows the evaluation session for developed security visualization. Publication 3 focus on

user experience perspective by following a UCD study using a usability testing. In publication IV, visualization system platform developed, based on LwM2M system, the implemented solution has been evaluated with incident reports, which demonstrating the feasibility of the system.

Communication: Manuscripts relating to research work has been published in academic conference proceedings and journals. All six Publications 1-6 are peer-reviewed and have been presented in hosted scientific conferences. Publication 1 has been presented virtually due to COVID pandemic.

3.2 Systematic Literature Review

The definition of Systematic Literature Review (SLR) is a method to identify, evaluate and interpret all existing available research relevant to a particular question, or topic, or phenomenon of interest [37]. This method has been widely used as a way of synthesising scientific evidence to answer a specific research question in a way that is transparent and reproducible, while seeking to present all existing published evidence related to the topic in a trustworthy, rigorous and editable way [40, 36].

In Publication 5, the SLR methodology has been used to get a systematic analysis of current research work related to security visualization, aims to identify research gaps in the current visualization landscape. The results do not only provide the observations and insights from existing practices, including use cases, visualization techniques implementation, but also shed light for research work in industrial environments.

A 8-step review process proposed by study [54] has been followed: Identify the purpose; Draft protocol and train the team; Apply practical screen; Search for literature; Extract data; Synthesize studies; Write the review. Also the procedures of SLR in this dissertation have taken inspiration from the methods outlined in [33]. The gathered papers through Systematic Literature Review method have undergone both qualitative and quantitative analysis, as detailed in Publication 5.

Other non-systematic literature methods such as targeted literature review and gap analysis [28] have been used in Publication 1,2,3,4 and 6. The main goal of targeted literature review is to take an in-depth approach to a particular question but avoid the all-encompassing review, considering how time and resources consuming of conducting SLR. Publication 1,2,3,4 have performed such literature review be-

fore designing security visualization systems for different industrial scenarios. Gap analysis has been seen as an analysis of topic areas in which evidence is sparse or nonexistent, often conducted as part of a literature review [28], all Publication 1-6 have conducted such analysis when identifying the research gaps and insufficient work in existing literature review. Publication 1 and 3 show the shortage of using security visualization in building automation and the maritime industry.

3.3 User-Centered Design

The main approach used in this dissertation for security visualization design is User-Centered Design (UCD) method combined with a persona-design method which used for representing users' requirements [51]. UCD is a well-known method aims at designing the products by involving users throughout the design process. As defined by the ISO 9241-210 standard [34], the objective of using UCD aims to make interactive systems more usable by focusing on the use of the system and applying human factors and usability features. The user-centered design process, as described in the ISO 13407 [30] standard, establishes four activities that start, from the conception of considering the user's needs for the development of the software products, until the evaluation of developed systems. Figure 3.1 illustrates a general UCD process contains the four activities, which have been adhered in Publication 3 for designing security visualization dashboard in building automation scenario.

Understanding and specifying the context of use: Specifying the goal of security visualization is critical since cybersecurity visualization is such a broad concept including multiple aspects such as network security, malware detection and so on. Thus, the context of use such visualization significantly shapes the design of product and our target is focusing on increasing human users' situational awareness in smart buildings.

Specifying the user and organizational requirements: Knowing the users is quite highly priority for usable design and it helps to clarify their actual needs and requirements. Publication 3 has defined multiple stakeholders roles regarding their background and work tasks based on their profile. Both interview persona-design have been conducted for a deep understanding and identifying their needs and requirements for security visualization. this allows authors to get more ideas of how visualization dashboard can support end users' work and what has been crucial elements for security and safety.

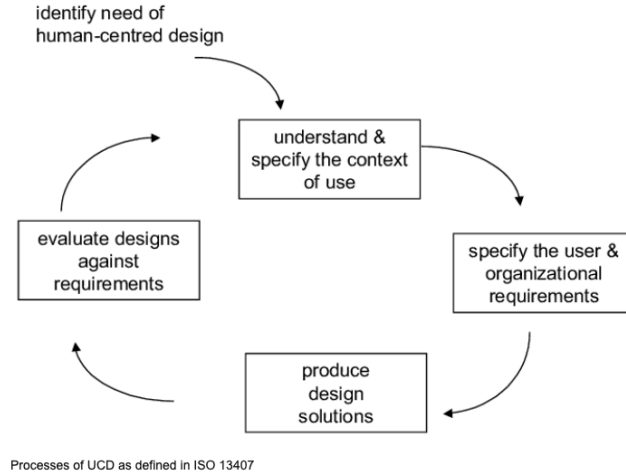


Figure 3.1 Four steps of a design process in UCD method [30].

Producing design solutions: The proposed design is based on the analysed requirements of end users. The common objective of security visualization is to increase both cybersecurity and safety situational awareness in smart home. So the security visualization designed for house managers is an at-one-glance dashboard showing holistic view of security posture. This security dashboard is designed with easy-to-follow visualizations that reflecting the overview safety status and cybersecurity situation of SigFox devices and network in the smart buildings. a mobile application is designed for visualizing the security information in their smart home. The designed high-fidelity prototypes of both visualization solutions and iterated once after testing with end users.

evaluating designs against requirements: The designed solutions were evaluated by usability testing and interviews with end users. Generally, usability testing the usability evaluation methods are defined as procedures which are “composed of a set of well-defined activities for collecting usage data related to end-user interaction with a software product and/or how the specific properties of this software product contribute to achieving a certain degree of usability [18]. To get more information about the users’ cognitive processes, the participants are usually asked to think aloud while conducting the test tasks [42]. Through such a process, the strength and weakness points of the system were uncovered and discussed. We tested the visualization solu-

tions with 6 participants from each user group. After usability testing, we conducted structured interview with each participant to get more feedback and suggestions. Based on these results, we had another iteration of the design and made it align with the preferences of the end users.

Publication 3 presented the use of UCD methods during security development. The design follows the same procedures as suggested in Figure 3.1. Requirements were derived from an understanding of stakeholders' roles within the context of building automation. Three developed security visualization dashboards have been evaluated and tested with the intended end-user roles. Current research work has showed the usage and limitations of using such methodology in visualization and more industrial use cases are needed, as discussed in Publication 5.

4 PRIMARY STAKEHOLDER ROLES

This chapter presents the study on identifying and analyzing key stakeholder roles in the operational environment. Those stakeholders who have benefited from security visualization show different needs and demands for security monitoring based on their profiles. Publication 5 reviews existing security visualization systems and provides a taxonomy of distinct targeted stakeholder roles across various industry sectors. Publication 1 and 3 define several primary stakeholders in the maritime and building automation industries, respectively. In publication 2, additional stakeholder roles from the supply chain process are included for a comprehensive analysis.

Although a wide range of stakeholders are involved in operational environments, this dissertation emphasizes the roles of stakeholders who are actively participating and responsible during the operational stages, especially considering the workflow when security incidents occur. All publications 1, 2 and 3, also primarily focus on the profiles and needs of those operational stakeholders.

4.1 Cybersecurity stakeholders across industries

Key stakeholders in cybersecurity management vary depending on different industrial and operational environments. Defining these stakeholders clarifies their needs and aids in understanding the context of their security operations. The generic stakeholder roles interacting with cybersecurity systems are broadly classified into two categories: *Non-expert* and *Expert* users. According to the study by [59], *expert* users are defined as "*those who have prior cybersecurity experience in terms of coding, configuring systems, system administration tasks, testing codes, or security experts.*" In contrast, *non-expert* users are "*those who do not possess any such specific skills, and simply interact with the systems for fulfilling their daily activities (either personal or professional)*". Non-expert users generally lack cybersecurity situational awareness.

Publication 5 summaries different stakeholders into the same two groups: *non-*

experts and *experts*, by reviewing existing cybersecurity visualization systems developed for various industrial environments. The differentiation between these two groups is crucial in understanding the profiles and dynamics of security operations of different stakeholder roles. More concretely, *non-experts* are these roles who have no deep cybersecurity expertise. One subgroup of non-experts are those who work on daily operation and management in the operational environments, for example, field operators, dispatchers and managers. The other non-experts may have some cybersecurity knowledge but limited expertise, for example, IT helps, software engineers who developed the systems for industrial usage. Both group plays play vital roles in maintaining operational security and efficiency, even though they lack of cybersecurity expertise.

However, *expert* users typically require specialized knowledge in cybersecurity. their responsibilities demand a expertise level of operations, including threats hunting, systems configuration, risk assessment or other mitigation implementation. In industrial environments, *experts* are clearly identified as part of dedicated security teams and their roles vary from security analysts, IT defenders to security officers or security managers.

Table 4.1 below provides a detailed overview of specific stakeholder roles across different industrial environments as extracted in Publication 5.

Table 4.1 Stakeholder roles supported by current visualization systems.

Industries	Experts	Non-Experts
Smart Grids	Analysts; Network security operators; Security operators; Cyber defenders; SOC operators; trainees.	Operators; Dispatchers; Building administrators; Power engineers; System engineers; Power grid staff; IT specialists; Instructors.
Smart Factories	Security teams.	Managers; Operators; supervisors; Operation staff.
Water Facilities	forensics experts.	Operators; Network administrators.
Generic ICS/CPS	Security officers; Analysts; IT defenders; Network security managers; Network security officers;	Operators; OT defenders; Systems designers; Military commanders.

This table also reflects the diverse nature of stakeholders within each industrial environment, with a diversity and the specificity of different roles. The division between experts and non-experts has been highlighted in the Publication5, which indicating cybersecurity management and collaboration among these stakeholders

role is multifaceted fired requiring the consisting understanding of different roles.

Among all stakeholder roles, cybersecurity analysts can be expected as who will cause most critical and long last mistakes since they work closely involved with the developing, working, and maintenance of IT systems [59]. However, the situational is the opposite in the operational systems. non-experts are might be the one who firstly spot some anomalies such as filed operators, either by noticing software failure from monitoring screen, or devices as well as machinery fault during their operations. thus their cybersecurity situational awareness is essential for ensuring availability of operational systems. Compared to traditional IT systems, cybersecurity situational awareness also included the physical systems, especially for operators, their concerns lay in how this cybersecurity risk or issues affect the operational status of the machine, or even physical security. Thus how also these distinction between those two different groups is critical, as it influences how security visualization systems are designed and implemented, to ensure that all stakeholders, from both user groups, regardless of their expertise levels, are adequately protected against or being aware of cyber attacks and threats.

4.2 Key stakeholders in Maritime & building automation

In order to further explore the specific roles in various industry environments, this dissertation analyzes two multi-stakeholder environments that need to strengthen cybersecurity situational awareness: the maritime industry and building automation.

Recognizing the cybersecurity challenges introduced by digitization in the maritime industry, Publication 1 examines the operational environment in the terminal area, especially defining the "port asset" as more than hardware and software systems as well as those associated infrastructure at the terminal, but also those IoT sensors, gateways and other intelligent devices situated close-by in the fairway area, which are considered navigational channels near the port. Recent cyber attacks targeting port assets have indicated the sector's deficient cybersecurity situational awareness. The diversity of stakeholders who taking part in port operation also has increased complexity of the port ecosystem. Therefore, both legacy systems and newly installed smart sensors and devices are susceptible to cyber threats and breaches without robust cybersecurity management.

Drawing on work of [14], Publication 1 identifies different key stakeholders in-

cluding both non-experts and experts have been defined to enhance comprehension of their involvement and collaboration in cybersecurity monitoring and defense. As shown in Table 4.2, *Terminal operators*, *Security analysts* and *Security managers* are listed as three primary stakeholders. Although port stakeholders includes more roles such as port authority, IT/OT staff and ship crews, these three key stakeholders are most representative ones for cybersecurity operations, they are responsible for threat monitoring and incidents response.

Likewise, another operational environment with low cybersecurity situation awareness is building automation. Publication 3 explores a residential area where smart buildings are installed with Sigfox IoT smart sensors, and devices. Those IoT devices are integrated to facilitate the monitoring of key physical parameters, such as motion detection, temperature, humidity, and air quality monitoring. Most stakeholders in smart buildings are *non-expert* users, and three various roles have been presented and discussed in Publication 3. Table 4.2 lists all three stakeholder roles.

Table 4.2 Stakeholder roles in two industrial sectors as studied in Publication 1 and Publication 3.

Maritime	-	Building Automation	-
Terminal operators	Non-Experts	House managers	Non-Experts
Security analysts	Experts	IT personnel	Non-Experts
Security managers	Experts	Residents	Non-Experts

In both multi-stakeholder environments, *non-expert* stakeholders have been seen as one of the most vulnerable assets in the cybersecurity defense due to as lack of awareness and cybersecurity training. These stakeholders generally have difficulties identifying the potential anomalies or keep dated with recent cyber incidents. Below shows more concrete profile of different *non-expert* stakeholders from two scenarios:

- *Terminal operators*: These stakeholders are physically present in the harbour area for managing daily operations for a safe and efficient cargo handling. They work closely with compliance with safety regulations and standards for a seamless terminal activities. To maintain the security and safety in the port area, they are responsible for cybersecurity monitoring of all port assets.
- *House managers*: Who are responsible for providing the maintenance of all smart buildings, overseeing the daily operation to ensure the safety and functionality for all residences. Their duties include handle administrative tasks, manage inventories and repairs work. Within smart building, they also need

to monitor and understand the cybersecurity situation of all smart devices, ensuring a secure and safe living environment.

- *IT personnel*: These stakeholders work at the third company who installed the smart sensors and device in smart buildings. Their main task is to provide technical support, including troubleshoot issues, devices upgrading, repairing work. They are responsible for managing and maintaining IoT devices and infrastructure, ensuring all smart devices and systems operate securely and efficiently. However, for certain cybersecurity incident, they need to contact security teams for further investigation.
- *Residents*: The inhabitants of the smart buildings with diverse background and personal experience. This user group represents the typical consumers base for IoT or other newer technology, predominantly consists of non-technical individuals who have no knowledge of IT or cybersecurity.

Among all these non-experts, only *IT personnel* may have limited knowledge of cybersecurity, while the rest of stakeholders lack cybersecurity expertise. The integration of smart devices in both port area and small buildings, has made these stakeholders' daily operations more efficient and productive. However, this advancement also necessitates that they acquire a basic understanding of the cybersecurity status within their operational environments. In most cases, they work closest to the operational stage of machinery, making them critical in identifying and encountering problems or spotting anomalies at the earliest stage.

In term of *expert* users, Publication 1 have explored their profiles and needs. In maritime industry, experts refer to "*who are security professionals. These users are proficient in a variety of security operations including security analysing, forensic investigation, threat detection, risk assessment, incident response and so on*". It is realistic that each stakeholder locate in the port area have their own security team. Thus, two roles have been defined in Publication 1 as *Security analysts* and *Security managers*. Both stakeholders work from the same security team belongs to one of stakeholders.

Security analysts are specialists responsible for investigating the cyber threats and risk, as well as potential attacks. They work report incidents to their responsible managers. for maintaining the overall cybersecurity by flattening threats, attacks and corrective responses undertaken on port assets to operators. They often report incidents to their responsible managers, and communicate with other stakeholder security teams. *Security managers* also belongs to security team, focus on handling

report from analysts and communicating with other stakeholder security teams as well as terminal operators.

In addition to those operational staff, Publication 2 also introduces the additional stakeholder roles from the supply chain process. Supply chain compromises have become one of the most prevalent initial infection vector towards the Information and Communication Technology/Operational Technology (ICT/OT). That make the various stakeholders' involvement and responsibilities regarding to cybersecurity management cannot be neglected. Following the brief description of various types of suppliers and providers in [16], Publication 3 defined four stakeholder roles as follows:

- *Manufacturers*: Factories that design, develop, manufacture, and deliver products and components to their customers. Sometimes these factories assemble the devices for different product users.
- *Vendors*: Firms that supply the devices or components including hardware and software components that can be purchased from multiple manufacturers.
- *Installers*: Private companies that design and deploy systems, including install the devices and provide software solutions. They provide services related to the installation, management, operation or maintenance of products, networks, infrastructure, applications or any other network and information systems, via assistance or active administration carried out either on customers' premises or remotely. [16]
- *Service Providers*: Network and cloud computing services providers, providing networking, storage and communications, also can be infrastructure as a service; platform as a service; software as a service (SaaS) and network as a service. They focus on ensuring the connectivity of devices and data transfer during operational phases.

Addressing supply chain cyber risks requires collaboration and defense from all supply chain stakeholders. It is evident that cyber risks arising from partners, suppliers and vendors could have systemic implications [16]. Effective ICT/OT supply chain cybersecurity requires commitment, direct involvement, and constantly support from all stakeholders. These four generic roles are identified in the publication 3, serving for a purpose that can be adaptive to both maritime and building automation scenarios. They also can be customized for other industry sectors.

*Should I separate operational roles and supply chain roles to different subsection?

4.3 Workflows

Workflow for cybersecurity management among various stakeholder roles varies in different industrial environment, it can change depending on regulations and custom in different scenarios even in the same industry. Illustrating workflow in a multi-stakeholder environments helps shows the communication flow between different stakeholders, which also indicates their different levels of cyber situational awareness.

In addition to these categories of key stakeholders, it is essential to consider their operation and interact with in a multiple-stakeholder environment. Particularly in terms of cybersecurity management, which highly demand collaboration and communication.

This thesis focusing on illustrating the workflow of , in incident sharing.

Publication 1 describes a collaborative cybersecurity defense scenario between multiple stakeholders work in different ports. In this scenario, one *Security managers* received a cyber incident which details an active malware infection at another port, and then they share the report to security analysts and terminal, for investigation and be aware of the incident.

For incident sharing,

Publication 2 provides a brief scenario of collaborative defense in maritime industry, the use case have revealed the workflow and communication between stakeholder's from security teams and terminal operators in a scenario of when security teams received the news of a ransomware attack has occurred in other port.

Publication 3 summaries the workflow for both maritime and smart buildings.

While non-experts usually cannot perform further investigate, the common workflow is to report security issues to expert users for assistance and security professional will perform analysis and check up on reported devices and systems.

Publication 3 further shows a detailed workflow including supply chain stakeholders' role for two industrial scenarios.

*how visualizations match to following sections, explain more. Figure 4.2 illustrates the workflow from two industrial use.

connecting,

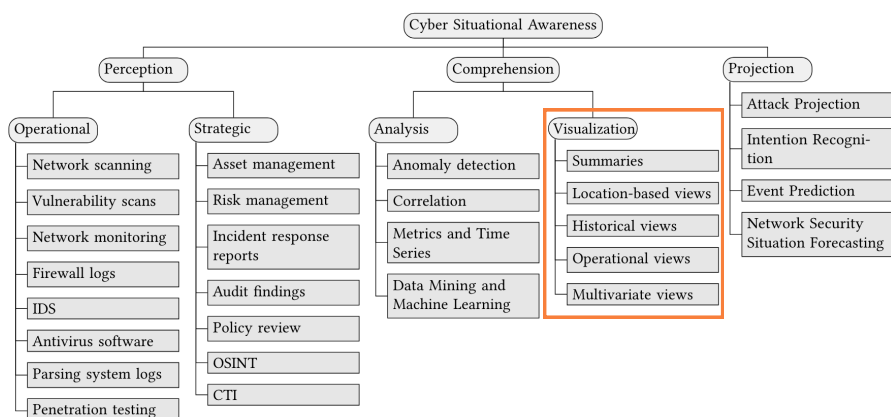


Figure 4.1 workflows in different use case?.

various ppl has different

In addition to key primary roles, stakeholders from such as chain also can be responsible for the

based the operational security stakeholder's roles publication 3 also defined those stakeholders in the supply chain. CNSSA system model and architecture [73] relationship in maritime and

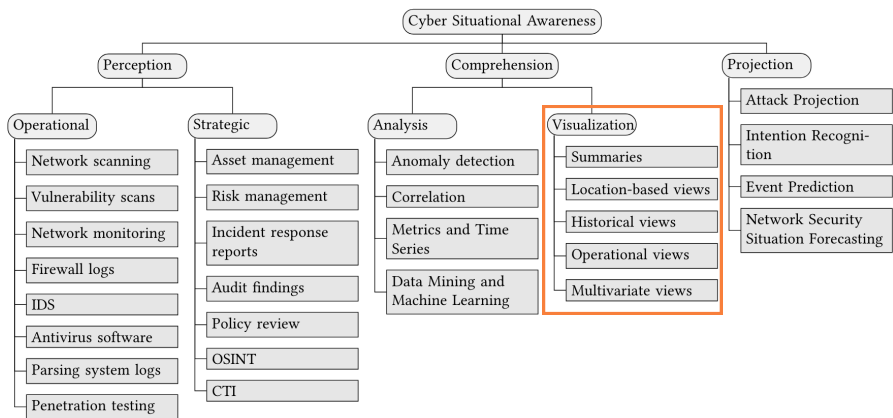


Figure 4.2 workflows in different use case?.

This chapter focuses on illustrating the design of operational security visualization. Cybersecurity visualization design in this thesis covers two industrial scenarios: Maritime industry and building automation. This section will describe three subsections, from presenting a review of cybersecurity visualization, and implementation of role-based security dashboard design in two industrial scenarios.

5.1 Visualization Interfaces Design

Security visualization systems are expected to developed based on features and characters of different roles. The expertise level of stakeholders' shows the significant different requirements of security dashboard. those who belongs to non-experts users group, thus the functionality of the security dashboard and what is for their situational awareness of cybersecurity in the environment.

holistic cybersecurity posture in environments, increasing visibility of cybersecurity postures of systems and devices installed in operational environment will improve their cyber situational awareness,

Current visualization lacks of capabilities of illustrating security posture for different stakeholders, with consideration of their distinct background and needs in terms of cybersecurity.

5.2 Maritime

For non-expert users: The ideas is to provide overall security posture of devices and systems without delivering too much overwhelming security information on them. Publication 1 designed the security dashboards for three stakeholder roles in maritime industry. Publication 3.5 for building automation.

Publication 4 describe the developed security visualization for both house man-

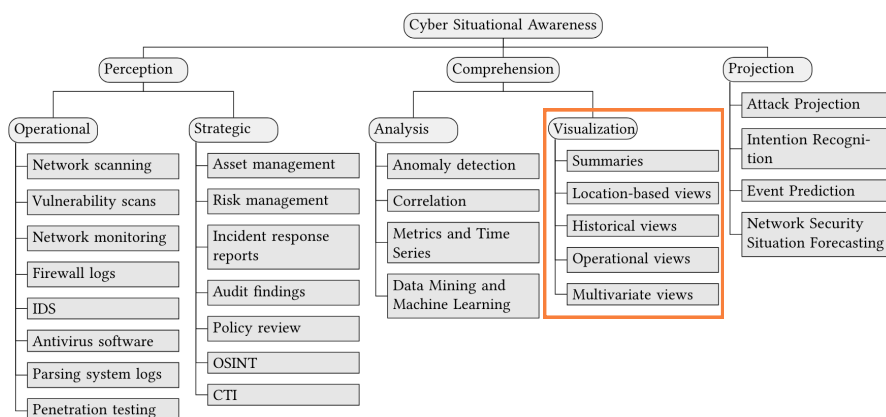


Figure 5.1 workflows in different use case?.

agers.

security monitoring, scatter based plot showing device health of the whole area
multiple user roles in,

are they background or they are contribution,

publication also defines other stakeholders' roles

for security analysts and operators, so that senses in my options and and professionals status,

also the scatter chart in this scenario we explored the also scatter chart based on the visualization to show how risky the devices is, for non-expert users.

location, map-based visualization for demonstrating the security posture in the harbour area, showing the cybersecurity health for a variety of IoT devices and systems being installed in the harbour for GPS location, or smart sensors.

Figure 1 shows the UIs for maritime and building automation.

Figure 5.1 illustrates the workflow from two industrial use.

following section for designing:

the summaries views:

holistic view from maritime scenarios, or from the building automation

risk, threats summary and tendency

cybersecurity postures, ongoing attacks or devices anomalies

maritime for non expert users, or building automation, the designing common:

cybersecurity health of different devices for the entire harbour and fairway area.

historical risks and threats for operators to be aware and see.
 located map: treemap, heatmap for devices monitoring,
 both publication 3 and 4 focus on the designing of security dashboard for building automation
 IT, summaries for different security types and ongoing security incidents incidents and examples.
 Publication 5 summarizes the design for building t
 publication 6 it shows the detailed visualization for designing, increasing for.
 publication 5 and 4 shows the designed. showed the extension version for the security issues.
 [45], [14],

5.2.1 Building automation/security analysts

Publication 2 and 3 clearly developed the security dashboards for non-experts users, for both *Terminal operators* and *House managers*,

A holistic views for operational environments are developed. both design are coordinated views for facilitating their comprehension of overall security posture in maritime and smart buildings. As figure 1 shows and view.

For delivering the overall, comprehensive dashboard for security monitoring, covering from cybersecurity health of devices to physical security of the environment, the design have employed multiple views based on the categorizations in **study [62], which emphasising the important of using visualization for increasing cyber situational awareness:

Summaries: all security information regarding devices, all rooms information number, devices information, sensors information. all sensor data and reading. total numbers of security and physical alarms.

Location-based views: As multiple devices and sensors have been installed in all smart buildings, considering to the large scale of readings and data and closeness of those smart buildings, heatmap view has been implemented for showing the distribution of each sensors, and reading with showing ID number directly instead of employing a geographical location view. by contrast, for a large maritime scenarios including both harbour and fairway, the security visualization used a map-based view combined with scatter chart, as the inspired in the work of [49], which showing security incidents as worldwide.

Historical views: previous risks and threats, for showing which devices are more vulnerable. historical security incidents, risks from each devices, physical alarms.

Operational views: showing devices anomalies, ongoing attack. security alarms, those who needs immediately action needs to be highlight for non-experts to ensure no delay and misunderstanding for delaying cyber attack mitigation.

Multivariate views: heatmap shows ID and readings for locating a specific sensors, same as in a map view, for non experts to spot which devices are.

REFERENCES

- [1] Hooman Alavizadeh, Julian Jang-Jaccard, Simon Yusuf Enoch, Harith Al-Sahaf, Ian Welch, Seyit A Camtepe, and Dan Dongseong Kim. “A survey on cyber situation-awareness systems: Framework, techniques, and insights”. In: *ACM Computing Surveys* 55.5 (2022), pp. 1–37.
- [2] Yazeed Alrowaili, Neetesh Saxena, Anurag Srivastava, Mauro Conti, and Pete Burnap. “A review: Monitoring situational awareness of smart grid cyber-physical systems and critical asset identification”. In: *IET Cyber-Physical Systems: Theory & Applications* 8.3 (2023), pp. 160–185.
- [3] Marco Angelini and Giuseppe Santucci. “Cyber situational awareness: from geographical alerts to high-level management”. In: *Journal of Visualization* 20 (2017), pp. 453–459.
- [4] Giacomo Assenza, Luca Faramondi, Gabriele Oliva, and Roberto Setola. “Cyber threats for operational technologies”. In: *International Journal of System of Systems Engineering* 10.2 (2020), pp. 128–142.
- [5] Benjamin Bach, Euan Freeman, Alfie Abdul-Rahman, Cagatay Turkay, Saiful Khan, Yulei Fan, and Min Chen. “Dashboard Design Patterns”. In: *IEEE Transactions on Visualization and Computer Graphics* 29.1 (2023), pp. 342–352. DOI: 10.1109/TVCG.2022.3209448.
- [6] Georgios Bakirtzis, Brandon J Simon, Cody H Fleming, and Carl R Elks. “Looking for a black cat in a dark room: Security visualization for cyber-physical system design and analysis”. In: *2018 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE. 2018, pp. 1–8.
- [7] Fabian Konrad Böhm. “Leveraging Visual Analytics for Cybersecurity”. PhD thesis. Universität Regensburg, 2022.

- [8] Victor Cobilean, Harindra S Mavikumbure, Brady J McBride, Bjorn Vaagen-smith, Vivek Kumar Singh, Ruixuan Li, Craig Rieger, and Milos Manic. “A Review of Visualization Methods for Cyber-Physical Security: Smart Grid Case Study”. In: *IEEE Access* (2023).
- [9] Allan Cook, Richard G Smith, Leandros Maglaras, and Helge Janicke. “SCIPS: using experiential learning to raise cyber situational awareness in industrial control system”. In: *International Journal of Cyber Warfare and Terrorism (IJCWT)* 7.2 (2017), pp. 1–15.
- [10] Angelo Corallo, Mariangela Lazoi, Marianna Lezzi, and Angela Luperto. “Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review”. In: *Computers in Industry* 137 (2022), p. 103614.
- [11] R Jordan Crouser, Erina Fukuda, and Subashini Sridhar. “Retrospective on a decade of research in visualization for cybersecurity”. In: *2017 IEEE International Symposium on Technologies for Homeland Security (HST)*. IEEE. 2017, pp. 1–5.
- [12] “cybersecurity visualisation”. In: (). [Online; accessed 08-Oct-2023]. URL: <https://www.logsign.com/blog/how-to-do-cybersecurity-data-visualization/#:~:text=Cybersecurity%20data%20visualization%20refers%20to,be%20gathered%20from%20various%20sources>.
- [13] Kaitlyn DeValk and Niklas Elmqvist. “Riverside: A design study on visualization for situation awareness in cybersecurity”. In: *Information Visualization* 23.1 (2024), pp. 40–66.
- [14] Athanasios Drougkas, Anna Sarri, Pinelopi Kyranoudi, and Antigone Zisi. “Port cybersecurity: Good practices for cybersecurity in the maritime sector”. In: *ENSISA* 10 (2019), p. 328515.
- [15] Mica R Endsley. “Toward a theory of situation awareness in dynamic systems”. In: *Human factors* 37.1 (1995), pp. 32–64.
- [16] European Union Agency for Cybersecurity (ENISA). *Good Practices for Supply Chain Cybersecurity*. Technical Report 1. Accessed: 2024-05-22. Heraklion, Greece: European Union Agency for Cybersecurity, Nov. 2020. URL: <https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity>.

- [17] Antti Evesti, Teemu Kanstrén, and Tapio Frantti. “Cybersecurity situational awareness taxonomy”. In: *2017 international conference on cyber situational awareness, data analytics and assessment (Cyber SA)*. IEEE. 2017, pp. 1–8.
- [18] Adrian Fernandez, Emilio Insfran, and Silvia Abrahão. “Usability evaluation methods for the web: A systematic mapping study”. In: *Information and software Technology* 53.8 (2011), pp. 789–817.
- [19] Stephen Few and Perceptual Edge. “Dashboard confusion revisited”. In: *Perceptual Edge* (2007), pp. 1–6.
- [20] Ulrik Franke and Joel Brynielsson. “Cyber situational awareness—a systematic review of the literature”. In: *Computers & security* 46 (2014), pp. 18–31.
- [21] Oscar Garcia-Morchon, Sandeep Kumar, and Mohit Sethi. *Internet of Things (IoT) Security: State of the Art and Challenges*. RFC 8576. Apr. 2019. DOI: 10.17487/RFC8576. URL: <https://www.rfc-editor.org/info/rfc8576>.
- [22] John R Goodall. “Introduction to visualization for computer security”. In: *VizSEC 2007: Proceedings of the Workshop on Visualization for Computer Security*. Springer. 2008, pp. 1–17.
- [23] Andrei Gurtov, Madhusanka Liyanage, and Dmitry Korzun. “Secure communication and data processing challenges in the Industrial Internet”. In: *Baltic Journal of Modern Computing* 4.4 (2016), pp. 1058–1073.
- [24] Robert Gutzwiller, Josiah Dykstra, and Bryan Payne. “Gaps and opportunities in situational awareness for cybersecurity”. In: *Digital Threats: Research and Practice* 1.3 (2020), pp. 1–6.
- [25] Adam Hahn. “Operational Technology and Information Technology in Industrial Control Systems”. In: *Cyber-security of SCADA and Other Industrial Control Systems*. Ed. by Edward J. M. Colbert and Alexander Kott. Cham: Springer International Publishing, 2016, pp. 51–68. ISBN: 978-3-319-32125-7. DOI: 10.1007/978-3-319-32125-7_4. URL: https://doi.org/10.1007/978-3-319-32125-7_4.
- [26] Tobias Heer, Oscar Garcia-Morchon, Rene Hummen, Sye Loong Keoh, Sandeep S. Kumar, and Klaus Wehrle. “Security challenges in the IP-based internet of things”. In: *Wireless Personal Communications* 61.3 (2011), pp. 527–542. DOI: 10.1007/s11277-011-0385-5.

- [27] AR Hevner, ST March, and K Park. “Design Research in Information Systems Research”. In: *MIS Quarterly* 28.1 (2010), pp. 76–105.
- [28] Rachel Huelin, Ike Iheanacho, K Payne, and K Sandman. “What’s in a name? Systematic and non-systematic literature reviews, and why the distinction matters”. In: *The evidence* (2015), pp. 34–37.
- [29] Martin Husák, Tomáš Jirsík, and Shanchieh Jay Yang. “SoK: Contemporary issues and challenges to enable cyber situational awareness for network security”. In: *Proceedings of the 15th International Conference on Availability, Reliability and Security*. 2020, pp. 1–10.
- [30] ISO13407 ISO. “13407: Human-centred design processes for interactive systems”. In: *Geneva: ISO* (1999).
- [31] Jay Jacobs and Bob Rudis. *Data-driven security: analysis, visualization and dashboards*. John Wiley & Sons, 2014.
- [32] Soo-Yeon Ji, Bong-Keun Jeong, and Dong Hyun Jeong. “Evaluating visualization approaches to detect abnormal activities in network traffic data”. In: *International Journal of Information Security* 20 (2021), pp. 331–345.
- [33] Liuyue Jiang, Asangi Jayatilaka, Mehwish Nasim, Marthie Grobler, Mansoor Zahedi, and M Ali Babar. “Systematic Literature Review on Cyber Situational Awareness Visualizations”. In: *IEEE Access* (2022).
- [34] Timo Jokela, Netta Iivari, Juha Matero, and Minna Karukka. “The standard of user-centered design and the standard definition of usability: analyzing ISO 13407 against ISO 9241-11”. In: *Proceedings of the Latin American conference on Human-computer interaction*. 2003, pp. 53–60.
- [35] Teemu Kanstrén and Antti Evesti. “A study on the state of practice in security situational awareness”. In: *2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*. IEEE. 2016, pp. 69–76.
- [36] Staffs Keele et al. *Guidelines for performing systematic literature reviews in software engineering*. 2007.
- [37] Barbara Kitchenham. “Procedures for performing systematic reviews”. In: *Keele, UK, Keele University* 33.2004 (2004), pp. 1–26.

- [38] Tero Kokkonen. “Architecture for the cyber security situational awareness system”. In: *Internet of Things, Smart Spaces, and Next Generation Networks and Systems: 16th International Conference, NEW2AN 2016, and 9th Conference, ruSMART 2016, St. Petersburg, Russia, September 26-28, 2016, Proceedings 16*. Springer. 2016, pp. 294–302.
- [39] Adrian Komadina, Željka Mihajlović, and Stjepan Groš. “Analysis of the Design Space for Cybersecurity Visualizations in VizSec”. In: *2022 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE. 2022, pp. 1–11.
- [40] Guillaume Lame. “Systematic literature reviews: An introduction”. In: *Proceedings of the design society: international conference on engineering design*. Vol. 1. 1. Cambridge University Press. 2019, pp. 1633–1642.
- [41] Katya Le Blanc, Aditya Ashok, Lyndsey Franklin, Jean Scholtz, Eric Andersen, and Michael Cassiadoro. “Characterizing cyber tools for monitoring power grid systems: What information is available and who needs it?” In: *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE. 2017, pp. 3451–3456.
- [42] James R Lewis. “Usability testing”. In: *Handbook of human factors and ergonomics* (2012), pp. 1267–1312.
- [43] Anna-Pia Lohfink, Simon D Duque Anton, Hans Dieter Schotten, Heike Leitte, and Christoph Garth. “Security in process: Visually supported triage analysis in industrial process data”. In: *IEEE transactions on visualization and computer graphics* 26.4 (2020), pp. 1638–1649.
- [44] Inês Macedo, Sinan Wanous, Nuno Oliveira, Orlando Sousa, and Isabel Praça. “A tool to support the investigation and visualization of cyber and/or physical incidents”. In: *World Conference on Information Systems and Technologies*. Springer. 2021, pp. 130–140.
- [45] Apostolos Malatras, Zoran Stanic, Ifigeneia Lella, Ricardo De Sousa Figueiredo, Eleni Tsekmezoglou, Marianthi Theocharidou, Rossen Naydenov, and Anastasios Drougkas. “ENISA Threat Landscape: Transport Sector (January 2021 to October 2022)”. In: (2023).
- [46] Alexandre Gil de Sá Martins. “Visualization of security in industrial control systems respecting IEC-62443”. PhD thesis. 2020.

- [47] Raffael Marty. *Applied security visualization*. Addison-Wesley Professional, 2008.
- [48] James McCarthy, Don Faatz, Nikolas Urlaub, John Wiltberger, Tsion Yimer, et al. *Securing Distributed Energy Resources: An Example of Industrial Internet of Things Cybersecurity*. Tech. rep. National Institute of Standards and Technology, 2022.
- [49] Sean McKenna, Diane Staheli, Cody Fulcher, and Miriah Meyer. “Bubblenet: A cyber security dashboard for visualizing patterns”. In: *Computer Graphics Forum*. Vol. 35. 3. Wiley Online Library. 2016, pp. 281–290.
- [50] Sean McKenna, Diane Staheli, and Miriah Meyer. “Unlocking user-centered design methods for building cyber security visualizations”. In: *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE. 2015, pp. 1–8.
- [51] Tomasz Miaskiewicz and Kenneth A Kozar. “Personas and user-centered design: How can personas benefit product design processes?” In: *Design studies* 32.5 (2011), pp. 417–430.
- [52] Sas Mihindu and Farzad Khosrow-shahi. “Collaborative visualisation embedded cost-efficient, virtualised cyber security operations centre”. In: *2020 24th International Conference Information Visualisation (IV)*. IEEE. 2020, pp. 153–159.
- [53] Evgenia Novikova, Mikhail Bestuzhev, and Igor Kotenko. “Anomaly detection in the HVAC system operation by a RadViz based visualization-driven approach”. In: *Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26–27, 2019 Revised Selected Papers 5*. Springer. 2020, pp. 402–418.
- [54] Chitu Okoli. “A guide to conducting a standalone systematic literature review”. In: *Communications of the Association for Information Systems* 37 (2015).
- [55] Cyril Onwubiko. “Understanding Cyber Situation Awareness.” In: *Int. J. Cyber Situational Aware*. 1.1 (2016), pp. 11–30.

- [56] Ken Peffers, Tuure Tuunanen, Marcus A Rothenberger, and Samir Chatterjee. “A design science research methodology for information systems research”. In: *Journal of management information systems* 24.3 (2007), pp. 45–77.
- [57] Oskars Podzins and Andrejs Romanovs. “Why SIEM is Irreplaceable in a Secure IT Environment?” In: *2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)*. 2019, pp. 1–5. DOI: 10.1109/eStream.2019.8732173.
- [58] Antonis Protopsaltis, Panagiotis Sarigiannidis, Dimitrios Margounakis, and Anastasios Lytos. “Data visualization in internet of things: tools, methodologies, and challenges”. In: *Proceedings of the 15th international conference on availability, reliability and security*. 2020, pp. 1–11.
- [59] Tashfiq Rahman, Rohani Rohan, Debajyoti Pal, and Prasert Kanthamanon. “Human Factors in Cybersecurity: A Scoping Review”. In: *Proceedings of the 12th International Conference on Advances in Information Technology*. IAIT ’21. Bangkok, Thailand: Association for Computing Machinery, 2021. ISBN: 9781450390125. DOI: 10.1145/3468784.3468789. URL: <https://doi.org/10.1145/3468784.3468789>.
- [60] Prashanth Rajivan and Nancy Cooke. “Impact of team collaboration on cybersecurity situational awareness”. In: *Theory and Models for Cyber Situation Awareness* (2017), pp. 203–226.
- [61] Ronald S. Ross, Victoria Yan Pillitteri, and Kelley L. Dempsey. *Assessing Enhanced Security Requirements for Controlled Unclassified Information*. NIST Special Publication 800-172A. National Institute of Standards and Technology, Mar. 2022. DOI: 10.6028/NIST.SP.800-172A. URL: <https://doi.org/10.6028/NIST.SP.800-172A>.
- [62] Alper Sarikaya, Michael Correll, Lyn Bartram, Melanie Tory, and Danyel Fisher. “What do we talk about when we talk about dashboards?” In: *IEEE transactions on visualization and computer graphics* 25.1 (2018), pp. 682–692.
- [63] Jean C Scholtz, Lyndsey Franklin, Aditya Ashok, Katya LeBlanc, Christopher Bonebrake, Eric Andersen, and Michael Cassiadoro. “Employing a user-centered design process for cybersecurity awareness in the power grid”. In: *Journal of Human Performance in Extreme Environments* 14.1 (2018), p. 4.

- [64] Younho Seong, Joseph Nuamah, and Sun Yi. “Guidelines for cybersecurity visualization design”. In: *Proceedings of the 24th Symposium on International Database Engineering & Applications*. 2020, pp. 1–6.
- [65] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A Ghorbani. “An evaluation framework for network security visualizations”. In: *Computers & Security* 84 (2019), pp. 70–92.
- [66] Hadi Shiravi, Ali Shiravi, and Ali A Ghorbani. “A survey of visualization systems for network security”. In: *IEEE Transactions on visualization and computer graphics* 18.8 (2011), pp. 1313–1329.
- [67] Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, and Mikael Gidlund. “Industrial Internet of Things: Challenges, Opportunities, and Directions”. In: *IEEE Transactions on Industrial Informatics* 14.11 (2018), pp. 4724–4734. DOI: 10.1109/TII.2018.2852491.
- [68] Muammer Semih Sonkor and Borja García de Soto. “Operational technology on construction sites: A review from the cybersecurity perspective”. In: *Journal of Construction Engineering and Management* 147.12 (2021), p. 04021172.
- [69] Diane Staheli, Tamara Yu, R Jordan Crouser, Suresh Damodaran, Kevin Nam, David O’Gwynn, Sean McKenna, and Lane Harrison. “Visualization evaluation for cyber security: Trends and future directions”. In: *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*. 2014, pp. 49–56.
- [70] Koen Tange, Michele De Donno, Xenofon Fafoutis, and Nicola Dragoni. “A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities”. In: *IEEE Communications Surveys Tutorials* 22.4 (2020), pp. 2489–2520. DOI: 10.1109/COMST.2020.3011208.
- [71] Dave Thaler, Hannes Tschofenig, and Mary Barnes. “Architectural considerations in smart object networking”. In: *Tech. no. RFC 7452* (2015).
- [72] Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul. “Security Operations Center: A Systematic Study and Open Challenges”. In: *IEEE Access* 8 (2020), pp. 227756–227779. DOI: 10.1109/ACCESS.2020.3045514.

- [73] Rongrong Xi, Shuyuan Jin, Xiaochun Yun, and Yongzheng Zhang. “CNSSA: A Comprehensive Network Security Situation Awareness System”. In: *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications*. 2011, pp. 482–487. DOI: 10.1109/TrustCom.2011.62.
- [74] Pavel Yermalovich. “Dashboard visualization techniques in information security”. In: *2020 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE. 2020, pp. 1–6.
- [75] Narges Yousefnezhad, Avleen Malhi, and Kary Främling. “Security in product lifecycle of IoT devices: A survey”. In: *Journal of Network and Computer Applications* 171 (2020), p. 102779. ISSN: 1084-8045. DOI: <https://doi.org/10.1016/j.jnca.2020.102779>. URL: <https://www.sciencedirect.com/science/article/pii/S1084804520302538>.
- [76] Tianye Zhang, Xumeng Wang, Zongzhuang Li, Fangzhou Guo, Yuxin Ma, and Wei Chen. “A survey of network anomaly visualization”. In: *Science China Information Sciences* 60 (2017), pp. 1–17.
- [77] Haisheng Zhao, Wenzhong Tang, Xiaoxiang Zou, Yanyang Wang, and Yueran Zu. “Analysis of visualization systems for cyber security”. In: *Recent Developments in Intelligent Computing, Communication and Devices: Proceedings of ICCD 2017* (2019), pp. 1051–1061.

bibliographythesis_bibliography

APPENDIX A APPENDIX

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

PUBLICATIONS

