UiA University of Agder

Cybersecurity Master's Thesis

A Cyber Situational Awareness Framework for Security Operations Center Incident Response in High Availability and Safety-Critical Systems

SINDRE-NICOLAI BARVIK FREDRIKSEN & KJARTAN ERLAND

SUPERVISORS
Nadia Saad Noori & Lucia Castro Herrera

University of Agder, 2024
Faculty of Social Sciences
Department of Information Systems

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	**Ja**
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	**Ja**
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	**Ja**
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	**Ja**
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	**Ja**
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	**Ja**
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	**Nei**

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	**Ja**
Er oppgaven båndlagt (konfidensiell)?	**Nei**
Er oppgaven unntatt offentlighet?	**Nei**

Acknowledgements

First off, we want to sincerely thank our supervisors, Nadia Saad Noori and Lucia Castro Herrera, for their got-getter attitudes, continuous guidance, and support and for keeping us marginally sane while working on our thesis. Nadia, thank you for your overly ambitious and positive attitude, which caused us to reach beyond what we initially thought we would do. Lucia, thank you for taking the time when we are about to lose our minds to provide some much-needed guidance and feedback.

We also want to sincerely thank our colleague Robert Rhind for his great input and expertise on the subject matter, for giving feedback, challenging us to achieve excellent results, and for keeping "the lads" motivated throughout the thesis process.

We also wish to extend our thanks to Jeroen Wijnands for showing interest, answering our post on Reddit, taking time out of your day to chat, and giving two Norwegian students your opinions and guidance.

Finally, thank you to all the people who took time out of their day to participate in our study. Your time and input have been invaluable. You provided great insight and the information necessary for us to do our research and write this paper. If we ever meet, come say hi, we definitely owe you a beer.

Abstract

Owners of Operational Technology (OT) in different sectors from industry, critical infrastructure and other services are increasingly utilizing connected technologies in production processes, systems, and environments that make up their operations, exposing traditionally isolated networks to the Internet (Ashibani & Mahmoud, 2017). With cyber-attacks becoming a regular occurrence, industrial organizations face an ever-increasing challenge in protecting their assets as the cyber threat landscape widens due to Information Technology (IT) being introduced into the OT domain (Dragos, 2024). This means that cyber operations are not necessarily limited to the digital domain and may, in worst-case scenarios, lead to severe physical damage to critical infrastructure and personnel (The Norwegian National Security Authority, 2024). Critical infrastructure and OT are experiencing increased threats from the digital domain, and the current geopolitical situation has caused a spike in cyber-attacks that directly or indirectly impact critical OT environments (The Norwegian National Security Authority, 2024). To increase their cyber-resilience and respond to digital malicious actors targeting their environments, OT organizations may employ Managed Security Service Providers (MSSP) to protect their complex and highly contextualized OT environments from threats that originate in the cyber-realm. However, due to the inherent differences between IT and OT, MSSPs and Security Operations Centers (SOC) experience difficulties when integrating OT into the scope of their enterprise SOC operations (Dragos, 2023). Therefore, when securing systems that consist of OT, MSSPs are dependent on additional sources of knowledge and context to develop the Cyber Situational Awareness (CSA) necessary to effectively monitor and respond to cyber-events that span the IT and OT domains.

With this exploratory study, we aim to determine how OT impacts the development of CSA during Incident Response (IR) in a SOC. Additionally, we investigate how MSSPs can operationalize people, processes, and technologies to effectively provide security operations to organizations that operate and maintain OT environments. We investigate how people, processes, and technology operate in a complex socio-technological environment to determine how the MSSPs and the SOC develop and maintain CSA during cross-domain IR.

This study expands upon the work of Andreassen et al. (2023) by constructing a conceptual framework that illustrates the process of developing CSA in OT-SOC IR. We apply Collective Intelligence (CI) theory and Endsley's (1995) theory of Situation Awareness (SA) to create a theoretical lens and explain how CSA and shared SA are developed in cross-domain and multi-actor environments. Data was gathered through a systematic assessment of 27 peer-reviewed publications and 11 interviews with 14 respondents, varying from engineers to OT security specialists. Using the framework for SA in SOC-IR by Andreassen et al. (2023), theory, and the interview data, we have created a dynamic framework illustrating the process of developing CSA in OT-SOC IR. The framework illustrates how different actors (people, processes, and technologies) cooperate and coordinate across domains towards building CSA during incident response. Further, the framework captures the information flow and decision-making process at different levels to enable SOC operators to correlate cyber incidents with events that impact availability and operational safety in OT environments. Lastly, we explain

how the environment changes when OT is incorporated into the scope of the SOC and highlight how elements of cognition, cooperation, and coordination act as the foundation in combined IT and OT cyber-IR.

Contents

List of Figures

List of Tables

List of Abbreviations	
Abbreviation	Meaning
CERT	Computer Emergency Response Team
CI	Collective Intelligence
CIA	Confidentiality, Integrity & Availability
CIM	Computer-Integrated Manufacturing
CISO	Chief Information Security Officer
CPS	Cyber-Physical System
CR	Control Room
CSA	Cyber Situational Awareness
CSO	Chief Safety Officer
CSIRT	Computer Security Incident Response Team
CTO	Chief Technical Officer
EWS	Engineering Workstation
GDPR	General Data Protection Regulation
HMI	Human Machine Interface
HSE	Health, Safety, and Environment
IACS	Industrial Automation and Control System
ICS	Industrial Control System
ICT	Information and Communication Technology
IM	Incident Management
IR	Incident Response
IRT	Incident Response Team
IT	Information Technology
MSSP	Managed Security Service Provider
OEM	Original Equipment Manufacturer
OT	Operational Technology
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SA	Situational Awareness
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SIS	Safety Instrumented System
SLR	Systematic Literature Review
SOC	Security Operations Center
SOP	Standard Operating Procedure
SPAN	Switch Port Analyzer

Chapter 1

Introduction

In their annual review for 2023, Dragos (2024) reports that advanced cyber threat activity towards critical infrastructure has been increasing due to the escalation of worldwide conflicts between nations in different regions. Dragos (2024) also states that ransomware attacks have shown a 50% increase in reported incidents from industrial organizations . Gartner presented an article back in 2012 that predicts how "*Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans*", suggesting that organizations have to adopt and implement a security control framework (Moore, 2021). Sophisticated malware targeting critical infrastructure, not only to steal information but to interrupt, sabotage, and destroy, poses an entirely different threat landscape. The nature of the Operational Technology (OT) domain operating in the physical world enables malicious actors to threaten the physical safety of humans and the environment. As such, securing and safeguarding OT systems is of utmost importance.

In 2015, on the 23rd of December, Ukrainian power companies experienced power outages that affected many customers (CISA, 2021). Malware had previously been reported in various infrastructure sectors across Ukraine. These reports indicated that this malware, attributed to BlackEnergy, had been found on companies' IT computer networks. The investigated incident led the IR team to discover that the attack had been caused by a complex, remote attack against three electrical plants in the region, leaving around 225.000 people without power during the holiday season. According to the report, spear-phishing was used to distribute the malware, and as it spread, the threat actors were able to seize control of the OT environment, leading to a loss of power.

With the ever-increasing cyber threats towards the OT environment and the consequences it may have, and as Gartner (2021) stated, a prediction of physical harm by the year 2025, proper security controls in this domain are much needed. To effectively comprehend the OT domain, its environment, and its technological distinctions from IT, SOCs must address these challenges. As such, due to the differences that separate IT and OT, the SOC requires measures and processes that provide the knowledge and understanding necessary to develop CSA of cyber-incidents that occur in the OT domain (Kayan et al., 2022; Pöyhönen et al., 2021). The SOCs role is to act as a security control for OT organizations' environments, as well as security monitoring, prevention, and IR. With its security tools, the SOC must gather information, and the analysts must perceive and understand it to make adequate decisions.

Baskerville et al. (2014) highlight in their study an organizational focus on prevention and response in regard to a cyber-attack. Though each of these paradigms does not ignore the other in a cyber incident, traditionally, what OT has focused on is prevention. Baskerville et al. (2014) highlight this point by addressing the context switch of an OT environment going from performance to control. OT focuses more on availability and up-time than the traditional confidentiality, integrity, and availability (CIA) prioritization in the IT domain

(Tuptuk & Hailes, 2018).

This highlights an aspect of how an industrial SOC's CSA plays a role in IR and how the security monitoring of the OT environment aims to prevent cyber-attacks. With a traditionally IT-oriented SOC introducing OT into their workflow, therefore, we pose the following research questions, addressing the notion of CSA in OT-SOC incident response:

1. How does Operational Technology change Cyber Situational Awareness in SOC incident response?
2. How are people, processes, and technologies in MSSPs operationalized to provide Operational Technology Security-Operations-as-a-Service?

This study aims to investigate and create an understanding of how the integration of OT systems and environments into the scope of the SOC changes how analysts develop and maintain CSA during incident response. How does a Managed Security Service Provider (MSSP) adapt from a traditional IT domain to handle OT incidents as well? To answer these questions and gain knowledge and understanding of these concepts, we have developed a dynamic framework for CSA in OT-SOC incident response to visualize how a security team in a SOC handles OT incidents that span both the IT and OT domains.

1.1 Rationale and Motivation

The rationale and motivation for this study are inspired by the framework A Dynamic Framework Enhancing Situational Awareness in Cybersecurity SOC—IR by Andreassen et al. (2023) (Figure 1.1). In the semester leading up to writing the Master's thesis, we conducted background work on the effect of implementing OT into a Security Operations Center (SOC) and its impact on incident response across the decision-making levels. We discovered a gap in the body of knowledge on the concept of OT-SOC. Per our research, we could not find any relevant literature specifically covering CSA in OT-SOC. The closest we found was shared ICS SOC (Dimitrov & Syarova, 2019) and collaboration between cybersecurity professionals and industrial stakeholders (Fink & Shulga, 2018; Kanamaru, 2020). Additionally, a motivational aspect of pursuing this topic is that both authors are SOC analysts, as the added interest in Operational Technology's effect on a SOC and how we, as analysts in the IT domain, would handle OT incidents.

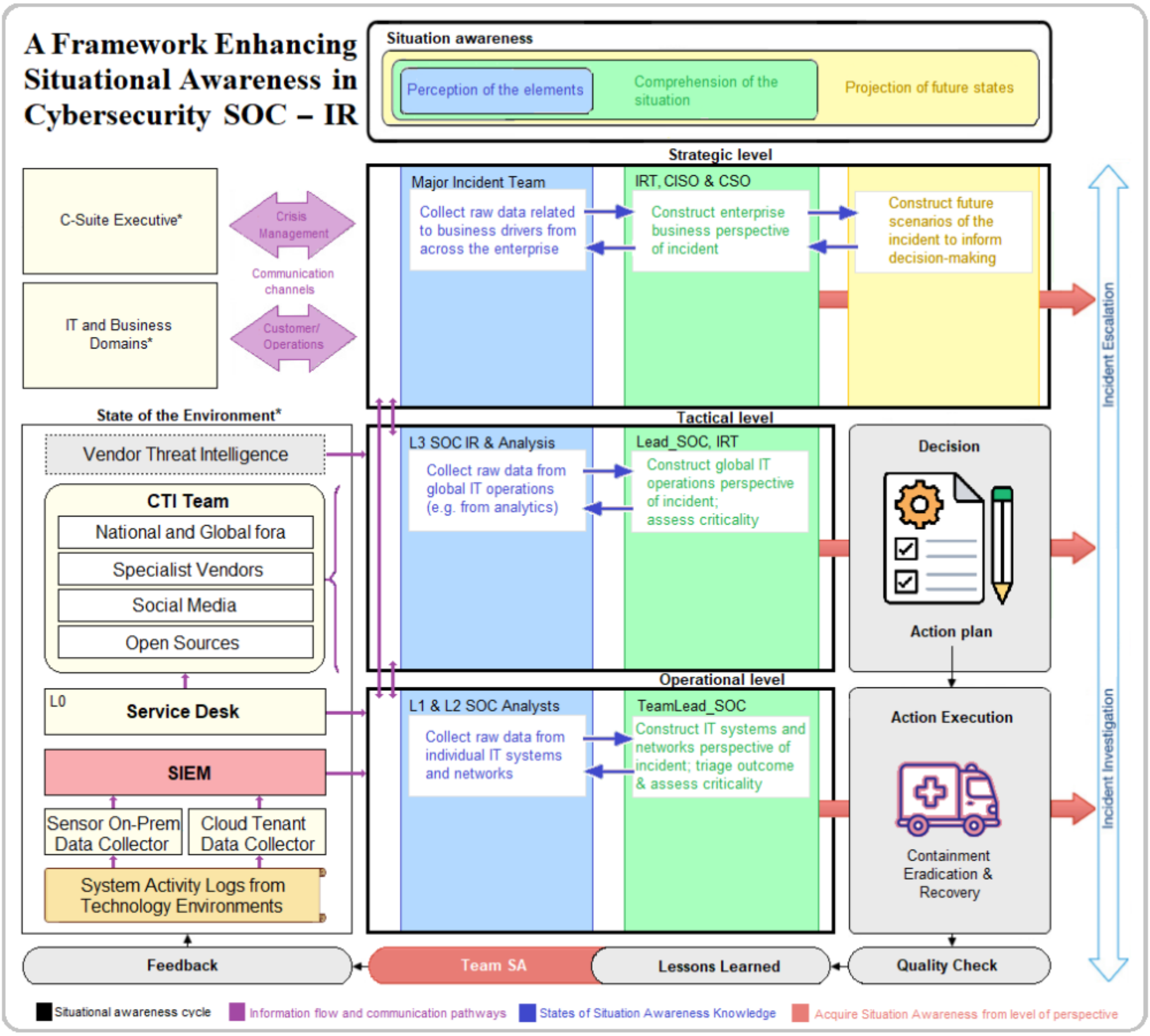

A Framework Enhancing Situational Awareness in Cybersecurity SOC – IR
Situation awareness
Perception of the elements
Comprehension of the situation
Projection of future states
Strategic level
C-Suite Executive*
Crisis Management
Communication channels
Customer/ Operations
IT and Business Domains*
Major Incident Team
Collect raw data related to business drivers from across the enterprise
IRT, CISO & CSO
Construct enterprise business perspective of incident
Construct future scenarios of the incident to inform decision-making
Incident Escalation
State of the Environment*
Tactical level
Vendor Threat Intelligence
CTI Team
National and Global fora
Specialist Vendors
Social Media
Open Sources
L3 SOC IR & Analysis
Collect raw data from global IT operations (e.g. from analytics)
Lead_SOC, IRT
Construct global IT operations perspective of incident; assess criticality
Decision
Action plan
Operational level
L0
Service Desk
SIEM
Sensor On-Prem Data Collector
Cloud Tenant Data Collector
System Activity Logs from Technology Environments
L1 & L2 SOC Analysts
Collect raw data from individual IT systems and networks
TeamLead_SOC
Construct IT systems and networks perspective of incident; triage outcome & assess criticality
Action Execution
Containment Eradication & Recovery
Incident Investigation
Feedback
Team SA
Lessons Learned
Quality Check
Situational awareness cycle
Information flow and communication pathways
States of Situation Awareness Knowledge
Acquire Situation Awareness from level of perspective

Figure 1.1: A Dynamic Framework Highlighting Situation Awareness in Cyber IR (Andreassen et al., 2023, p. 240)

1.2 Research Approach

In order to ascertain the concepts of how OT can change Cyber Situational Awareness (CSA) in a SOC for incident response, this study relies on a qualitative approach. During this research's data-gathering phase, we used semi-structured interviews and published and peer-reviewed articles from scientific journals. The study initially started with a preliminary Systematic Literature Review (SLR) in the Fall of 2023, where we compiled a small list of articles addressing topics surrounding OT and SOC. Our goal was to expand our knowledge of how a SOC would adapt to the integration of OT into its scope and manage incidents in OT environments. This led to the initial research in January 2024, when the expanded SLR was established. The qualitative research method led us to conduct semi-structured interviews, which aimed to extract as much information as possible with the questions while having room for great discussions on the topics. Our structured approach was to categorize the questions into four main parts: (1) Situational Awareness, (2) Operational Technology, and (3) Security Operations Center and incident response. In the last part (4), we presented a preliminary framework based on the SLR. Before engaging the study's main topic and themes, the initial (1) set of questions was to establish the interviewee's role and experience in their field as well as their knowledge of SA and its concepts. The second (2) and third (3) parts were about knowledge, experience, and opinions on the subject matters of OT, SOC, and incident response: the systems, processes, and how security monitoring of OT would function. In the last section (4) of the interviews, we presented an initial framework based on the data and information from the SLR and asked the interview subjects for thoughts and feedback. We conducted a total of 11 interviews in the span of 3 weeks during April of 2024, where the allocated time for each interview was 60 minutes, but some reached 90 minutes. The interview subjects of this study consisted of a range of cybersecurity professionals, OT and IT SOC analysts, and an OT engineer.

1.3 Thesis Overview

The thesis is summarized in the bullet points below, highlighting each chapter's structural elements and content.

- Introduction - overview of the problem statement and research questions of the thesis.
- Background and Related Work - Introduces and discusses the literature review as well as the theoretical lens through which the thesis is formed.
- Research Approach - Presents and argues for the methodology of research this thesis is based on. Additionally, data collection, interview methodology and its limitations, data analysis, and ethical considerations are presented.
- Results - Presents our findings from the qualitative method of semi-structured interviews.
- Discussion and Summary of Findings - The framework is presented and we discuss our findings in relation to the empirical data and theory.
- Conclusion - Our conclusion is presented, and a brief mention of limitations in the study and our contribution to the theory and industry.

Chapter 2

Background and Related Work

In the following chapter, we address the methodology, process, and results of the SLR that form the foundation of the thesis. Initially, we provide a brief explanation of what an SLR is and why it is important. Subsequently, we provide an overview of the selected methodology and inclusion criteria, the search and screening process, and the resulting articles included in the review. This will serve as the basis for the theoretical lens, which will be used to frame and guide the analysis of qualitative data.

2.1 Literature Review

An SLR is the process of conducting a methodological run-through of related literature and screening for relevancy of the themes and topics (Xiao & Watson, 2017). SLR enables the researchers to identify gaps in the body of knowledge and summarize the themes and topics on which the study is based by compiling a list of related work (Xiao & Watson, 2017). As Kitchenham & Charters (2007) presented in their Guidelines for performing SLR in Software Engineering, which Xiao & Watson (2017) build upon. Our rationale and motivation for conducting an SLR is "*to provide a framework/background in order to appropriately position new research activities.*" and research OT and Cyber Situational Awareness (Kitchenham & Charters, 2007, p. 3).

Different review styles or methodologies are used in qualitative research and SLR methods, such as Meta-Analysis and Meta-Interpretation (Xiao & Watson, 2017). We have decided to use thematic synthesis for our SLR, as this method was shown to be the most relevant and best fit for our research, considering the vast number of themes and topics we had to work with. Clustering data and using data extraction to identify themes and subjects from said data is known as thematic synthesis (Thomas & Harden, 2008). By using this review type for our SLR, we enable the review protocol and literature search in accordance with our research questions to gather and synthesize relevant data.

2.1.1 Method

The methodology provided by Xiao & Watson (2017) allows for a rigorous SLR, albeit time-consuming, literature review. Figure 2.1 illustrates the eight steps involved in this process. Initially, our procedure involved developing research questions and designing a review protocol to begin the literature search. Kitchenham & Charters (2007, p. 12) states that *"a pre-defined protocol is necessary to reduce the possibility of researcher bias"*. As such, having a thorough review protocol is important to best avoid any form of presuppositions or bias when conducting the SLR.

The literature search process started with the methodology the review protocol was designed for, a review of the titles and abstract, and then a full-text review in order to gain an overview of the literature. Parallel with narrowing down the body of work, we screened for inclusion as set by the review protocol and research questions. A large set of articles were generated due to the initial set of title and abstract reviews, and to assess the quality of the articles, we made the full-text review and started the process of extracting the data. Lastly, we analyzed and synthesized the data using spreadsheets to structure and organize the data properly according to the themes and topics discovered during the SLR.

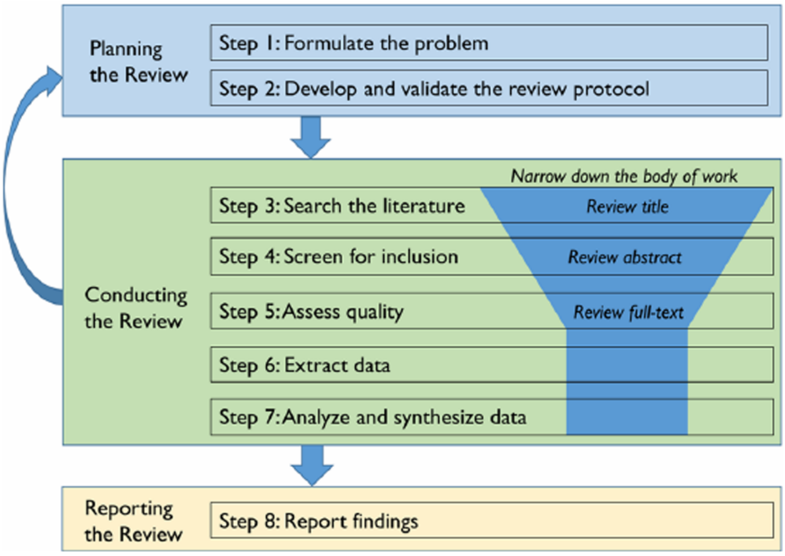

Planning the Review
Step 1: Formulate the problem
Step 2: Develop and validate the review protocol
Narrow down the body of work
Step 3: Search the literature
Review title
Step 4: Screen for inclusion
Review abstract
Conducting the Review
Step 5: Assess quality
Review full-text
Step 6: Extract data
Step 7: Analyze and synthesize data
Reporting the Review
Step 8: Report findings

Figure 2.1: Process of Systematic Literature Review (Xiao & Watson, 2017, p. 103)

Literature Inclusion Criteria

The literature criteria that we have set and outlined for our review protocol to strengthen and validate the literature search are as follows:

- The literature must be written in English or Norwegian.
- The article must be Peer-Reviewed.
- The article must contain a combination of keywords relating to the research problem.
- The article should not be older than 10 years. However, should the contents of the literature still be considered relevant to the current start of the topic area, it could be included regardless of publication date.

Search Process

The search procedure of an SLR aims to gather information and articles systematically, accumulating a set of relevant literature (Webster & Watson, 2002). There are three search methods, and due to the process this search goes through, electronic databases are the primary source of literature and information; backward and forward searching comes in second and third. Web of Science, IEEE Xplore, Scopus, and Google Scholar were the electronic databases we used. To find the literature systematically, we used a set of in-depth keywords on each database to specify our searches and to cover most of the ground to ensure we did not miss anything. The approach was to use operators in combination with keywords, synonyms, topics, and related concepts (i.e. "Operational Technology" OR OT OR ICS AND "Security Operations Center" OR SOC OR CSIRT). Table 2.1 presents an overview of the keywords and related concepts and abbreviations used during the search process.

Keyword	**Related Concepts (Abbreviation)**
Cybersecurity	- *Cyber Defence* - *IT Security* - *Information Security*
Situational Awareness	- *Situational Awareness (SA)* - *Cyber Situational Awareness (CSA)* - *Situation Awareness*
Operational Technology	- *Operational Technology (OT)* - *Industrial Control Systems (ICS)* - *Industrial Automation and Control Systems (IACS)* - *Cyber Physical System (CPS)* - *Critical Infrastructure (CI)* - *Safety Critical Systems* - *Safety Instrumented System (SIS)*
Framework	- *Standard Operating Procedure (SOP)* - *Workflow* - *Information Flow*
Security Operation Center	- *(SOC)* - *Computer Security Incident Response Team (CSIRT)* - *Computer Emergency Response Team (CERT)* - *Industrial SOC*
Safety	- *Safety*
Incident Management	- *Incident Response (IR)* - *Cyber Incident Management*
Enterprise/Organization	- *Managed Security Service Provider (MSSP)*

Table 2.1: Keywords and Related Concepts used in the Search Process

Screening

We employed the exclusion/inclusion criteria based on the review protocol and the research questions we initially formed to conduct the screening process (Kitchenham & Charters, 2007). The way this process works and its intended use is to screen each article and decide whether it will be added to the pool of references (Xiao & Watson, 2017). To highlight this process, we have used the PRISMA statement - a guideline/roadmap of what has been done in the systematic review of collected literature in line with the review protocol (Sarkis-Onofre et al., 2021). Figure 2.2 visualizes our preliminary literature review and screening process after the initial collection of articles.

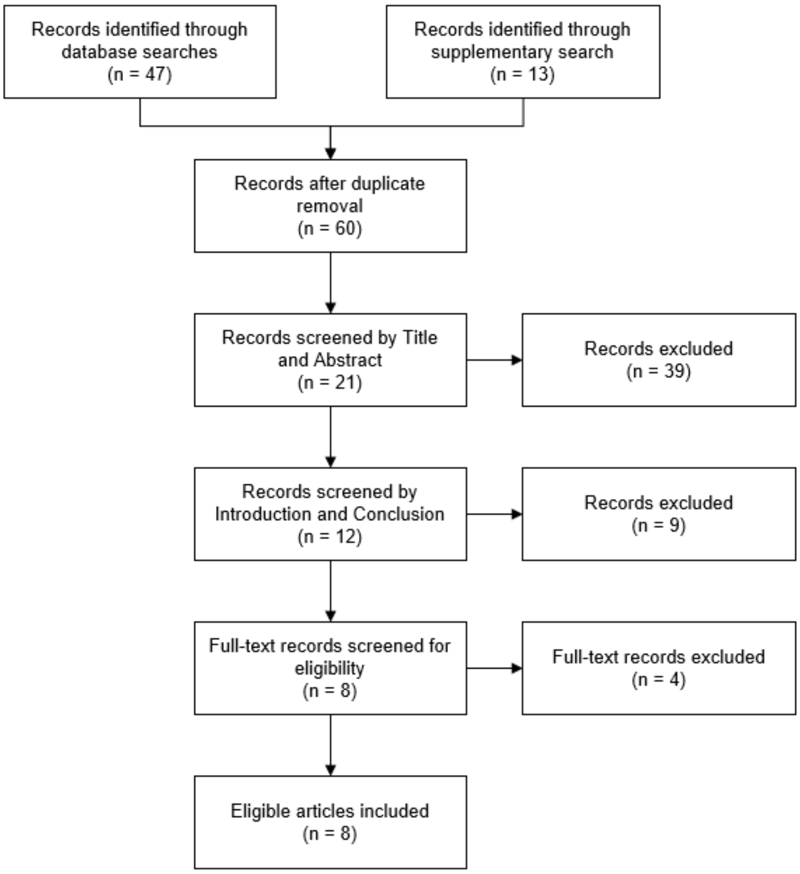

Records identified through database searches (n = 47)
Records identified through supplementary search (n = 13)
Records after duplicate removal (n = 60)
Records screened by Title and Abstract (n = 21)
Records excluded (n = 39)
Records screened by Introduction and Conclusion (n = 12)
Records excluded (n = 9)
Full-text records screened for eligibility (n = 8)
Full-text records excluded (n = 4)
Eligible articles included (n = 8)

Figure 2.2: PRISMA Model: Preliminary Search Screening Process

From the initial search across the various scientific databases using the keywords from Table 2.1, we sourced and included 72 peer-reviewed academic publications. Additionally, from a previous literature review relevant to the scope of the study (Figure 2.2), we identified another two relevant peer-reviewed publications. With a preliminary total of 74 publications, we adapted the process of Xiao & Watson (2017) (Figure 2.1), adding an extra screening step to ensure a more thorough screening process. Consequently, after screening the included articles by title and abstract, introduction and conclusion, and full-text eligibility, we were left with 21 articles. Furthermore, during the final full-text screening step of the SLR process, we discovered additional interesting topics and avenues of research that were highly relevant to our study. Therefore, adhering to the review protocol, we conducted supplementary backward, forward, and database searches to cover gaps in the SLR on topics we had previously missed due to high relevance bias. The supplementary searches yielded another 11 articles, which were screened following the same process as the initial 74 publications. This resulted in the inclusion of an additional six articles, bringing the final total of the SLR to 27 peer-reviewed academic publications. Figure 2.3 depicts the entirety of the screening process, and the final list of included literature is listed in Table 2.2.

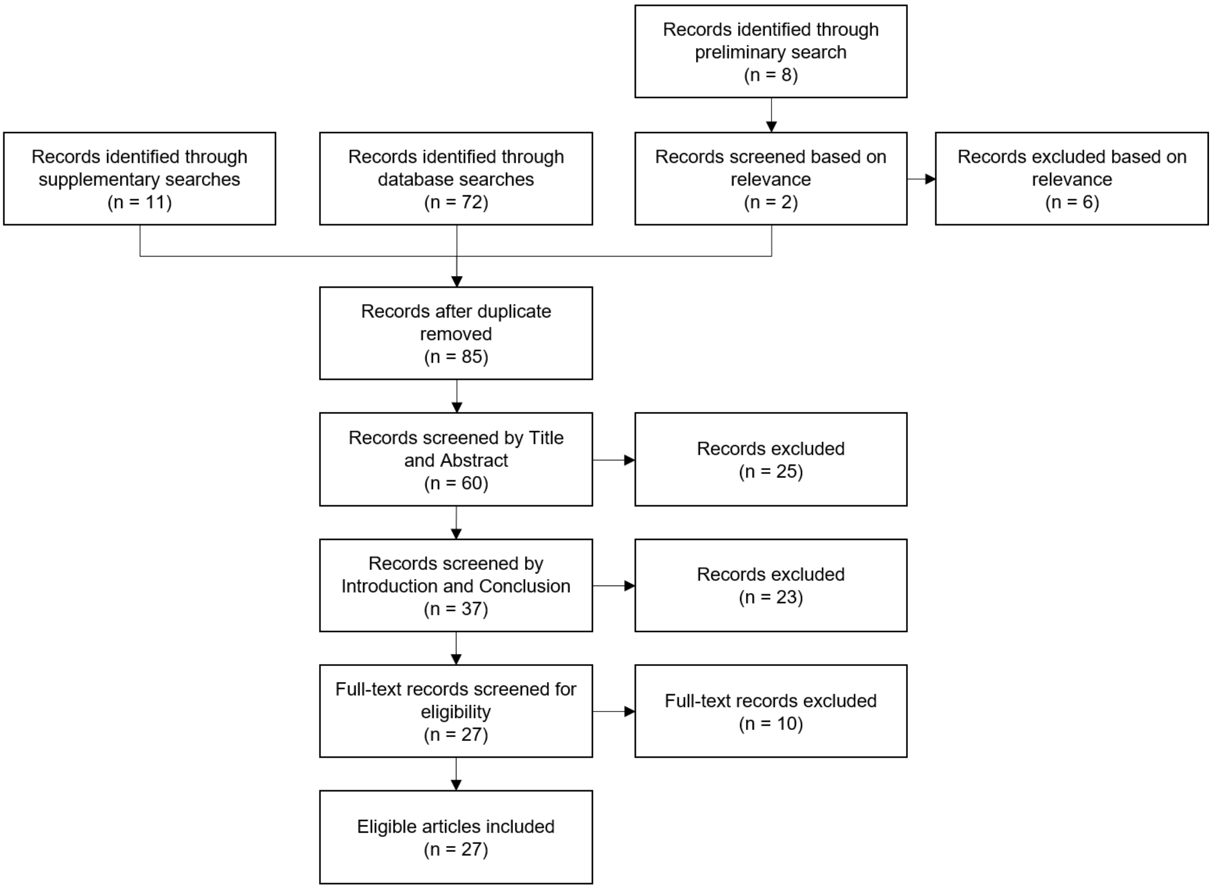

Records identified through preliminary search (n = 8)
Records identified through supplementary searches (n = 11)
Records identified through database searches (n = 72)
Records screened based on relevance (n = 2)
Records excluded based on relevance (n = 6)
Records after duplicate removed (n = 85)
Records screened by Title and Abstract (n = 60)
Records excluded (n = 25)
Records screened by Introduction and Conclusion (n = 37)
Records excluded (n = 23)
Full-text records screened for eligibility (n = 27)
Full-text records excluded (n = 10)
Eligible articles included (n = 27)

Figure 2.3: Prisma Model: Screening Process

Author (Year)	Journal	Title	Major Theme(s)
Vielberth et al. (2020)	IEEE Access	Security Operations Center: A Systematic Study and Open Challenges	SOC, Security Management, Security Operations
Ahmad et al. (2021)	Computers & Security	How can organizations develop situation awareness for incident response: A case study of management practice.	Situational Awareness, SOC
Endsley (1995)	Human Factors	Toward a theory of situation awareness in dynamic systems	Situation Awareness
Evesti et al. (2017)	IEEE	Cybersecurity situational awareness taxonomy	Taxonomized Cyber Situation Awareness
Kanamaru (2020)	Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)	Safety and Security in ICS, and SOC Incident Response	Safety & Security System, IT/OT, IACS
Franke & Brynielsson (2014)	Computers & Security	Cyber-Situational Awareness and digital/human sensor	Computer security, Taxonomy, Decision making, Monitoring
Piggin & Boyes (2015)	IET	Safety and security — A story of interdependence	Safety & Security in IACS Information Security, CPS
Fink & Shulga (2018)	IEEE International Conference on Industrial Internet (ICII)	Helping IT and OT Defenders Collaborate	Conceptual and practical challenges for IT and OT personnel's cooperation
Smith et al. (2021)	Computers & Security	The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework	Information flow and incident response for agile IRT

Author (Year)	Journal	Title	Major Theme(s)
Tuptuk & Hailes (2018)	Journal of Manufacturing Systems	Security of smart manufacturing systems	Cyberattacks on ICS
Ashibani & Mahmoud (2017)	Computers & Security	Cyber physical systems security: Analysis,challenges and solutions	Challenges and solutions to CPS security
Furrer (2022)	Springer	Safety and Security of Cyber-Pyhiscal Systems - Chapt. 4 Safety, Security and Risk	Safety, security(and risk) of CPS
Tadda & Salerno (2010)	Springer	Cyber Situational Awareness - Issues and Research - Chapt. 2 Overview of Cyber-Situation Awareness	Overview of Cyber Situational Awareness
Pöyhönen et al. (2021)	Digital Transformation, Cyber Security and Resilience of Modern Societies - Springer Cham	Cyber Situational Awareness in Critical Infrastructure Organizations	Cyber Situational Awareness in Critical Infrastructure
Matthews et al. (2016)	The Cyber Defense Review	Cyber Situational Awareness	General overview of Cyber Situational Awareness
Nyre-Yu et al. (2019)	Proceedings of the Human Factors and Ergonomics Society Annual Meeting	Observing Cyber Security Incident Response: Qualitative Themes From Field Research	Incident response, CSIRTs, sharing, Organization
Lu et al. (2014)	International Conference on Security Technology	An Analysis of Cyber Physical System Security Theories	CPS, Security
Akbarzadeh & Katsikas (2022)	IEEE Open Journal of the Industrial Electronics Society	Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems	CPS, OT, IT
Humayed et al. (2017)	IEEE Internet of Things Journal	Cyber-Physical Systems Security — A Survey	CPS security
Vincente et al. (2001)	International Journal of Human-Computer Studies	How do operators monitor a complex, dynamic work domain? The impact of control room technology	OT Operators, Controll Room
Dimitrov & Syarova (2019)	2019 Big Data, Knowledge and Control Systems Engineering	Analysis of the Functionalities of a Shared ICS Security Operations Center	ICS, SOC
Armellin et al. (2023)	2023 International Conference on Electrical, Communication and Computer Engineering	Integrating OT data in SIEM platforms: an Energy Utility Perspective	OT, SIEM, CPS
Shafi (2012)	2012 12th International Conference on Computational Science and Its Applications	Cyber Physical Systems Security: A Brief Survey	CPS, Security
Kayan et al. (2022)	ACM Computing Surveys	Cybersecurity of Industrial Cyber-Physical Systems: A Review	CPS, Cybersecurity
Onshus et al. (2022)	Journal of Cybersecurity and Privacy	Security and Independence of Process Safety and Control Systems in the Petroleum Industry	OT, Cybersecurity, Safety
Williams (1994)	Computers in Industry	The Purdue enterprise reference architecture	OT, Purdue
Habib & Chimson (2022)	Procedia Computer Science	CPS: Role, Characteristics, Architectures and Future Potentials	CPS, Characteristics

Table 2.2: Final List of Articles Included in the SLR

As the screening process and literature review are done, the results of the SLR and its given themes and topics are presented in the following sections, starting with OT.

2.2 Operational Technology (OT)

Operational Technology refers to physical systems, such as industrial systems or hardware, that monitor and control physical processes via physical devices in real time (Akbarzadeh & Katsikas, 2022; Kayan et al., 2022). In industrial areas today, all the physical components, machines, and processes that make the operations turn to produce electricity or manufacturing are all encompassed by OT. These components may be Programmable Logic Controllers (PLC), Remote Terminal Unit (RTU), and Supervisory Control and Data Acquisition (SCADA) systems (Tuptuk & Hailes, 2018). Under the umbrella of the term OT, we have Industrial Control Systems (ICS). ICS are computers, operating systems, and protocols like Modbus that operate in traditionally isolated environments, controlling systems from water plants, industrial productions, and oil refineries in real-time of these components in the physical world (Ashibani & Mahmoud, 2017; Franke & Brynielsson, 2014).

The Purdue model is is a structural model for ICS security and it is increasingly adopted by critical infrastructure operators. The model is part of the Purdue Enterprise Reference Architecture (PERA), which was designed as a reference model for data flows in Computer-Integrated Manufacturing (CIM) (Onshus et al., 2022; Tuptuk & Hailes, 2018; Williams, 1994). The model provides a network segmentation template for different components, processes, controls and IT-systems connected to within the context of OT. Figure 2.4 highlights zones or levels of the Purdue model, where level 0-3 is in the domain of OT, where PLC and other components reside (Onshus et al., 2022). Figure 2.4 illustrates the hierarchical structure of components and processes of OT and traditional IT systems and equipment in an ICS (Williams, 1994).

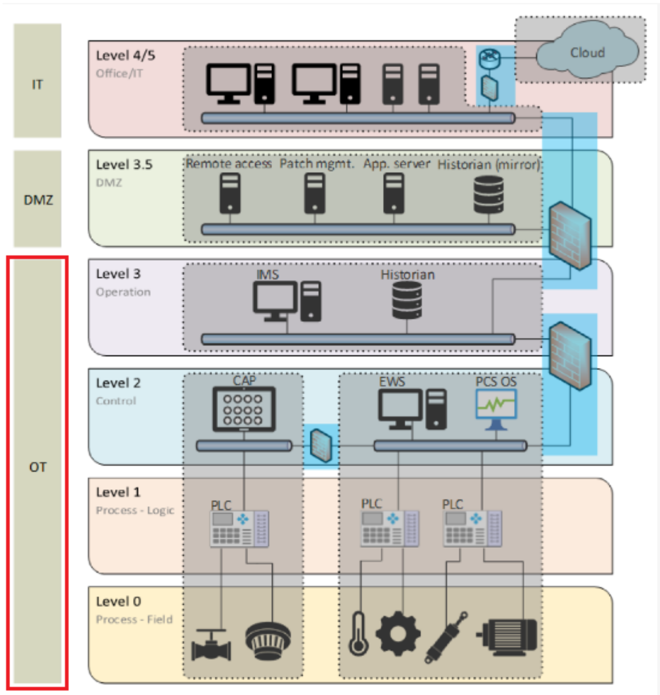


Figure 2.4: The Purdue model (Onshus et al., 2022, p. 25)

OT operates on the physical layer, in contrast to the cyber layer of IT, and as such, the human aspect is a part of the characteristics of OT (Akbarzadeh & Katsikas, 2022). Within level 2 of the Purdue model, we have the Control layer, where the physical layers of the OT environments are monitored and controlled via the SCADA systems and Human-Machine Interface (HMI) module (Kayan et al., 2022). OT systems are characterized as zero-tolerance real-time systems where safety and availability are critical attributes to be maintained at all times (Furrer, 2022; Lu et al., 2014; Piggin & Boyes, 2015). For OT and ICS environments to be operated efficiently, these systems are increasingly interconnected with the Internet for improved automation and functionality by remote systems (Ashibani & Mahmoud, 2017). Because of the interconnectivity, the collaboration between OT and IT has resulted in Cyber-Physical Systems (CPS) (Akbarzadeh & Katsikas, 2022). The clear distinction between the two is that OT deals with the physical aspects and components of the industrial environments through ICS on the lower levels of the Purdue model, while CPS is the interconnectivity and collaboration between IT and OT across all levels.

2.2.1 Cyber-Physical Systems (CPS)

Fink & Shulga (2018) highlighted the comprehensive definition of CPS as per The United States President's National Security Telecommunications Advisory Committee:

> "*Decentralized network of objects (or devices), applications, and services that can sense, log, interpret, communicate, process, and act on a variety of information or control devices in the physical environment. These devices range from small sensors on consumer devices to sophisticated computers in Industrial Control Systems (ICS). Ultimately, the devices have some type of kinetic impact on the physical world, whether directly or through a mechanical device to which they are connected.*"

In simpler terms, Akbarzadeh & Katsikas (2022) explain that CPS are systems that "[...] *integrate computation, communication, and controlling capabilities of Information and Communication Technology (ICT), with the traditional infrastructures. This integration facilitates the monitoring and controlling of objects in the physical world* [...]". Within the term CPS, the enabling technology of ICT/IT is the cyber layer. The connected nature of the physical systems and machines in the physical world, the physical layer, and the computers that control and manage them is the foundation of what defines CPS (Ashibani & Mahmoud, 2017; Lu et al., 2014; Shafi, 2012). Though CPS at first was categorized into these two layers, CPS architecture in its entirety mainly consists of a three-layer structure: Application-, Transmission- and Perception Layer (Ashibani & Mahmoud, 2017). Figure 2.5 highlights this architecture, showing the differences in the physical and cyber layers, as well as the interconnectivity between the layers in which CPS is defined.

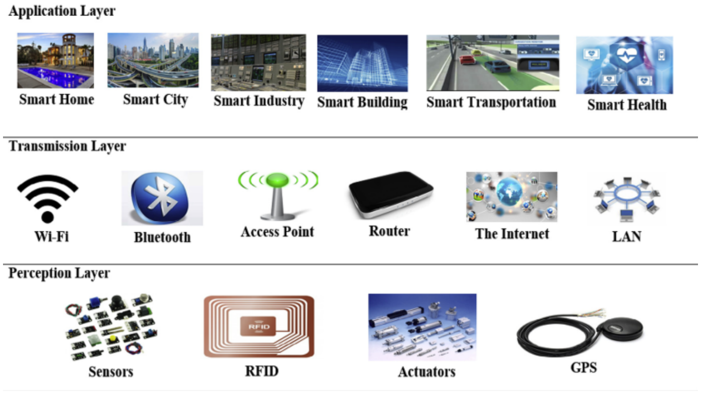


Figure 2.5: Three-Layer Architecture of CPS (Ashibani & Mahmoud, 2017)

To further expand on the notion of the CPS architecture, within the proposed three-layer architecture of Ashibani & Mahmoud (2017), Figure 2.6 expands on the architectural design on CPS, where the interconnectivity between the layers, also highlighting the importance of cloud-enabling systems on the top layer. The continuous connection between the physical devices (sensors, PLCs, etc.) and the cyber-infrastructure (Cloud technologies) is what CPS is composed of (Habib & Chimsom, 2022).

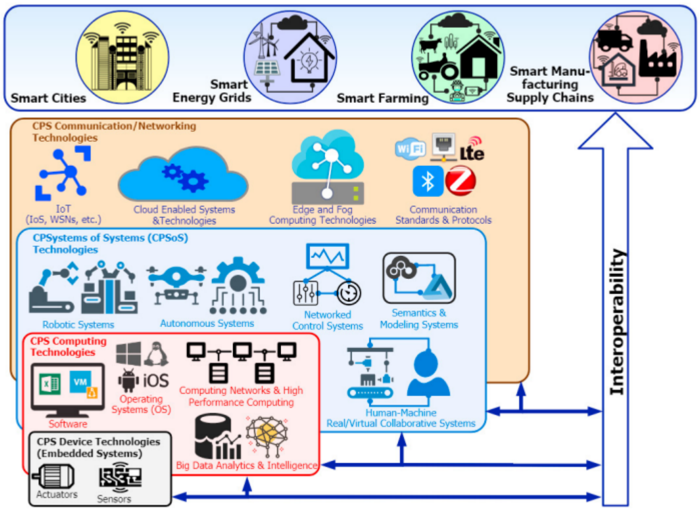

Smart Cities
Smart Energy Grids
Smart Farming
Smart Manu-facturing Supply Chains
CPS Communication/Networking Technologies
IoT (IoS, WSNs, etc.)
Cloud Enabled Systems &Technologies
Edge and Fog Computing Technologies
Wi Fi
lte
Communication Standards & Protocols
CPSystems of Systems (CPSoS) Technologies
Robotic Systems
Autonomous Systems
Networked Control Systems
Semantics & Modeling Systems
CPS Computing Technologies
VM
iOS
Software
Operating Systems (OS)
Computing Networks & High Performance Computing
Human-Machine Real/Virtual Collaborative Systems
CPS Device Technologies (Embedded Systems)
Actuators
Sensors
Big Data Analytics & Intelligence
Interoperability

Figure 2.6: CPS Architecture (Habib & Chimsom, 2022)

2.2.2 Information Technology (IT) vs Operational Technology (OT)

IT is the enabling technology that bridges the gap from the previously isolated OT/ICS system environments to the modern CPS, where the differences between the two are technological and a matter of perspective and priority (Kayan et al., 2022). As such, in contrast to IT, OT systems can have errors as long as it doesn't affect production and cause downtime, and the dependability towards safety rather than security plays a part when introducing the CIA triangle in the OT domain (Fink & Shulga, 2018; Lu et al., 2014). Furrer (2022, p. 116) defines security as "*[...] [protecting] the confidentiality, integrity, and availability (CIA) of computer system data and information from unauthorized and malicious accesses*".

The difference in safety and security regarding the CIA triangle is based on the prioritization of the system. In IT systems, the main priority is ensuring the confidentiality of the data that make up a system's various processes (Piggin & Boyes, 2015). While having a high level of service availability may be desirable, a service that occasionally experiences outages is not critical to corporate business operations (Piggin & Boyes, 2015). The opposite of that is true for OT/ICS environments, where downtime *is* critical. Piggin & Boyes (2015) lists "*control, system safety, system availability, plant/machine protection, operation/production and time-critical responsiveness in real-time operation*" as the emphasis of ICS. To highlight the differences between IT and OT while making a comparison between the two, Kayan et al. (2022) presents Table 2.3 with a comparison of the different attributes. The clear difference between the two domains is apparent when comparing the attributes, where applications are "time-sharing" for IT and "real-time" for OT. Additionally, the difference in protocols used, where OT uses insecure Modbus as an example, whereas IT uses secure TCP/IP and HTTP(S) (Tuptuk & Hailes, 2018).

	Information Technology (IT)	Operational Technology (OT)
Protocols	HTTP, TCP/IP, FTP, UDP, SMTP	Modbus, Fieldbus, DNP3, BACnet
Operations	Stochastic	Deterministic
Patching (Updating)	Easy to patch	Hard to patch
Applications	Time-sharing	Real-time
Skilled Personnel	Available	Hardly available
Deployment Cost	Low	High
Security Focus	Confidentiality	Availability
Authentication Method	Available	Barely available
Lifecycle	3–5 Years	Over 20 Years
Communication	User-centered	Machine-centered

Table 2.3: Fundamental Differences Between IT and OT Domains (Kayan et al., 2022, p. 7)

IT Security mainly relies on the system's Confidentiality, Integrity, and Availability of the data/information in the system, whereas OT relies on the system's dependability (Furrer, 2022). In Figure 2.7, Tuptuk & Hailes (2018) provides a clear distinction between the two domains and presents a model showcasing this differences, further highlighting the key aspects of OT and IT - Safety and Information Security (Confidentiality), respectively.

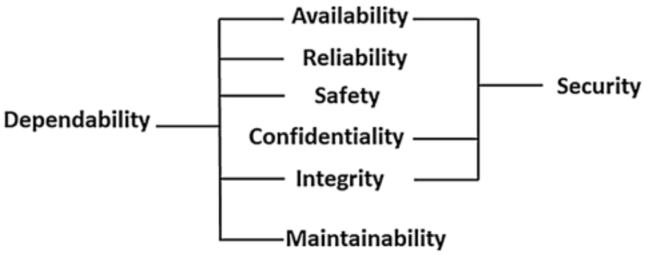


Figure 2.7: Difference and Comparison of Dependability and Security of IT and OT (Tuptuk & Hailes, 2018, p. 97)

2.2.3 Cybersecurity in IT and OT Safety

According to Furrer (2022, p. 90), security and safety are "*strongly required properties of a cyber-physical system...*" because of the two domains' interconnectivity, as was previously discussed. When combined with the physical characteristics of OT and the internet/cyber connectivity of IT, a CPS's vulnerabilities and risks can have serious repercussions in the real world (Ashibani & Mahmoud, 2017). A cyber-attack or system failure in an OT environment and the essential applications within a CPS can have serious real-world consequences, both to human safety and the environment. Safety is therefore essential when integrating IT into the OT sector and in a CPS (Ashibani & Mahmoud, 2017).

Ashibani & Mahmoud (2017) cites a few actual cyber-attacks against CPS, among them being Stuxnet. Iran's nuclear development was halted as a result of the 2010 attack on the Bushehr Nuclear Power Plant, which was able to compromise the computer systems and interfere with the facility's automated operations. There have been many incidents like this, as mentioned, where cyber-attacks on the cyber layer of CPS lead to severe real-world consequences, further highlighting the criticality of safety and (cyber)security in OT and IT, respectively (Ashibani & Mahmoud, 2017).

2.3 Security Operations Center (SOC)

The SOC is an internal or external organizational unit, traditionally associated with IT security, whose importance has grown significantly due to the need to prevent major cyber incidents (Vielberth et al., 2020). Essentially, the primary responsibility of a SOC is to detect, analyze, and respond to cybersecurity threats and incidents (Vielberth et al., 2020). By combining and managing processes, technologies, and people, a SOC provides organizations with situational awareness, risk mitigation, and aid in the fulfillment of regulatory requirements, enhancing the organization's overall security posture (Vielberth et al., 2020). Having a SOC provides organizations with a considerable advantage as incident response teams, processes, and technologies do not have to be set up reactively post-incident (Ahmad et al., 2021). Furthermore, to gain visibility and enable detection and analysis, SOCs utilize technologies such as Security Information and Event Management (SIEM) systems (Pöyhönen et al., 2021; Vielberth et al., 2020). The SIEM system collects security-relevant data in a centralized manner from systems and security technologies such as firewalls, intrusion detection and prevention systems, and antivirus (Pöyhönen et al., 2021; Vielberth et al., 2020). Providing analysts with the data required for the incident analysis, detection, and management process (Figure 2.8). During this process, analysts aggregate information and form a situation-specific analysis, applying their training, skills, and experience to triage and select the necessary course of action (Ahmad et al., 2021; Pöyhönen et al., 2021).

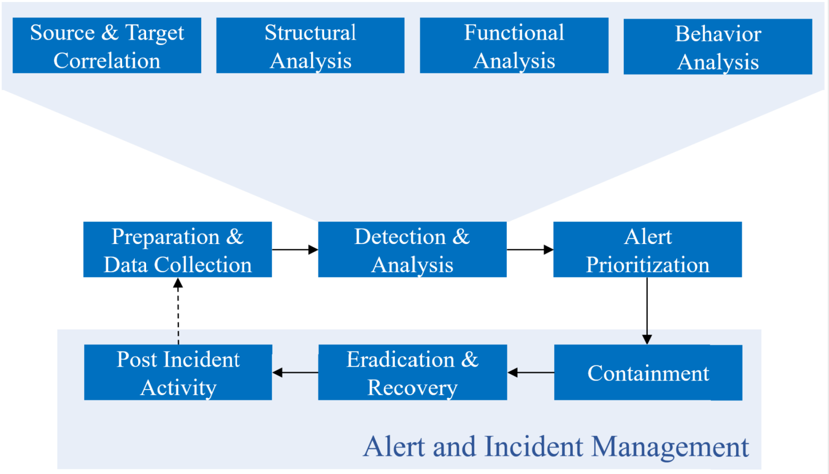


Figure 2.8: Incident Analysis, Detection, and Management Process (Vielberth et al., 2020, p. 227766)

A common notion throughout the literature is that SOCs are predominantly associated with IT systems and security (Ahmad et al., 2021; Kanamaru, 2020; Vielberth et al., 2020). However, there are mentions and discussions regarding SOCs concerning industrial and critical infrastructure applications (Dimitrov & Syarova, 2019; Kanamaru, 2020; Pöyhönen et al., 2021), safety management (Ahmad et al., 2021), and challenges in the SOC resulting from the increased complexity of IT and OT environments (Vielberth et al., 2020). This can likely be attributed to an increase in the number of cyber-attacks affecting ICSs, requiring new defensive capabilities to ensure the protection of OT infrastructure (Dimitrov & Syarova, 2019). The assessed literature presents two methods of using SOCs to monitor and protect OT environments. Dimitrov & Syarova (2019) presents a shared industrial or ICS SOC, which directly monitors the operational environment by collecting data from the SCADA, data historian, and operator. On the other hand, Kanamaru (2020) and Pöyhönen et al. (2021) clearly separate the responsibilities of the OT operator or maintainer and the SOC, suggesting that the SOC remains responsible for and monitors IT systems, networks, and related security products (Firewalls, Intrusion Prevention and Detection systems, etc.) while the operator and maintainer remain responsible for the OT (Kanamaru, 2020; Pöyhönen et al., 2021). Instead, the SOC, maintainer, and operator continuously cooperate during monitoring by sharing symptomatic events, domain knowledge and information, and during incident management and post-incident activities (Kanamaru, 2020).

2.3.1 Industrial Control Rooms

In industrial organizations, the Control Room (CR), often referred to as the control center or control station, makes use of various processes, technologies, and people to monitor and control physical operations in complex and dynamic systems (Kayan et al., 2022; Vincente et al., 2001). The operators situated in the CR utilize on-board OT systems to obtain an overview of the current situation and ensure control and safety in the operation and its physical processes (Onshus et al., 2022). Onshus et al. (2022) refer to the Gartner Glossary when defining OT systems, describing it as “hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events”. In these systems, HMIs facilitate the interaction between the CR and the ICSs overseeing the processes, providing operators with an interface to monitor and control their operations (Kayan et al., 2022). Additionally, operators rely on multiple sources of information to stay situationally aware, such as field operators or alarm screens, control room panels and displays (Kayan et al., 2022; Vincente et al., 2001). CRs show a close resemblance to, but are fundamentally different from SOCs (Figure 2.9 & 2.10), while SOCs are primarily concerned with security and cyber incidents, CRs are focused on maintaining the availability and safety of physical operations (Onshus et al., 2022; Vielberth et al., 2020).

During the literature review, most of the literature identified on the topics of industrial control rooms and control centers were dated, not relevant to the current state of technology, or only contained brief mentions of the concepts without providing any significant insight. While we managed to identify a few articles by Vincente et al. (2001), Kayan et al. (2022), and Onshus et al. (2022) that addressed some aspects related to industrial control rooms, literature on the subjects seemed to be scarce, lacking, or non-descriptive.

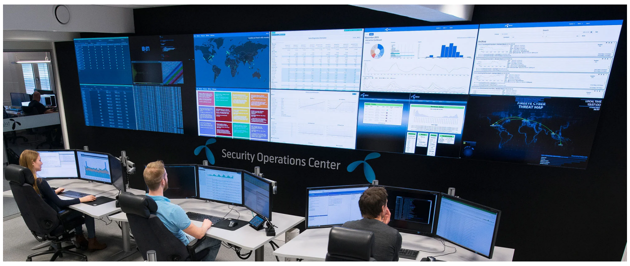


Figure 2.9: Telenors Security Operations Center (Telenor, n.d.)

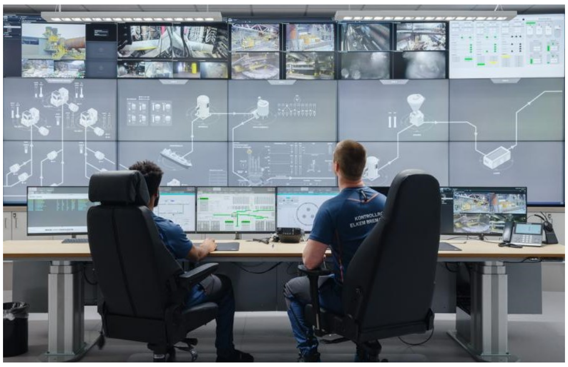


Figure 2.10: Elkem’s Control Room in Bremanger (Afry, 2023)

2.3.2 SOC Structure and Personnel

Like every other organizational unit, the SOC has several different roles and responsibilities (Vielberth et al., 2020). Most SOCs operate as tiered entities across which expertise and capabilities are distributed into different levels of incident response, where higher tiers correlate with higher levels of expertise and specialization (Nyre-Yu et al., 2019). Based on findings from Vielberth et al. (2020), Ahmad et al. (2021), and Nyre-Yu et al. (2019), SOCs are usually comprised of various tiers of analysts which represent the operations core capabilities, and dedicated managers that supervise the security operations team. A simplified overview of the relationship and interactions between the various tiers of analysts, the SOC manager, and external stakeholders is depicted in Figure 2.11.

- **Tier 1 Analysts** (L1) monitor, prioritize, investigate, and respond to security alerts, and are typically responsible for the initial filtering and triaging of alerts once they are detected (Ahmad et al., 2021; Nyre-Yu et al., 2019). Upon detection, tier 1 analysts determine whether an alert is justified or a false positive, they subsequently assess the risk of justified alerts and collect raw data to enrich alerts and build context (Ahmad et al., 2021; Nyre-Yu et al., 2019; Vielberth et al., 2020). Low-severity incidents are usually managed entirely by tier 1 analysts, while complex or higher-severity incidents are escalated to more senior analysts (Ahmad et al., 2021; Vielberth et al., 2020).

- **Tier 2 Analysts** (L2) are tasked with reviewing the more critical security incidents escalated by tier 1 analysts. These analysts have more experience and are aware of the affected systems and have a better understanding of the scope of an attack (Vielberth et al., 2020). Using the context data provided by the first tier, tier 2 analysts conduct a short, more in-depth investigation to determine the right course of action to contain or remediate the threat (Nyre-Yu et al., 2019; Vielberth et al., 2020). Incidents that require further investigation or action, or if the tier 2 analyst encounters issues with identifying or mitigating the attack, are escalated to tier 3 analysts.

- **Tier 3 Analysts** (L3) are the most experienced workforce in a SOC and are often proficient in threat hunting, vulnerability assessment, and penetration testing (Vielberth et al., 2020). These analysts handle major incidents and critical security alerts escalated from tier 1 and 2 analysts, performing deeper analysis to better understand cause and effect, and determine or develop remedial measures and prevention activities (Nyre-Yu et al., 2019; Vielberth et al., 2020). Most importantly, tier 3 analysts proactively work to identify potential threats, security gaps, and vulnerabilities in relevant systems and provide recommendations on how to best remove or reduce risk (Vielberth et al., 2020).

- **SOC Managers** are experienced security analysts who supervise the SOC team and handle the administrative side of the operations. Responsibilities include providing technical guidance and training, creating processes, reviewing incident reports, and implementing crisis communication plans. Additionally, the SOC manager reports to top-level management, acting as the SOCs representative and management bridge (Vielberth et al., 2020).

- **External Personnel** “[...] can be included in any SOC operation, and therefore, depending on the architecture and operating model of a SOC, more or less external personnel are involved in the different SOC roles and groups.” (Vielberth et al., 2020, p. 227762).

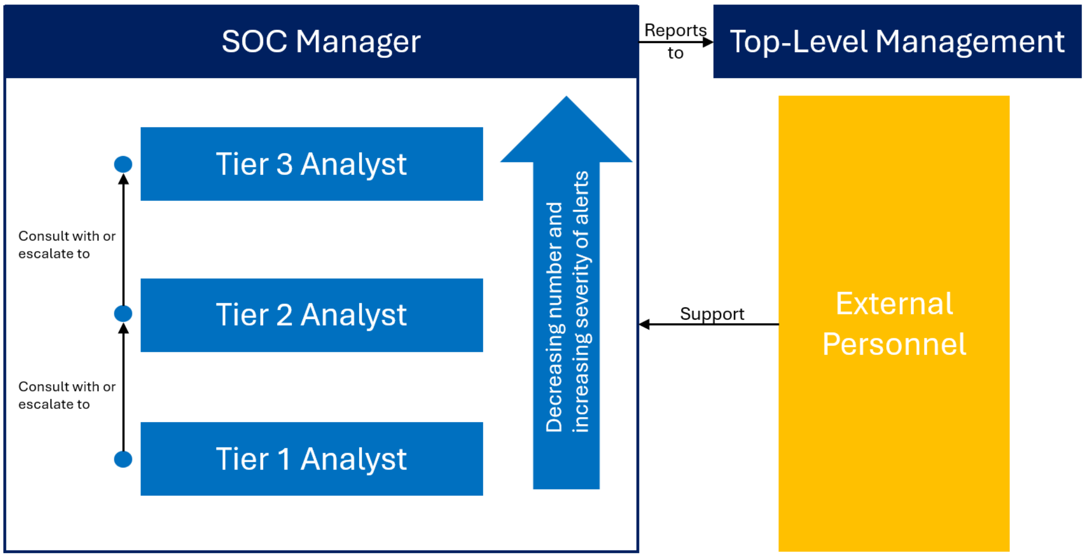


Figure 2.11: Interaction of Different Roles Within a SOC (adapted from Vielberth et al. (2020))

2.3.3 Challenges

Due to a lack of literature addressing SOC challenges that fit the criteria of the review, this section is largely based on Vielberth et al. (2020) review of 158 academic publications. From these publications Vielberth et al. (2020) present a series of challenges that impose the development and improvement of SOCs, some of which we found relevant to our work. Additionally, the findings of Nyre-Yu et al. (2019) provide some backing to the challenges proposed by Vielberth et al. (2020). These challenges address the collaboration of experts, integration of domain knowledge, and increasing technological complexity (Vielberth et al., 2020).

The first of these challenges is the absence of collaboration between experts, which is also brought up by Nyre-Yu et al. (2019) as an issue impeding progress in SOCs. Due to a lack of collaborative efforts among analysts and analysts and stakeholders who work on different sites, analysts tend to work on problems independently (Nyre-Yu et al., 2019; Vielberth et al., 2020). This could result from time pressure or lack of communication and collaboration platforms supporting SOC-specific requirements (Vielberth et al., 2020). Additionally, the tiered nature of the SOC accentuates the issue by creating notable differences in the experience and knowledge available on the individual tiers (Nyre-Yu et al., 2019). Consequently, this causes a reduction in overall staff interaction, motivation, and efficiency and creates a separation of expertise (Nyre-Yu et al., 2019; Vielberth et al., 2020).

Increased complexity caused by the growth and expansion of IT infrastructure into CPS and physical applications makes it progressively harder to identify threats and incidents (Vielberth et al., 2020). Current tools work well for detecting known attacks and attack patterns but become insufficient when previously unseen and unknown situations occur. Hence, including security and non-security experts' perspectives and domain knowledge becomes crucial in understanding and dealing with these situations. Non-security experts, such as engineers, are becoming increasingly invaluable due to their knowledge, which provides the insight necessary to evaluate whether an alert or the reported behavior is malicious or benign, especially in the context of CPS. Additionally, tying human experts and machines closer together and providing them with processes and technologies to transfer knowledge in either direction is a significant challenge for SOCs. The combination of domain knowledge from humans and explicit knowledge from machines can be leveraged to further the capabilities of the SOC (Vielberth et al., 2020).

As IT and OT become more interconnected into CPSs, the complexity of the technological environments increases, introducing notable challenges for SOCs (Vielberth et al., 2020). More complicated and intertwined infrastructure, numerous data sources, and exceedingly diverse data make it difficult for SOC personnel to maintain situational awareness and a cohesive overview. Analysts have poor visibility into networks due to difficulties keeping track of all the devices in the network. The increasing number of devices increases the amount of data sources, which in turn increases the overall number of events and potentially the amount of irrelevant or useless data and the number of false-positive alerts. Additionally, the data captured from the infrastructure is as diverse as its sources, making it hard to process, analyze, understand, and link, hindering the discovery of whether individual events are part of a bigger attack. Consequently, this results in analysts becoming "[. . .] *overloaded with a high volume of [false positive] alerts and face a typical "needle in a haystack" problem when trying to filter the noise.*" (Vielberth et al., 2020, p. 227773).

2.4 Cyber Incident Management and Response

Incident Response (IR) and Incident Management (IM) are established concepts encompassing the preparation for and response to unplanned incidents that negatively affect an organization (Smith et al., 2021). Understanding how organizations can protect their resources from sophisticated and persistent cyberattacks is a significant challenge for research and practice (Ahmad et al., 2021). When a cyber incident occurs, IM and IR are the final barriers to what may become an unmitigated disaster (Tuptuk & Hailes, 2018). The purpose of IM and IR is to prevent the success of cyberattacks, minimize the impact through containment, and return to regular operation in the shortest possible time by eradicating the threat from the organization (Ahmad et al., 2021; Furrer, 2022). In most cases, lower severity cyber incidents will be handled by security analysts or IT personnel, while higher severity and major IR will likely be handled by an experienced cross-functional team (Ahmad et al., 2021). Furthermore, while IR is the act of responding to an incident, IM is the preparation and planning facilitating effective IR. The objective of IM is to plan and prepare for how to best respond to an incident such that decisions can be made quickly and proper action can be taken to mitigate the impact of the attack (Furrer, 2022). Ensuring that the necessary resources, governance structure, and processes are in place before an incident to allow responsible individuals to operate rapidly and effectively (Ahmad et al., 2021; Tuptuk & Hailes, 2018). This is crucial when considering that "[IR] *takes place under considerable time pressure in a dynamic and rapidly changing organizational environment with high levels of information load, information diversity and task uncertainty.*" (Ahmad et al., 2021, p. 2). As such, IM must facilitate for "[...] *command, control and coordination of diverse people, processes, and technologies to develop situation awareness of the threat and incident environment within a rapidly evolving organizational context.*" (Ahmad et al., 2021, p. 2). Essentially, these activities need close collaboration between operational, tactical, and strategic stakeholders and be adaptive to the highly dynamic nature of cyber-incidents, requiring cross-disciplinary team efforts, communication, and shared situational awareness to respond effectively (Ahmad et al., 2021; Nyre-Yu et al., 2019; Pöyhönen et al., 2021; Smith et al., 2021).

2.4.1 Industrial Cyber Incident Management and Response

The increased threat towards OT systems presents a series of challenges for traditional IM and IR teams (Smith et al., 2021). Industrial technologies do not operate in the same manner as IT equipment; when IT devices are compromised, the impact is often limited to the functionality of those devices (Smith et al., 2021). However, in OT environments, cyber incidents can negatively impact critical equipment and operations, potentially compromising human and environmental safety or leading to a loss of availability, impairing essential services such as energy or communications (Ashibani & Mahmoud, 2017; Smith et al., 2021). "*[IR] within [OT environments] is characterized by high levels of uncertainty and unpredictability and requires a multi-disciplined team that encompasses personnel business operations, [OT], IT, security operations and media engagement to be effective.*" (Smith et al., 2021, p. 1). Still, industrial organizations often have limited and poorly established documentation, awareness and training, response, and other cyber-IM measures (Tuptuk & Hailes, 2018). Consequently, many of the processes applied in IR are driven by approaches used for IT, and as a result, may prove ineffective or cause the situation to deteriorate by amplifying the impact of cyber incidents on industrial infrastructure (Smith et al., 2021). This is a result of the inherent differences between OT and IT. IR in OT infrastructure requires other considerations and defense strategies and should reflect the safety critical context of such systems (Smith et al., 2021). Although maintainers and operators of OT systems typically have IR plans and contingencies in place for physical incidents such as loss of essential power, supplies, and output, it is only recently that these plans have started to consider cyber impact (Smith et al., 2021).

From a selection of literature discussing IM and IR in the industrial context, we have identified a series of requirements that impact IR efforts in OT environments (Table 2.4). Generally, it is first necessary to determine whether existing IR measures apply to OT and evaluate whether or not they accommodate the characteristics of such systems (Smith et al., 2021). Additionally, to prepare operators and other OT personnel for possible cyber incidents, methods and tools should be implemented that support the response process and consider the nature of industrial technologies. We have identified four key requirements for IR in industrial environments:

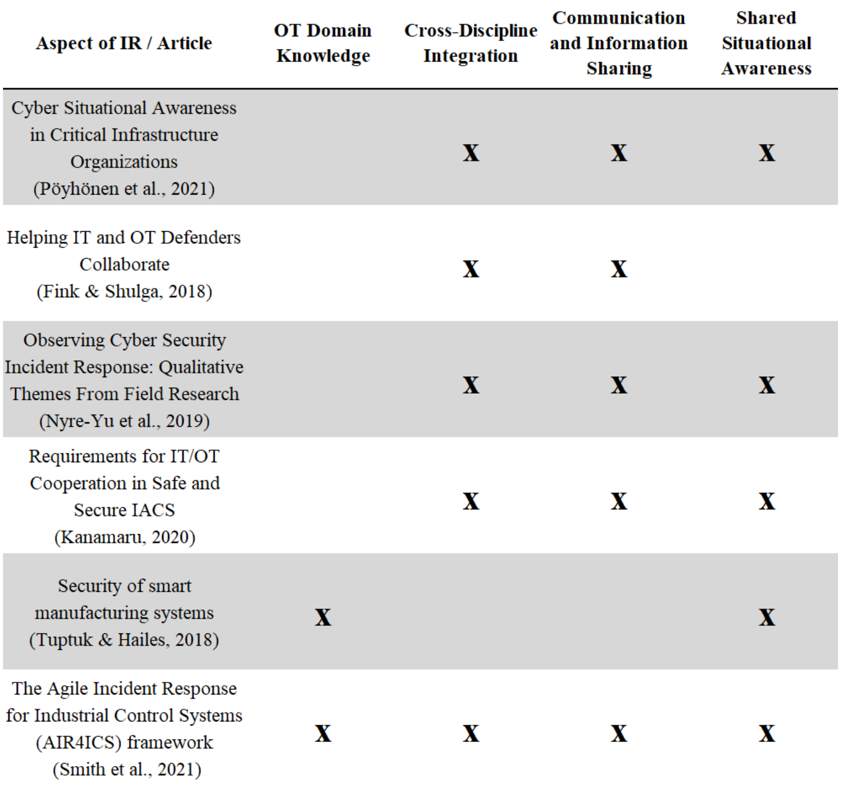
1. **Domain Knowledge of OT -** Considering the highly contextualized and varied nature of OT systems, a core element of any response is domain knowledge and an understanding of existing system requirements (Smith et al., 2021). In many cases, "[...] *there is a lack of information about systems, and how systems work, which is commonly attributed to how old and complex OT systems might be, as well as the lack of people having the appropriate expertise being available.*" (Smith et al., 2021, p. 5). As such, the individuals involved in IR must develop their knowledge of OT systems to allow them to operate effectively within the environment.

2. **Cross-Discipline Integration -** In the OT domain, cyber incidents rarely originate solely from the physical side, and the consequences of a single compromised device will often propagate and carry repercussions along the entire process (Smith et al., 2021). This means that individual incidents may have a significant impact further down the production line, affecting several domains within the organization. Therefore, the IR team should include stakeholders from other business units, such as engineers, physical plant operators, business analysts, management, etc., creating a multi-disciplined team that facilitates knowledge exchange between the various groups and the cyber security professionals (Fink & Shulga, 2018; Pöyhönen et al., 2021; Smith et al., 2021). Providing a more holistic view of the situation and the responders with the ability to understand the implications of the incident on their work and that of others (Smith et al., 2021).

3. **Communication and Information Sharing -** In many cases, when IR crosses IT/OT

boundaries, communication between stakeholders from different domains, departments, levels in the organizational hierarchy, and 3rd party organizations often becomes problematic (Fink & Shulga, 2018; Smith et al., 2021). IR teams tend to be very hierarchical, with individuals being assigned specific roles, leading to the creation of information silos (Smith et al., 2021). This causes IR participants to focus on their tasks without understanding what others are doing. In the rapidly changing and high-pressure environment of industrial IR, a lack of communication increases the risk of mistakes, information deterioration, or redundant efforts as tasks are duplicated or responsibility for crucial information becomes unclear (Smith et al., 2021). Information sharing between interest groups and continuous communication is essential for IR, ensuring SA, coordination, and operational efficiency (Fink & Shulga, 2018; Pöyhönen et al., 2021).

4. **Shared Situational Awareness -** The efficiency of the response to a cyber-incident is dependent on the IR team's ability to develop and sustain shared SA throughout the lifetime of the incident (Ahmad et al., 2021). Shared awareness is a requirement for good management, a key component of effective cyber defense operations, and considered a critical attribute of organizational IR, enabling stakeholders to understand what is happening and facilitating the dynamic shift of tasks as the situation develops (Ahmad et al., 2021; Nyre-Yu et al., 2019; Pöyhönen et al., 2021; Smith et al., 2021). This necessitates cross-discipline cooperation, information sharing, and communication, and that all members are informed and involved in the planning and implementation of the response (Ahmad et al., 2021; Pöyhönen et al., 2021; Smith et al., 2021). Providing the IR team with shared awareness of the incidents cyber-threat landscape and the broader organizational context (Ahmad et al., 2021).



Aspect of IR / Article	OT Domain Knowledge	Cross-Discipline Integration	Communication and Information Sharing	Shared Situational Awareness
Cyber Situational Awareness in Critical Infrastructure Organizations (Pöyhönen et al., 2021)		X	X	X
Helping IT and OT Defenders Collaborate (Fink & Shulga, 2018)		X	X	
Observing Cyber Security Incident Response: Qualitative Themes From Field Research (Nyre-Yu et al., 2019)		X	X	X
Requirements for IT/OT Cooperation in Safe and Secure IACS (Kanamaru, 2020)		X	X	X
Security of smart manufacturing systems (Tuptuk & Hailes, 2018)	X			X
The Agile Incident Response for Industrial Control Systems (AIR4ICS) framework (Smith et al., 2021)	X	X	X	X

Table 2.4: Classification of Literature with Respect to Critical Aspects in Industrial IR

2.5 Situational Awareness

In dynamic environments, such as large-systems operations, human decision-makers must make multiple decisions over a short span of time (Endsley, 1995; Pöyhönen et al., 2021). To arrive at a well-informed conclusion, decision-makers must build awareness related to a situation, or Situational Awareness (SA), by utilizing prior knowledge and current perceptions of reality to understand what is happening and predict potential future outcomes (Pöyhönen et al., 2021; Tadda & Salerno, 2010).

SA is a varied and well-studied phenomenon that can be viewed from multiple perspectives. From a technical perspective, SA involves compiling, processing, and fusing data (Franke & Brynielsson, 2014). At the same time, the cognitive side is concerned with the human capacity to comprehend the technical implications and draw conclusions to come up with informed decisions (Franke & Brynielsson, 2014). The most widely accepted definition of SA in the reviewed literature, as discussed by Franke & Brynielsson (2014), Pöyhönen et al. (2021), Tadda & Salerno (2010), Evesti et al. (2017), and Ahmad et al. (2021), is the one provided by Endsley (1995). From a cognitive perspective, Endsley (1995) defines SA as "*the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*". As such, SA can be considered as a state of knowledge that can be achieved at different levels, the quality of which is dependent and based on an individual's preconceptions, abilities, experiences, and training (Ahmad et al., 2021; Endsley, 1995; Pöyhönen et al., 2021; Tadda & Salerno, 2010).

Figure 2.12 illustrates the process of attaining SA of the environment, the relationship between SA, decision-making, and action execution, and the three levels of SA. These levels denote progressively increasing awareness levels and makeup SA, which is a foundation for conclusions and the following decision-making (Franke & Brynielsson, 2014; Pöyhönen et al., 2021). Initially (Figure 2.12 L1), the operator perceives their environment and attempts to obtain as much information about the situation's status, attributes, and dynamics as possible (Endsley, 1995). During level 2 (Figure 2.12 L2), the operator's preconceptions, abilities, experiences, training, and goals are applied to the gathered information to understand the situation (Endsley, 1995). In the final stage (Figure 2.12 L3), the gathered information and the understanding of the situation are combined by the operator to predict future outcomes and their implications (Endsley, 1995; Franke & Brynielsson, 2014). This knowledge is then used to inform decision-making which results in the execution of an action. Subsequently, changes in the environment resulting from the selected action are perceived by the operator as feedback that may or may not coincide with the operator's prediction (Endsley, 1995). The iterative process then starts again, with the operator basing SA on the altered state of the environment.

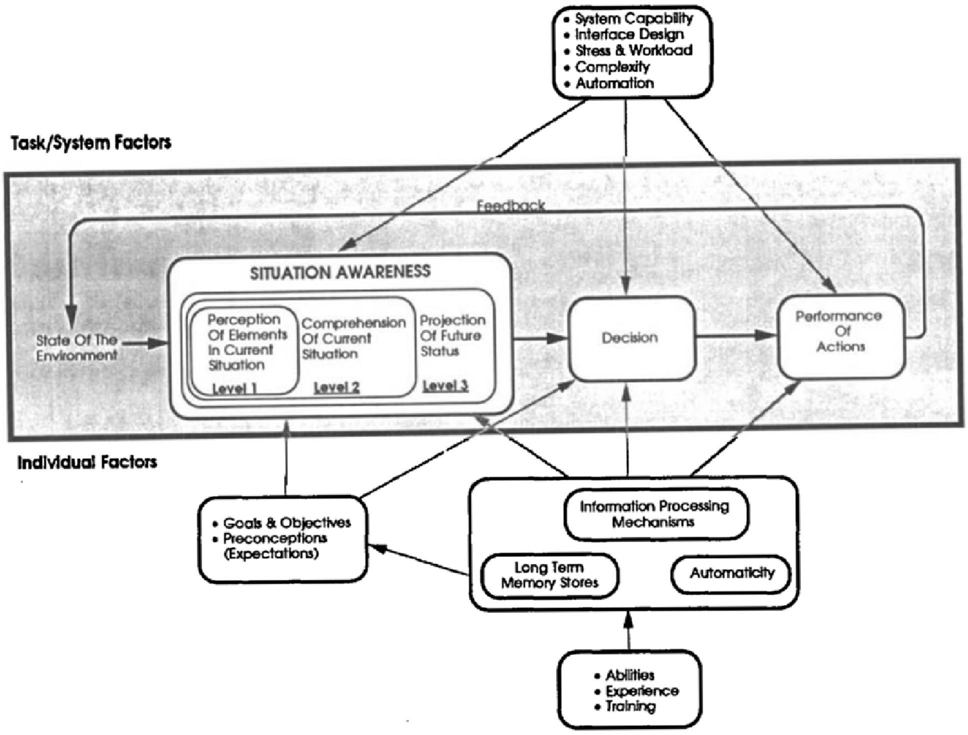


Figure 2.12: Model of Situation Awareness in Dynamic Decision Making (Endsley, 1995, p. 35)

2.5.1 Shared Situational Awareness

In addition to presenting SA from an individual perspective, Endsley (1995), Tadda & Salerno (2010), Ahmad et al. (2021), and Pöyhönen et al. (2021) discuss the concept of shared, organizational, or team SA. This shared SA concept applies to situations requiring several actors to cooperate in decision-making and carrying out actions (Endsley, 1995). In a team, each member possesses some specific set of information or SA elements determined by the individual's role or responsibilities within the team (Endsley, 1995). By sharing and coordinating each member's set of SA elements, all members can obtain SA of shared elements and better understand the situation as a whole (Endsley, 1995). Figure 2.13 presents a simple representation of team SA where the team members are represented as circles with SA elements. These circles intersect where members coordinate their information and obtain shared SA. Endsley (1995, p. 39) defines team or shared SA as "[...] *the degree to which every team member possesses the SA required for his or her responsibilities.*", while Tadda & Salerno (2010, p. 21) state that "*Shared Situation Awareness is then a consensus view of a number of individual views about a specific activity or set of activities.*". From a general perspective, shared SA is centered on knowledge management and information sharing to ensure that all relevant stakeholders have SA for all their individual requirements (Ahmad et al., 2021; Endsley, 1995; Pöyhönen et al., 2021).

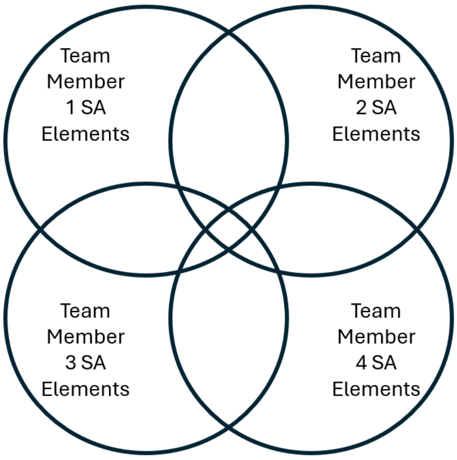

Team Member 1 SA Elements
Team Member 2 SA Elements
Team Member 3 SA Elements
Team Member 4 SA Elements

Figure 2.13: Team SA

In an organizational context, shared SA is considered one of the most significant goals in improving cybersecurity and a key component of effective cyber defense operations (Nyre-Yu et al., 2019; Pöyhönen et al., 2021). "*Facilitated by information sharing, the process of establishing shared awareness is not a one-way information flow, but rather a cycle that needs to include a feedback flow sometimes lacking in organizations.*" (Nyre-Yu et al., 2019, p. 439). This two-way information and feedback flow should exist between the organizations' strategic, operational, and technical/tactical decision-making levels (Nyre-Yu et al., 2019; Pöyhönen et al., 2021). Without feedback, analysts sending or escalating incidents may become uncertain regarding action and resolution (Nyre-Yu et al., 2019). Feedback aids in establishing a common operational picture, guide IR decision-making, and enables learning (Nyre-Yu et al., 2019). Additionally, notifying mid- and senior-level managers of an incident creates shared awareness among management and enables them to use the information provided in strategic decision-making or incident mitigation (Nyre-Yu et al., 2019). "*One caveat is that shared awareness must remain consistent throughout the incident response process and is typically maintained through documentation.*" (Nyre-Yu et al., 2019, p. 440). If maintained, documentation can ensure persistent awareness; otherwise, it can impede accurate and consistent awareness during a developing incident (Nyre-Yu et al., 2019).

2.5.2 Cyber Situational Awareness

Whilst not greatly different from SA in more traditional domains, Cyber SA (CSA) is a term largely discussed in the context of IT security and is considered to be a subset of SA that concerns digital technologies and networked systems, or the "cyber" environment (Ahmad et al., 2021; Evesti et al., 2017; Franke & Brynielsson, 2014; Tadda & Salerno, 2010). This is evident in the reviewed literature where most of the authors have adapted or based their definitions of CSA on Endsley's (1995) notion of SA (Table 2.5). The authors translate and adapt the three main levels of SA perception, comprehension, and projection into phrases such as gathering of data, information aggregation, and future impact assessment to better fit the context of the cyber environment. Additionally, the literature provides different definitions of CSA depending on the context in which CSA is addressed. From a holistic cybersecurity perspective Evesti et al. (2017, p. 1) state that the purpose of CSA is "[. . .] *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.*". While Ahmad et al. (2021, p. 10) consider CSA from a cybersecurity incident response point-of-view, arguing that organizations must "[. . .] *(1) 'collect the dots', i.e. collect alerts and raw details of the incident-related environment (perception), (2) 'connect the dots', i.e. synthesize elements of the incident with existing knowledge, and assess criticality and overall significance of the* *incident in the context of cybersecurity objectives (comprehension), and (3) 'project from the dots', i.e. construct possible incident scenarios in the immediate future to inform appropriate response (projection).*". Lastly, it is important to note that CSA is concerned with cyber incidents, offering added insight into a situation and is inherently a part of overall SA (Franke & Brynielsson, 2014). Therefore, CSA should be treated in combination with information from other domains and disciplines and contextualized for decision-makers to fully comprehend the situation (Franke & Brynielsson, 2014; Matthews et al., 2016).

SA Level / Article	**Level 1**	**Level 2**	**Level 3**
Toward a Theory of Situation Awareness in Dynamic Systems (Endsley, 1995)	"The first step in achieving SA is to perceive the status, attributes, and dynamics of relevant elements in the environment."	"Level 2 SA goes beyond simply being aware of the elements that are present to include an understanding of the significance of those elements in light of pertinent operator goals."	"The ability to project the future actions of the elements in the environment at least in the very near term forms the third and highest level of SA. This is achieved through knowledge of the status and dynamics of the elements and comprehension of the situation (both Level I and Level 2 SA)"
Cyber situational awareness - A systematic review of the literature (Franke & Brynielsson, 2014)	(i) basic perception of important data/ perception	(ii) interpretation and combination of data into knowledge/ comprehension	(iii) ability to predict future events and their implications/ projection
Cyber Situational Awareness in Critical Infrastructure Organizations (Pöyhönen et al., 2021)	data acquisition/ detection	information aggregation/ situational understanding	classification and analysis/ impact assessment towards the future
Cyber Situational Awareness - Issues and Research (Tadda & Salerno, 2010)	Perception is the attempt to answer the question "What are the current facts?"	Comprehension asks, "What is actually going on?"	Projection asks, "What is most likely to happen if...?"
Cyber Situational Awareness Taxonomy (Evesti et al., 2017)	gather information from the environment	understand gathered information	reflecting the gained understanding for the current environment
How organizations develop situation awareness for incident response: A case study of management practice (Ahmad et al., 2021)	(1)'collect the dots'	(2) 'connect the dots'	(3) 'project from the dots'

Table 2.5: Levels of SA as Described in the Literature

Independent of the context for which CSA is needed, whether for routine operational or command and control work related to a specific situation, CSA is often the result of a shared effort (Franke & Brynielsson, 2014; Pöyhönen et al., 2021). From a technical perspective, CSA can be considered a problem of collecting, synthesizing, and deriving insights from useful information (Ahmad et al., 2021). Hence, stakeholders must cooperate and share information to obtain a common understanding of the situation or shared CSA (Matthews et al., 2016; Pöyhönen et al., 2021). Shared CSA can be viewed as a state in which all relevant stakeholders possess the information necessary to achieve CSA regarding some situation in a cyber environment, such that they might accurately and efficiently manage their responsibilities (Endsley, 1995; Franke & Brynielsson, 2014; Tadda & Salerno, 2010). The assessed literature suggests that to achieve a high level of shared CSA stakeholders must understand the integrated meaning of what they are perceiving by leveraging technologies, processes, expertise, collaboration, and communication (Ahmad et al., 2021; Matthews et al., 2016; Pöyhönen et al., 2021). Various technologies are essential in that it is what make up the "cyber" environment and enable data gathering, analysis, and visualization. However, the foundation of shared CSA is dependent on the sharing of information and expertise through collaboration and communication between internal and external stakeholders across organizational levels (strategic, operational, and tactical) (Ahmad et al., 2021; Franke & Brynielsson, 2014; Pöyhönen et al., 2021).

2.6 Research Gap

Through a systematic assessment of the current body of knowledge on OT, SOC, SA, IR, and IM, we have noted some areas in which knowledge or research is lacking or dated and others in which we could not locate relevant literature. It should be mentioned that there is a rich and recent pool of literature on the individual topics themselves; it is, instead, where these topics coalesce that literature starts to get scarce.

To understand how CSA is established in a SOC setting, we need to understand how actors in and around the SOC work, their processes, and with whom they interact. However, when looking into SOCs, we found that there is a general lack of independent literature describing specific processes and interactions in SOCs, both between internal and external actors and entities. This corresponds to Vielberth et al. (2020), who found that there is inadequate literature on and precise definitions of the processes within SOCs. Similarly, there seems to be a shortage of literature on SOCs in the context of OT or ICS. The few articles we identified briefly address the concept of a shared ICS SOC (Dimitrov & Syarova, 2019) or the collaboration of cyber security professionals in SOCs and industrial stakeholders (Fink & Shulga, 2018; Kanamaru, 2020).

Our systematic literature review has revealed a significant research gap in OT SOCs and related processes. While recent research by Ahmad et al. (2021) and Andreassen et al. (2023) has contributed to our understanding of SA in SOC-IR from an IT perspective, we find a significant gap in research and literature on CSA in OT-SOC IR. Searches across Scopus and the Web of Science yielded seven results: one book, two conference papers, and four peer-reviewed articles (Figure 2.14 & 2.15). Among these results, we only found two articles to be somewhat relevant, although we did not find anything that directly addresses CSA in OT-SOC in general or CSA in OT-SOC IR. We also conducted searches on IEEE Xplore and Google Scholar but were unable to identify any research or literature relevant to the scope of this study. Furthering the relevance of this study and highlighting the need for research into OT-SOC, OT-SOC processes, and the topic area of this study, CSA in OT-SOC IR.

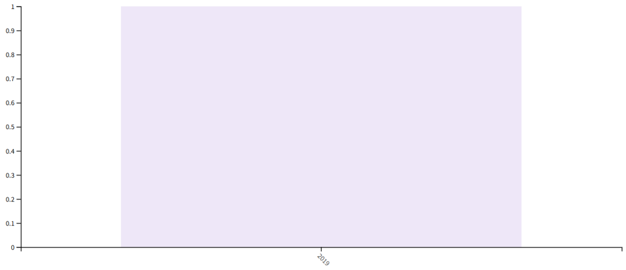


Figure 2.14: All Time Bar Chart of Publications by Year for OT AND CSA AND SOC AND IR (Web of Science, n.d.)

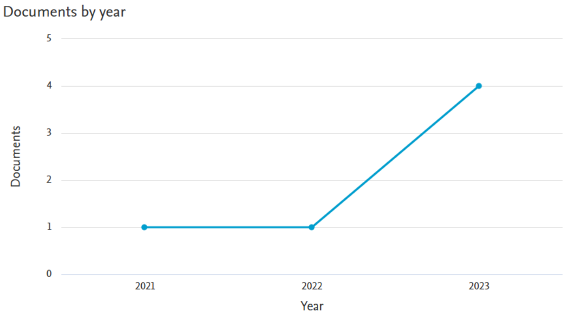


Figure 2.15: Publications by Year from 2021-2023 for OT AND CSA AND SOC AND IR (Scopus, n.d.)

2.7 Theoretical Lens

In short, the theoretical lens is a conceptual mechanism that guides the research, providing a uniform point of assessment through which all data is filtered and is how we interpret the phenomena we study (Niederman & March, 2019). We have identified two theories and two frameworks from the systematic literature review, which will make up the theoretical lens that drives our approach to data analysis. The theoretical lens will serve as a transformative or filtering device, allowing us to sort, contextualize, and transform our data into meaningful information to create a theoretical framework (Niederman & March, 2019). Additionally, the lens provides a means of highlighting relationships and patterns that would otherwise be difficult to notice due to information overload and many undifferentiated details (Niederman & March, 2019). Enabling us "[...] *to identify the components of the target, organize into categories attributes of the target, and propose the nature of relationships among these components and/or attributes.*" (Niederman & March, 2019, p. 5).

Our study aims to expand upon the work of Andreassen et al. (2023) on SA in cybersecurity SOC-IR. Based on the results of the SLR, we have selected two theories and two supporting frameworks. First, the study will be founded on Endsley's (1995) SA theory, which considers SA from an information-processing perspective. Secondly, due to the distinct differences in knowledge, skillsets, and priorities between the IT and OT domains, we theorize that SA during IR is dependent on the cooperation and coordination of knowledge and understanding from both domains. We therefore combine Collective Intelligence (CI) theory and Endsley's (1995) SA theory to explain how individuals and groups acquire SA in cross-domain and multi-actor environments. Lastly, the process model for SA in cybersecurity IR by Ahmad et al. (2021) and the Purdue Model as presented by Onshus et al. (2022) act as supporting frameworks. The process model by Ahmad et al. (2021) provides us with a starting point to better understand the underlying process of acquiring SA in cybersecurity IR. Additionally, the Purdue model by Onshus et al. (2022) provides an overview of the relationship between the IT and OT domains, allowing us to filter the various elements into their respective category. Combined, these theories and models provide a structured, holistic, and domain-aware lens, enabling us to better understand and describe CSA in OT-SOC IR.

2.7.1 Situational Awareness of the Environment

We have selected Endsley's (1995) SA theory foundation of our theoretical lens (Figure 2.16). Among the reviewed literature on SA and CSA within the cybersecurity domain, we found Endsley's (1995) conceptualization to be the most widely used and well-established theory on SA (Table 2.5). Furthermore, Endsley's (1995, pp. 34–35) description of SA as a continuous decision- or information-support process from the perspective of a single person or operator aligns with our research intention of understanding the CSA process of a SOC operator during OT IR. We also find Endsley's (1995) conceptualization to be simple and easy to comprehend, as the process has been separated into three distinct phases: perception, comprehension, and projection. SA's first phase is perceiving or acquiring information about the environment (Figure 2.16 L1). The second phase concerns comprehension, not just being aware but also understanding the importance of the acquired information in relation to some goal (Figure 2.16 L2). The final phase applies the information and understanding (phases 1 and 2) of the environment to predict potential future outcomes (Figure 2.16 L3). Following the completion of one or more phases, a decision is made, and an action is executed to change the environment based on the current level of SA. The altered state of the environment is used as feedback, and the process repeats itself. Although, as Endsley's (1995) SA theory considers SA from the perspective of an individual operator, it won't be sufficient by itself in describing the processes required to obtain SA in cross-domain and multi-actor environments.

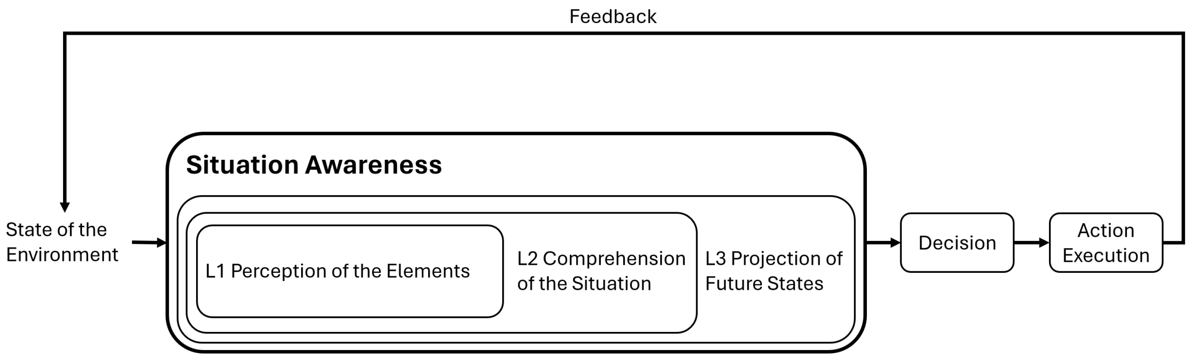

Feedback
Situation Awareness
State of the Environment
L1 Perception of the Elements
L2 Comprehension of the Situation
L3 Projection of Future States
Decision
Action Execution

Figure 2.16: Situation Awareness of the Environment (adapted from Endsley (1995))

2.7.2 Collective Intelligence Theory

There are numerous definitions of such an abstract concept as Collective Intelligence, depending on the context, domain, and the author describing it. From a generalized perspective, Malone et al. (2009, p. 2) explain CI as "*groups of individuals acting collectively in ways that seem intelligent*", while Hiltz & Turoff (1978, p. 44) define it as "*a collective decision capability [that is] at least as good as or better than any single member of the group.*". However, we find Levy's (1997, p. 13) conceptualization the best fit for our domain; he explains it as "*a form of universally distributed intelligence, constantly enhanced, coordinated in real-time, and resulting in the effective mobilization of skills.*". Additionally, the rationale provided by Wooley et al. (2015, p. 143) aids in clarifying our perspective and how we approach the concept, stating that "[CI] *includes a group's capability to collaborate and coordinate effectively, and this is often much more important to the group's performance than individual ability alone.*". Based on these conceptualizations and findings from the SLR, we identified three attributes that characterize CI in our domain.

In cross-domain and multi-actor environments, we consider CI an enabling factor for SA, which is facilitated by *Cognition*, *Cooperation*, and *Coordination* (Figure 2.17). *Cognition* is all forms of knowledge and awareness or the process of acquiring knowledge and understanding and plays a major role in the formation of CI (American Psychological Association, n.d.; Steyvers & Miller, 2015). This is essential as individuals or groups interact across domains and contexts, requiring them to obtain the knowledge necessary to understand and become aware of the environment they are interacting with. *Cooperation* is essential because actors on different hierarchical levels, domains, locations, and organizations must communicate and interact to share knowledge, experience, and information. Individuals or groups might possess one or more parts of the solution, such as general domain information or critical knowledge of some system, which, if shared, could contribute to resolving some situation, accentuating the importance of cooperation. Lastly, *Coordination* refers to synchronizing and aligning activities under conditions of task interdependence and uncertainty and is a key issue to solve for groups to work together effectively (Woolley et al., 2015). Both tacit and dynamic coordination can be facilitated through plans and routines, although "*dynamic situations often call for planning that occurs in real time*" (Woolley et al., 2015, p. 147).

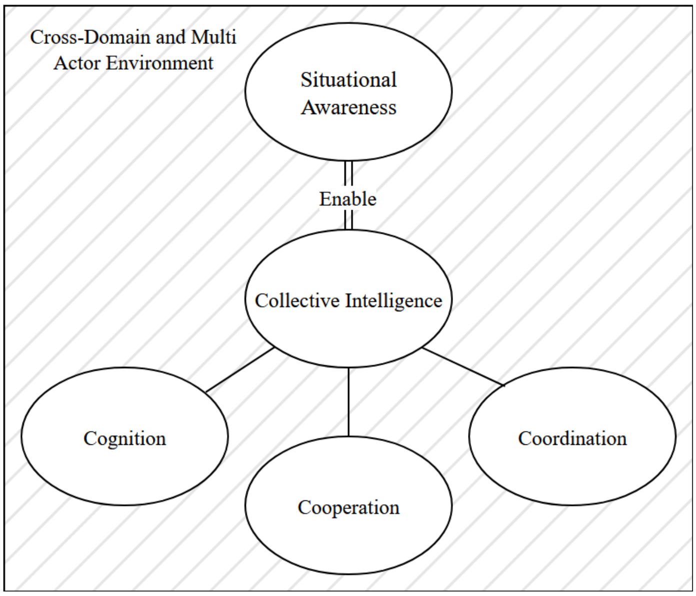


Figure 2.17: The Role of Collective Intelligence in Situational Awareness in Cross-Domain and Multi-Actor Environments

2.7.3 Situational Awareness in Incident Response

Ahmad et al. (2021) have developed and proposed a process model for SA in Cybersecurity IR (Figure 2.18) by studying the case of FinanceCentral's cybersecurity operations team. The model illustrates how "[. . .] *[SA] is implemented through processes that vertically and horizontally integrate stakeholders within IT and also across the broader enterprise*." (Ahmad et al., 2021, p. 9). Ahmad et al. (2021, p. 10) highlight three key components of the model: the stakeholders integral to the response process, process inputs (mental models, playbooks, business context, etc.), and process outputs (perception, comprehension, projection). Based on Endsley's (1995) SA theory, Ahmad et al. (2021, p. 10) model how SA is acquired during IR by illustrating task behavior (incident escalation and investigation) relative to the information processing behavior and flow between cybersecurity stakeholders. This gives us a holistic understanding of the stakeholders involved, how SA is developed during SOC IR in IT environments, and an example of the domain-specific application of Endsley's (1995) SA theory. Andreassen et al. (2023) applied this framework as a reference point to understand how security operations teams develop SA knowledge and adapt during enterprise detection & response. Their conceptual and final framework draws inspiration from Ahmad et al. (2021), in that they have extracted similar methods of depicting information process behavior, task behavior, and communication behavior. Although Andreassen et al. (2023) enrich and expand upon the process model proposed by Ahmad et al. (2021), presenting a framework based on relevant literature and informed by industry professionals.

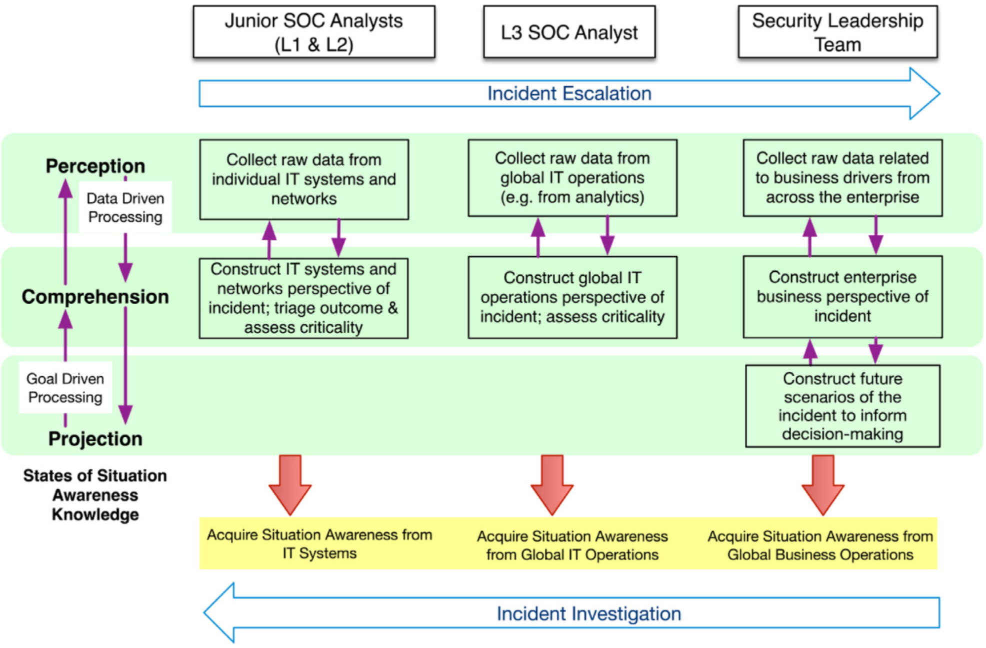

Junior SOC Analysts (L1 & L2)
L3 SOC Analyst
Security Leadership Team
Incident Escalation
Perception
Data Driven Processing
Comprehension
Goal Driven Processing
Projection
States of Situation Awareness Knowledge
Collect raw data from individual IT systems and networks
Collect raw data from global IT operations (e.g. from analytics)
Collect raw data related to business drivers from across the enterprise
Construct IT systems and networks perspective of incident; triage outcome & assess criticality
Construct global IT operations perspective of incident; assess criticality
Construct enterprise business perspective of incident
Construct future scenarios of the incident to inform decision-making
Acquire Situation Awareness from IT Systems
Acquire Situation Awareness from Global IT Operations
Acquire Situation Awareness from Global Business Operations
Incident Investigation

Figure 2.18: Situation-Awareness in Cybersecurity Incident Response (Ahmad et al., 2021, p. 10)

2.7.4 Domain Awareness

The Purdue reference architecture created by Williams (1994) "[. . .] *is a generalized network topology model for industrial facilities, and is often used as a reference architecture to organize systems and their interconnections*." (Onshus et al., 2022, p. 24). Even though Williams (1994) proposed the original framework, we found it to be too generalized and dated, instead deciding to use the version provided by Onshus et al. (2022, p. 25). Figure 2.19 provides a more recent perspective on the network topology in industrial facilities by, among other things, adding cloud to the model. This framework provides a compelling overview of the IT and OT domains, enabling us to categorize actors, entities, and processes into their respective domains. As such, we can better understand the who, what, why, and how involved in cross-domain interactions.

Mapping the SA process in multi-actor and cross-domain environments requires identifying and familiarizing ourselves with the elements that enable SA. First, we must understand who the stakeholders and actors are, who is cooperating, and who is communicating and sharing information. Second, we need to know what entities and systems are involved in the situation, the extent of the incident, and where the data comes from. Third, we must understand the reasoning and motivation behind why actors or entities interact. Lastly, we must understand how actors and entities interact and the processes underpinning SA. As such, the Purdue model (Figure 2.19) will act as a way of filtering and assigning these elements to their respective domain and clarify the processes that interconnect them across disciplines to facilitate CSA and shared SA.

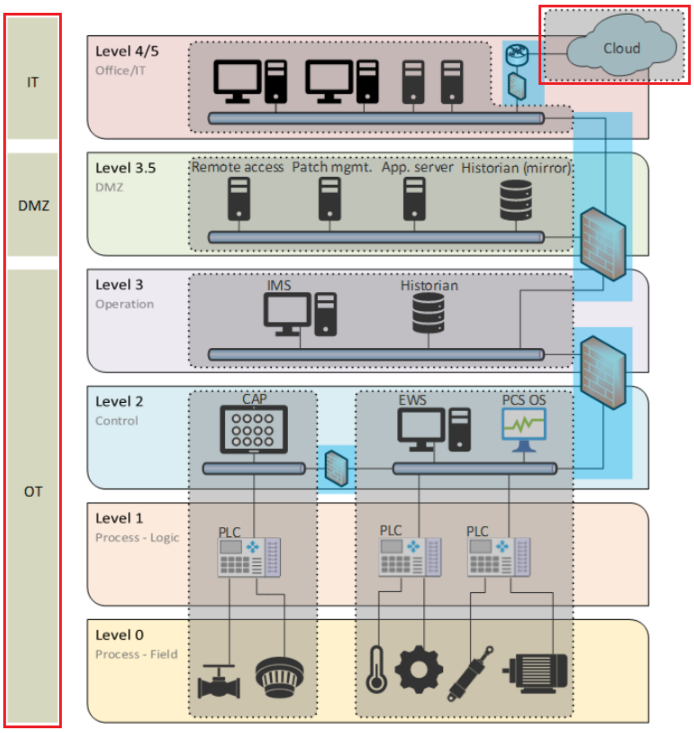


Figure 2.19: The Purdue Model: Example of Network Topology in an Industrial Facility (Onshus et al., 2022, p. 25)

Chapter 3

Research Approach

This chapter presents the chosen research approach, providing clarification and justification for our choice of methodology, research design, and methods for data collection and analysis. First, we provide an overview of the selected qualitative methodology and clarify the reasoning behind our choice. We then detail the research design and how this relates to the overall research approach. Thereafter, we address interviews as our data collection method and provide an overview of the study participants or unit of analysis. Lastly, our approach to data analysis is described before clarifying some of the limitations and ethical considerations of the selected approach.

3.1 Qualitative Methodology

This research aims to map and better understand how SOC operators establish and maintain CSA in a highly dynamic and multi-domain environment. As such, it is primarily concerned with uncovering the roles and responsibilities of the actors and entities involved, mapping information flows, and the processes and behaviors facilitating CSA during OT-SOC IR. Given the limited literature on the specific subject, the complexity of the issue, and context diversity, we find that the research issue calls for a qualitative approach. This is mainly because we are looking into a multi-faceted socio-technological phenomenon that is hard to quantify, requiring us to address the research issue through the perspectives of the interviewees. It is only through the opinions, interpretations, and experiences of the interviewees that we can gain the necessary insight and a sufficiently detailed understanding of the research problem. Therefore, to explore the research area through the perspective and understanding of the study participants, we have selected a qualitative approach to data collection and analysis.

Qualitative research is a broad term for research methods developed in the social sciences, which covers a wide range of techniques and philosophies that provide researchers with the means to study social and cultural phenomena (Hennink et al., 2020; Myers, 1997). "*Qualitative methods are typically used for providing an in-depth understanding of the research issues that embrace the perspectives of the study population and the context in which they live.*" (Hennink et al., 2020, p. 11). Consequently, this makes qualitative research "[. . .] *most suitable for addressing 'why' questions to explain and understand issues or 'how' questions that describe processes or behaviour.*" (Hennink et al., 2020, p. 11). By applying research methods such as interviews, we can examine and gain a detailed understanding of people's experiences (Hennink et al., 2020). This allows for the identification of issues from the perspective of the study participants, providing us with valuable insight and an understanding of their opinions and interpretations of aspects relating to the research problem (Hennink et al., 2020). Making qualitative research especially useful for exploring new topics or understanding complex issues, and the natural choice of methodology for this study (Hennink et al., 2020).

3.2 Research Design

Put simply, "*research design is a plan for collecting and analyzing evidence that will make it possible for the investigators to answer whatever questions he or she has posed*" (Ragin & Amoroso, 2019, p. 211). The design reflects the theoretical, methodological, and ethical considerations of what we seek to achieve and connects the empirical data to our research questions and conclusion (Flick, 2022; Yin, 2018). This affects multiple aspects of the study, from the details of data collection to the selection of techniques for data analysis and "*[control of] the influences that might bias the findings of [the] study*" (Flick, 2022, p. 3). As such, "*[t]he design's main purpose is to avoid the situation in which the evidence does not address the research questions.*" (Yin, 2018, p. 60). Furthermore, in qualitative research, there are several complexities, uncertainties, and ambiguities, such as researcher subjectivity, that are not easily considered when attempting to define the research procedure (Alvesson et al., 2022). Coinciding with Alevsson et al. (2022), we consider qualitative research design to be a reflexive and creative process, meaning that the design could be adapted based on the emergent conditions of the study along the way. Even though changes may occur, to provide structure, we have based the study on an interpretive-exploratory case study research design that we consider the best fit for our research problem and goal.

The aim of this study is to develop a holistic and accurate understanding of the phenomenon that is CSA in OT-SOC IR and describe it by expanding and creating an adaptation of the framework proposed by Andreassen et al. (2023) fitting the context of OT-SOC IR. We find the *case study* approach to be the most suitable research method for this study, considering that we are exploring and seek to explain a specific situation and its contextual intricacies. The case study approach is fitting in that it is a method that "[. . .] *study the particularity and complexity of a single case, coming to understand its activity within important circumstances*" (Stake, 1995, p. xi). Additionally, this approach is best suited for research where the researcher wants to understand a real-world case and assumes that this understanding is likely to involve important contextual conditions relevant to the case (Yin, 2018). As such, this method enables us to delimit the scope, allowing for a close focus on the chosen case to understand as much of it as possible (Tight, 2022). This facilitates an in-depth look at the case to identify dependencies and details essential to establishing and maintaining CSA in OT-SOC IR.

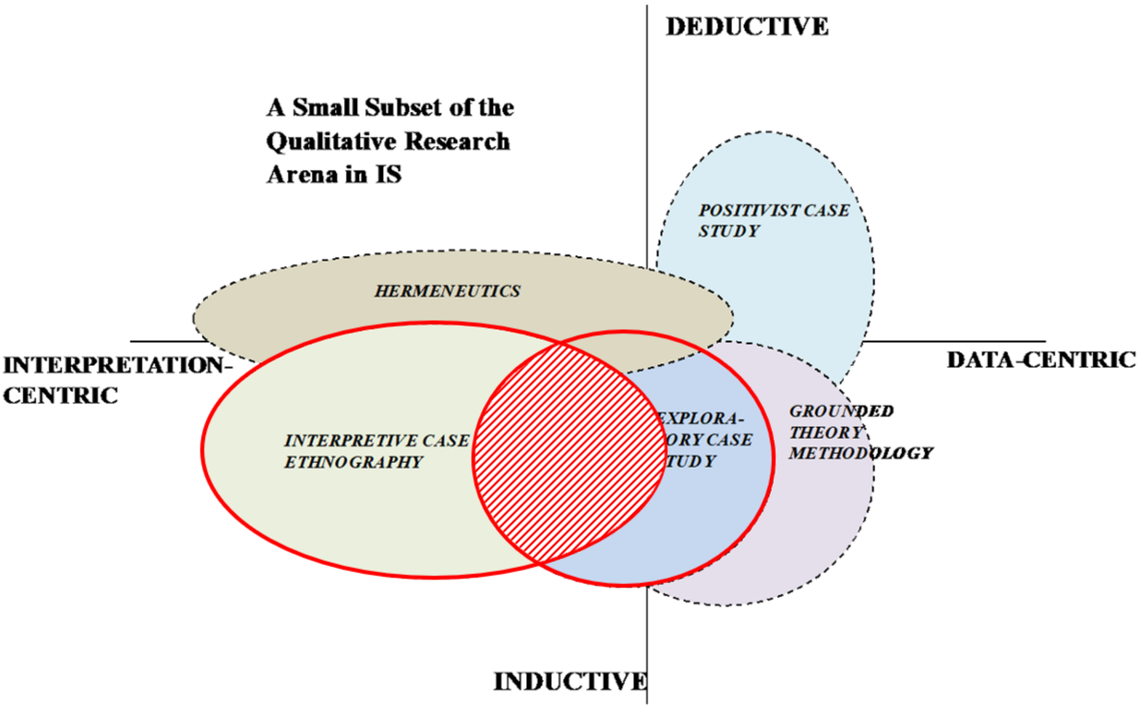

DEDUCTIVE
A Small Subset of the Qualitative Research Arena in IS
POSITIVIST CASE STUDY
HERMENEUTICS
INTERPRETATION-CENTRIC
DATA-CENTRIC
INTERPRETIVE CASE ETHNOGRAPHY
EXPLORATORY CASE STUDY
GROUNDED THEORY METHODOLOGY
INDUCTIVE

Figure 3.1: A Map of First-Generation Genres in Qualitative Research (Adapted from Sarker et al. (2018))

Currently, there are no standard templates or textbooks for case study design, making case studies rather flexible regarding epistemological orientation (Yin, 2018). However, based on the research problem and the study's goals with guidance from Sarker et al. (2018), we find that this study falls somewhere between interpretive and exploratory case studies (Figure 3.1). Therefore, we have adopted a combined interpretive-exploratory approach. Combining elements from both epistemological orientations is the solution we found to best support answering the research questions and creating a theory-informed and realistic picture of CSA in OT-SOC IR represented by the final framework (Sarker et al., 2018). Using the "*Four Elements of Qualitative Genres*" by Sarker et al. (2018, p. 758), we will elaborate and provide some clarity on what an interpretive-exploratory case study implies for our research design:

1. **Conception and Use of Data**: The study's data is gathered through a SLR and semi-structured interviews. The SLR data is regarded as facts, while the semi-structured interviews' data is a mix of what we regard as representative facts and the participants' subjective understanding and negotiated meanings (Sarker et al., 2018).

2. **The Nature and Role of Theory**: Theory is applied through a theoretical lens consisting of Endsley's (1995) theory of SA and Collective Intelligence theory (Malone & Bernstein, 2015; Woolley et al., 2015) and two supporting frameworks. This lens results from an SLR on relevant published and peer-reviewed academic publications and will be applied to inform and support the data collection and analysis process (Sarker et al., 2018). The purpose of the theory is to support the creation of a theory-informed narrative that answers the research questions.

3. **The Analysis Strategy Used**: This study utilizes explanation building to analyze the empirical data through a combined interpretive and deductive approach. First, the theoretical lens serves as the basis for creating categories to be used in a combined theoretical and open coding of the collected data. From the coded data, the theoretical lens and insights derived from the SLR will be applied to construct a theory-informed

narrative, building an explanation using empirical data guided by theory. Making the analysis interpretive in that we utilize theory to structure the analysis process and interpret and understand the data, and deductive in that we apply the theoretical lens to operationalize the analysis through pattern matching (Sarker et al., 2018). In doing so, we compare the empirically generated evidence with predicted patterns from theory to map and understand the phenomena we are studying (Sarker et al., 2018).

4. **The Nature of Claim about the Findings**: A common feature of exploratory and more data-centric interpretive case studies is that claims are often presented as a framework (Sarker et al., 2018). As such, the claims of this study will be that of novel insights as a framework that seeks to portray an accurate and plausible picture or interpretation of the CSA process in OT-SOC IR (Sarker et al., 2018).

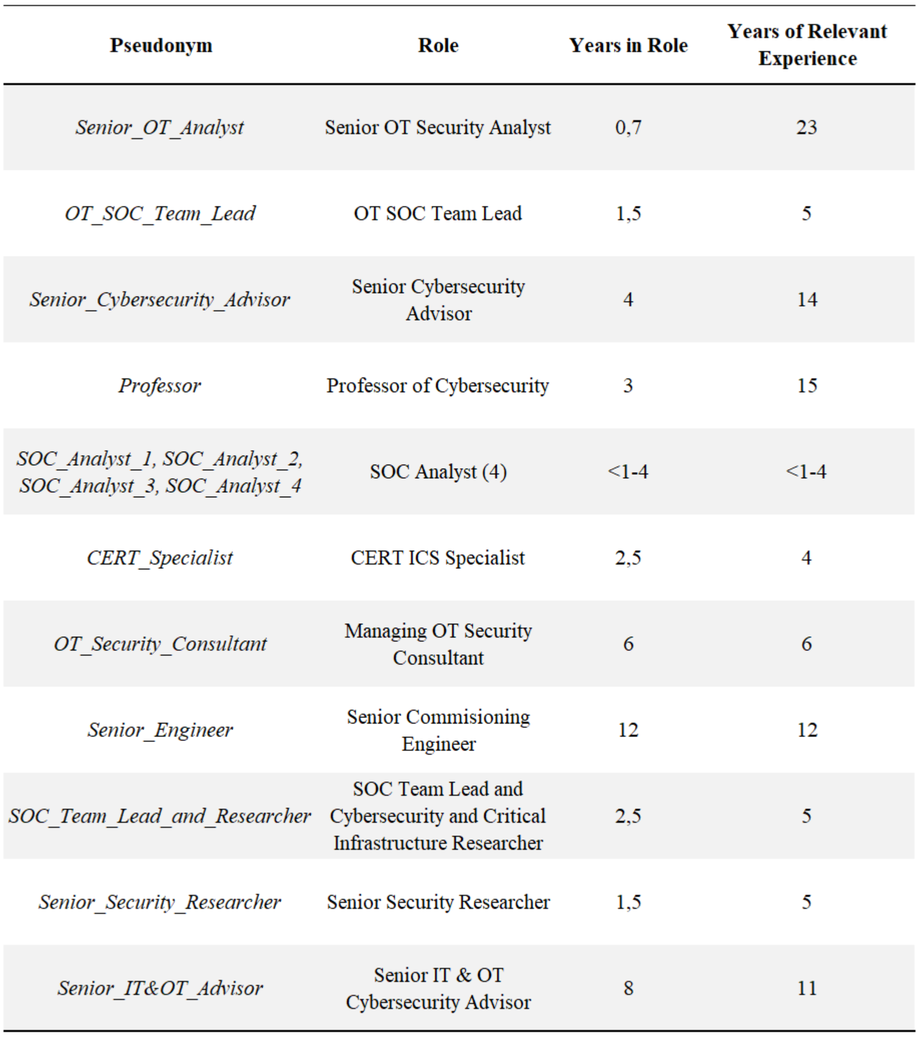
By adopting a combined interpretive exploratory case study approach, we seek to answer the research questions. As a result of the SLR, the theoretical lens guides both the creation of an interview guide and the subsequent deductive coding of the emerging data. After which, theory and empirical data are utilized in explanation building to create a theory-informed narrative, which serves as the basis for developing a conceptual framework describing CSA in OT-SOC IR. Having outlined the research design and methodological approach, the next section provides an overview and describes the process of data collection.

3.3 Data Collection

This section provides an overview of the study's data collection phase. First, we provide the rationale for selecting study participants and an overview of the selected participants. Thereafter, we briefly describe the selected method for data collection before detailing how it was executed. Lastly, using the summary provided by Myers & Newman (2007), we account for the challenges and pitfalls relating to the selected method of data collection and how we accommodated for those challenges and pitfalls.

3.3.1 Study Participants

Andreassen et al. (2023) developed the framework that we seek to expand upon by acquiring information and mapping the people, processes, and technologies of cybersecurity SOC-IR in the IT domain. As such, the framework (Figure 1.1) proposed by Andreassen et al. (2023) provides what we consider to be an accurate and representative overview of the IT side of the framework. Therefore, our task becomes to understand the OT domain and the intersection and pressure points between IT and OT and map the people, processes, and technologies relevant to OT-SOC IR. Initially, this study focused on SOCs, IT, and OT in the Norwegian context. However, due to issues in sourcing interview subjects, we broadened our scope to include European respondents and expanded the study accordingly to fit a global context. Consequently, when selecting informants, it was important that they had relevant experience and were qualified to provide information and knowledge pertinent to our case. To provide a rich and accurate representation of CSA in OT-SOC IR, we recruited individuals who hold relevant roles on different organizational decision-making levels and have a variety of backgrounds from multiple sectors applicable to the case. Due to OT's nature, we wanted to engage with engineering, academia, and OT cybersecurity experts to understand industry "best practices" and get the most thorough and nuanced answers. Hence, we have extracted knowledge from experienced individuals who physically commission and maintain, research, advise, secure, and monitor OT environments. This provided us with various perspectives that were useful for gaining a holistic and, at the same time, detailed understanding of the domain and the case, as well as its contextual intricacies. Participants include a senior OT security analyst, an OT SOC team lead, a senior commissioning engineer, a professor of cybersecurity, and four SOC analysts. Table 3.1 provides a complete overview of the informants, their roles, years in their current role, and years of experience relevant to the study.



Pseudonym	Role	Years in Role	Years of Relevant Experience
Senior_OT_Analyst	Senior OT Security Analyst	0,7	23
OT_SOC_Team_Lead	OT SOC Team Lead	1,5	5
Senior_Cybersecurity_Advisor	Senior Cybersecurity Advisor	4	14
Professor	Professor of Cybersecurity	3	15
SOC_Analyst_1, SOC_Analyst_2, SOC_Analyst_3, SOC_Analyst_4	SOC Analyst (4)	<1-4	<1-4
CERT_Specialist	CERT ICS Specialist	2,5	4
OT_Security_Consultant	Managing OT Security Consultant	6	6
Senior_Engineer	Senior Commisioning Engineer	12	12
SOC_Team_Lead_and_Researcher	SOC Team Lead and Cybersecurity and Critical Infrastructure Researcher	2,5	5
Senior_Security_Researcher	Senior Security Researcher	1,5	5
Senior_IT&OT_Advisor	Senior IT & OT Cybersecurity Advisor	8	11

Table 3.1: Subject Selection

3.3.2 Interviews

For this study, the chosen data collection method is qualitative semi-structured interviews. In qualitative research, interviews are the most common and one of the most important data-gathering tools and may be described as a conversation with a purpose (Hennink et al., 2020; Myers & Newman, 2007). This method of collecting data supports the exploratory nature of the study, aiding in providing explanations of the "hows" and "whys" relevant to the line of inquiry, as well as insights reflecting the informant's perspectives (Yin, 2018). This "*[permits] us to see that which is not ordinarily on view and examine that which is looked at but seldom seen.*" (Myers & Newman, 2007, p. 3). When conducting interviews, Yin (2018, p. 161) states that the interviewer has two main responsibilities: "*(a) following your own line of inquiry, as reflected by your [interview guide], and (b) verbalizing your actual (conversational) questions in an unbiased manner that serves the needs of your line of inquiry.*". The interview guide is an important part, serving as a memory aide and guiding the interview (Hennink et al., 2020). When conducting semi-structured interviews, the interview guide is often an incomplete script, supporting exploration by allowing the interviewer to improvise and follow up on topics or themes of relevance that arise during the interview (Myers & Newman, 2007).

Before conducting the interviews, we developed an interview guide that was carefully translated into Norwegian and English, containing the interview questions and important information about the interview, data privacy, and the informant's rights regarding the data (Appendix A). Guided by the research questions, we used the information and understanding acquired from the SLR to develop a series of questions for the preliminary interview guide. Subsequently, the initial questions underwent iterative pilot testing, reformulating any questions that seemed overly ambiguous and restructuring the line of questioning to ensure quality and relevance in the collected data. Corresponding to the nature of semi-structured interviews, the questions only serve as a guide and allow us to follow alternate lines of questioning into topics that emerge during the interview. Having constructed and ensured the quality of the questions, the translation of the interview guide, and the introduction detailing the informant's rights with regard to the General Data Protection Regulation (GDPR) and the Norwegian Personal Data Act, we submitted and received approval from SIKT on the interview approach and interview guide.

Every interview started with the participant being provided with information about the interview in their preferred language, how their data would be handled, their respective rights to the data provided, and that the interview would be recorded. This included statements on confidentiality and data anonymization, how the data would be used, and how the participants could contact us should they wish to view, alter, or withdraw their data (Hennink et al., 2020). While recording the interviews posed a series of privacy concerns that we needed to address, we considered the benefits far outweigh the added labor. Recording the interview allowed us to be more present by focusing on the conversation and following up on the participants' statements instead of note-taking. Additionally, this resulted in a more natural interview environment and engaging conversation between us and the participants. Furthermore, recording allows us to revisit and spend more time with the data to understand better and extract information that otherwise could have been forgotten or lost, facilitating more accurate and holistic data (Hennink et al., 2020). Before starting the interviews, we asked the participants if they had any questions regarding the introductory statement so that we could address any ambiguities or concerns before asking any questions. After that, we asked questions, adhering to the nature of semi-structured interviews, following the interview guide but pursuing emerging topics of interest.

3.3.3 Limitations of Interviews

While being a widely used and flexible method of collecting qualitative data, interviews pose a wide range of potential difficulties and pitfalls. Myers & Newman (2007) provides a summary of some of these pitfalls from which we have compiled a list of the problems that we had to account for:

- **Artificiality of the Interview** – Qualitative interviews involve interrogating someone who is a complete stranger and asking the informant to give or create opinions under time pressure (Myers & Newman, 2007).
- **Lack of Trust** – "*As the interviewer is a complete stranger, there is likely to be a concern on the part of the interviewee with regard to how much the interviewer can be trusted. This means that the interviewee may choose not to divulge information that he or she considers to be "sensitive". If this is potentially important information for the research, the data gathering remains incomplete.*" (Myers & Newman, 2007, p. 4).

- **Lack of Time** – "*The lack of time for the interview may mean that the data gathering is incomplete. However, it can also lead to the opposite problem– of subjects creating opinions under time pressure (when these opinions were never really held strongly to start with). In this case more data are gathered but the data gathered are not entirely reliable.*" (Myers & Newman, 2007, p. 4).
- **Constructing Knowledge** – "*Naive interviewers may think that they are like sponges, simply soaking up data that is already there. They may not realize that as well as gathering data, they are also actively constructing knowledge. In response to an interviewer, interviewees construct their stories– they are reflecting on issues that they may have never considered so explicitly before. Interviewees usually want to appear knowledgeable and rational, hence the need to construct a story that is logical and consistent.*" (Myers & Newman, 2007, p. 5).
- **Ambiguity of Language** – "*The meaning of our words is often ambiguous, and it is not always clear that subjects fully understand the questions.*" (Myers & Newman, 2007, p. 5).

Myers & Newman (2007) state that qualitative interviews are a powerful data-gathering technique when used to their full potential. They believe researchers utilizing qualitative interviews should be aware of potential problems and pitfalls and appreciate the technique's strengths and weaknesses (Myers & Newman, 2007). As a result of being aware, we could discuss and accommodate the challenges by adapting the interview guide and implementing various measures. Examples of such measures are the choice of recording the interview, providing information on how the data would be used and their rights relating to said data, simplifying the language of the questions, not asking for any sensitive information, and asking the informant if they have any questions before starting the interview. Additionally, our work in the cybersecurity field as SOC analysts helped us relate to the respondents and distill additional insights, which aided in reducing the impact of the limitations. However, we are aware that our experience and the implemented measures do not make the interviews a perfect process and that there might be discrepancies or unsolved challenges that we are unaware of. Nevertheless, the measures implemented due to being aware of the problems and pitfalls described by Myers & Newman (2007) significantly improved the quality of our data collection process and, consequently, the quality of the resulting data.

3.4 Data Analysis

After completing all the interviews and the data collection phase, we had 11 recordings of 14 respondents. These recordings were transcribed, translated, and anonymized to allow for coding and analysis using NVivo, a textual analysis tool that aids in organizing and structuring qualitative data. When translating the Norwegian interviews into English, we remained aware of translation bias and were cautious not to change the meaning of the data in any way. Therefore, both researchers checked and verified the final translated transcripts to ensure the quality and accuracy of the gathered data. Furthermore, before analyzing the interviews, a selection of codes or themes was derived from the theoretical lens and the SLR, including *cognition*, *cooperation*, *coordination*, and *people*, *processes*, and *technologies* for both IT and OT. These codes are aspects indicated by literature as facilitating factors for CSA in multi-actor and cross-domain environments. As the basis for the analysis, the transcribed interviews were analyzed by applying the theory-informed set of codes using NVivo, marking and allocating statements and themes into categories. For quality purposes and to ensure that the data was as complete as possible, both researchers coded and validated all interviews. Subsequently, we have applied explanation building to the resulting coded and categorized data. Explanation building is often presented in narrative form and seeks to "explain" a phenomenon by accounting for and describing the “hows” and “whys” of said phenomenon (Yin, 2018). As such, through a second analysis phase, we identified commonalities, differences, and overarching themes in the gathered data. Further structuring the coded data into six themes that explain how OT-SOC operators can establish and maintain CSA during IR. The findings section summarizes and presents the answers before the developed framework is presented, and the findings are discussed in relation to the theory in the discussion section.

3.5 Ethical Considerations

For this study, ethical considerations mainly relate to collecting data from a selection of informants. When collecting qualitative data, it is important to be aware of and take precautions to ensure that the data is handled with due regard to informant privacy and relevant legislation and guidelines. Informants are not obliged to take part in the interviews but participate on a voluntary basis. Accentuating the importance of handling the data with care, being transparent, and acquiring feedback and acceptance from the informant on how the data is gathered, stored, processed, and used. Prior to conducting the interviews, we developed an interview guide and general guidelines based on requirements and guidelines from SIKT, the GDPR, and the Norwegian Personal Data Act. The guidelines include avoiding asking for any personally identifiable information, the data only being accessible to the researchers, safe storage on the university’s preferred storage medium, deletion of all data upon project end, and providing all informants with information on how to access, alter, and delete their information. The final plan was submitted to and approved by SIKT, ensuring that we are in strict compliance with the guidelines governing open empirical research.

Chapter 4

Results

Following the interpretive-exploratory qualitative research method, we will present our results based on the semi-structured interviews. The findings form a theory-based narrative based on the theoretical lens on which this research is founded.

4.1 Findings

When analyzing the interviews, the data was categorized into themes and topics based on the coded nodes from the SLR. The analysis resulted in six topics; “Separate and Distinct domains”, “The State of the Environment and Data Collection”, “Actors Entities and Structure”, “Incident Preparation”, “Incident Response,” and “Post-Incident Activities.” With the categorized topics, we could start analyzing and comparing the outliers and commonalities of the interview data to guide the process in accordance with the interpretive-exploratory study, attempting to answer the RQs:

1. How does Operational Technology change Cyber Situational Awareness in SOC incident response?
2. How are people, processes, and technologies in MSSPs operationalized to provide Operational Technology Security-Operations-as-a-Service?

The following are the results of our findings from the interviews, starting with the distinction and separation of IT and OT.

4.1.1 Separate and Distinct Domains

From the SLR, we established that the literature clearly distinguishes between IT and OT, making it evident that these are separate but mutually dependent domains. The literature highlights multiple aspects and characteristics of the two categories of technologies, which the respondents also mentioned. An example of this is how the CIA triad changes and how safety becomes the determining factor when moving from IT to OT. When discussing the differing characteristics between IT and OT and how to deal with cybersecurity in OT environments, the *OT_ SOC_ Team_ Lead* stated:

> "*The CIA triangle, for example, is supposed to be reversed in OT. I'm not entirely sure that's true. It's just another way of seeing it, but everybody says it's in reverse in OT. No, it's just that you have the safety on top of everything.*"

Further establishing this point, the *Senior_ OT_ Analyst* also highlights the safety aspect of OT regarding the CIA triangle, saying:

> "*It's not CIA confidentiality, integrity, or availability. It's safety first, and that's why you need the visibility.*"

The *OT_SOC_Team_Lead* also highlights and backs up this claim, saying:

> "*The first aspect is safety. And then productivity, [availability] for the customer.*"

Adding to this point, the *SOC_Analyst_3* speaks from an IT perspective and highlights and acknowledges the core difference between the two domains, stating:

> "*[SOC analysts] essentially work on the basis of the CIA triad, but I think that in OT environments, it is much more important to ensure safety and reliability; that it runs as it should.*"

In accordance with the CIA triangle, OT is not just reversed; it does not quite fit the triangle. OT focuses on reliability and safety. Due to the nature of OT's environment being old and often unpatched, challenges arise in regards to cybersecurity, *OT_Security_Consultant* states:

> "[...] *in OT networks. A lot of machines are out of backup. A lot of unpatched machines. The risk for a company to get the OT infrastructure held as hostage is quite high.*"

As stated, reliability and safety are the core characteristics of OT, in contrast to IT, which focuses on the CIA. As such, due to the unpatched machines and lack of backups in the OT environment, *SOC_Team_Lead_And_Researcher* expresses concern about this, saying:

> "*These systems are not designed to be particularly resistant to these vulnerabilities. In other words, these systems only have vulnerabilities. They don't necessarily have any security mechanisms.*"

The OT systems and environment are not designed with cybersecurity in mind. The *Senior_Cybersecurity_Advisor* compounds this claim, addressing the issue of vulnerability and the general notion of cybersecurity of OT environments, stating:

> "*Many of these environments are not designed for cyber vulnerabilities as we see today, but the interconnection of networks and exposure that occurs is based on poor risk assessment.*"

With the lack of focus on cybersecurity in the OT environment, the impact of a cyber-attack could be disastrous. In OT environments, mechanisms exist to shut down processes and systems to ensure safety in the case of incidents. He continues, saying:

> "*Manipulating safety systems is in a way the worst thing a threat actor can do.*"

The OT environment is safety-critical. If an incident happens, it could lead to severe consequences. Reiterating and furthering this point, *Senior_OT_Analyst* highlights the notion of risk in the matter, stating:

> "[...] *things that are missing is a very clear, well-defined way of doing risk. Understanding the threats and risks is important because it's not likelihood; it's impact.*"

As previously stated, a lack of risk assessment of the OT environment is part of the design flaw, not focusing on cybersecurity. And when the notion is impact, not likelihood, it puts things in perspective. Additionally, OT systems and operations exist in the real world, with its physical systems doing work in real-time, as *CERT_Specialist* states, saying:

> "*Real-time is definitely an issue, speaking of OT environments. And which aspect that would not be as important in IT. Generally speaking, people have to be aware. That's the difference between IT and OT security. Because OT is going on in the real world.*"

With the distinction of the OT environment with its characteristics of safety and availability and IT's CIA triangle, the aspect of real-time is something the IT world must be aware of, as previously stated. Furthermore, IT's involvement in this environment will be covered later. However, the real-time aspect of OT systems affects IT applications as well, as *Senior_ Cybersecurity_ Advisor* explains:

> "*You see an increase in OT real-time export data from the OT environments and out to IT applications to further increase optimization or future smart maintenance.*"

The *CERT_ Specialist* highlights the distinction of the two domains, separating the aspect of security, stating:

> "*[A challenge] is also the understanding of something called IT and something called OT. What is the difference between them, and more specifically, what is the difference between IT security and OT security?*"

Combining safety, availability, and the real-time aspects of OT with the distinction of cybersecurity in the OT environment, IT applications being a part of this environment highlights some challenges. One of these challenges is knowledge and awareness. Applying cybersecurity in the OT domain, to be able to understand and know the OT systems a SOC monitors, is very important, as *Senior_ IT&OT_ Advisor* highlights:

> "*That [the SOC] has OT competence, I think. They have an understanding of how OT systems are different from IT systems. So if you're going to have a SOC for an OT system, you can't have a [MSSP] who has only delivered SOC services to an IT world without training [analysts] in the OT world.*"

Understanding and having knowledge of an OT environment is essential for a Security Operations Center and cybersecurity due to its distinct characteristics in contrast to IT. For this reason, having the perspective of each other's domain is very important. The *Senior_ Security_ Researcher* addresses this point by giving an example, saying:

> "*You've got people that have done an apprenticeship and then they've worked in a factory or in a power plant and then they've gone "Ohh well, rather than being promoted to like chief engineer or something, I'm gonna start going towards cybersecurity." And then you've got people who have been doing cybersecurity in IT who have gone: "Actually, I quite like the idea of OT." And neither of them really has any idea of what each other's actually doing, but they both have these weird priorities. What I would do is I'd specifically focus those groups together for as much cooperation as possible because that is the real weakness that we're currently seeing from a cultural perspective.*"

Having two different types of people across the two domains and not necessarily understanding each other is a problem. One thing is to understand the technological differences and distinctions and see the separation between IT and OT, but the cultural differences are there, too. As *OT_ SOC_ Team_ Lead* points out:

> "*Based on my experience, [OT] is more person-dependent than in IT.*"

Not only are the IT and OT systems and environments distinct and separate but there are cultural differences, too. IT may be more system-dependent than OT, so when a SOC is doing security monitoring of OT environments, the information that gets relayed across domains is dependent on the people relaying it to understand the domain language. *CERT_ Specialist* points out this challenge saying:

> "[...] *translate this information into understandable information. A lot of our Members are not IT educated; they are not in the IT field; they are technicians.*"

To summarize the findings concerning the distinction and separation of OT and IT, the respondents make it very clear that the CIA triangle clearly distinguishes between the two domains. OT and IT systems and environments are separate, not only for cybersecurity and safety reasons but also because of their cultural and domain distinctions. To understand the language of the domain and communicate that across, while having the knowledge and awareness of the two domains, they remain distinct in terms of their characteristics and perspectives on the importance of their operations. OT is focused on safety, availability, and real-time operations. At the same time, IT follows the characteristics of the CIA triangle, in which OT is not inverted, but safety is the most important aspect. This creates separation and distinction, as the two domains have different priorities and perspectives. From all the interviews, we get the impression that these points are commonalities across the interview subjects and paint a picture of the unique interconnectivity, yet how distinctly different IT and OT are. The separation yet parallel existence of IT and OT systems in the environment highlights the challenges, differences, and distinctions between them.

4.1.2 The State of the Environment and Data Collection

Even though IT and OT are separate and distinct domains, the reality is that the OT environment is composed of two different categories of technologies. With cybersecurity in mind, what does the OT environment look like, and how and from where is data collected in order to maintain SOC operations with its security monitoring? Both IT and OT technologies contribute to making up the environment and, by extension, data collection for the SOC, as mentioned. Therefore, the connectivity of the environment makes up for regular IT traffic within the environment as well, where *OT_SOC_Team_Lead* expresses the challenge of noise in the data collection of the environment, where IT is integrated, saying:

> "*We also have a lot of IT traffic in there, so that means that all that IT traffic or, as I was saying, guest Wi-Fi or general Wi-Fi that is used. The fact that Wi-Fi is used for other purposes, all that traffic is also SPAN'ed. So now you have the guy that goes into Facebook every morning; you also see that in your "OT" data. That's the noise.*"

The *Senior_OT_Security_Analyst* highlights this notion, adding to the argument that IT systems are part of the OT environment but not integrated into it, saying:

> "*Mostly, there won't be a lot of IT integration necessarily. My experiences with this is gonna be a lot of standalone systems, where IT integration has been plugged onto it.*"

As IT systems and applications are plugged onto the OT environment, what makes up the environment itself also consists of technologies that practically are the same, where *Senior_IT&OT_Advisor* states that, in essence, IT equipment is also OT equipment in how they function in the environment, saying:

> "*In practice, switches and routers in the OT world have exactly the same functionality as in the IT world.*"

Even though IT and OT equipment such as routers and switches are essentially the same, practically speaking, the environments themselves are far from the same or even similar. He later continues:

> "*For IT systems, it's often a bit of tailoring, OT systems are just tailoring. [...] You can say that "standard OT system" doesn't exist. You can talk about it in general terms, but everything is super specific. Because the process underneath is so specific.*"

As such, this highlights how the environments look like where the IT systems are separate yet plugged onto the OT environment by functioning practically the same as the IT equipment, as *Senior_IT&OT_Advisor* continues, stating:

> "*And that also applies to an OT server room. In the vast majority of cases, an OT server room is just a server room. So it's possible to distinguish between the two, and in an OT server room, there's nothing to say that you can't have some of the same monitoring as in an ordinary server room, for example.*"

When the SOC is doing security monitoring of the OT environment, with the combination of IT and OT data flowing in the network, in order to get the full understanding of the data that is collected from the OT systems, you need a point of contact in order to ascertain the situation, as *Senior_ OT_Analyst* states:

> "*You need to talk to the people who are responsible for the devices that you're actually looking at, so that would be the first thing to help them, to help you understand what kind of changes have been made, if any.*"

Due to the complexity of the environment, the SOC preferably has to get the information directly from the source. The people they have to talk to, who are responsible for the systems that they operate, are the process engineers. The *Professor* also highlights this point by addressing having a point of contact with the customer, saying:

> "*I'd made a list of friends at this company and process engineers so that I could call the person I thought could answer the question. And a SOC would be an assist to the [control center].*"

It is evident that cooperating and communicating with the customer is necessary to understand not only the environment and technology themselves but also the operations and processes that the SOC monitors. The *OT_SOC_ Team_Lead* points this out by highlighting how they are frequently communicating with their customers about this, saying:

> "*We have weekly meetings with the customer for incident review. That's what I meant by building the knowledge on the customer environment is that every week we call the customer for an hour or so, and then we say 'last week those were the events that we saw, that these were the most interesting'.*"

As he pointed out, building knowledge of the customer's OT environment is essential, and this can be achieved through communication and cooperation. This form of data collection is also achieved through alert tuning. The alerts and incidents that the SOC is dealing with on a daily basis need to be refined for the customer. Just as the *OT_SOC_ Team_Lead* pointed out, so does *Senior_ OT_Analyst*, saying:

> "*You have to tune it for every different industry and site. We have to do that with the outgoing traffic, but it's an order of magnitude harder with the internal traffic, just like if you were monitoring classic IT.*"

When the SOC monitors these environments, and as the two respondents highlight, to tune the alerts "for every site and industry," this form of data collection is one thing, but that implies a baseline of operations. The *OT_SOC_ Team_Lead* continues:

> "*Obviously, if it's targeting another device completely and this is something else, we need to re-ask, but what we provide to the customer is the assurance that we just need to know once because, after that, our knowledge base is being updated, our processes are being updated.*"

As part of the workflow of the SOC he describes, to update their knowledge database and processes of how alerts are handled, the *Senior_IT&OT_Advisor* adds to this, saying:

> "[...] *there's no reason why you shouldn't have the same monitoring there as you do in an IT environment, and in theory it should be easier because there should really be less information that changes in an OT environment.*"

Data collection and security monitoring of the OT environment from the SOC's perspective should be based on the baseline of the OT operations, in conjunction with the cooperation and input from the customers. As highlighted, this data coming from the processes themselves is static and should, in theory, be easier to monitor. However, to get to this point, *OT_Security_ Consultant* explains:

> "*The sensors collect traffic and send it to a central system like Guardian or Cyber Vision. The installation of such a [platform] doesn't mean a thing. [The SOC] first needs to see the information [from the environment], talk with the people involved who are working in the production lanes or in the cells, and verify the observed information, then there is a long process which is called 'baselining the system'.*"

Collecting this data from the sensors and feeding it into a central system is one thing, but in order to get context and understanding of the environment, he backs up the claim of having to converse with the customers. In addition to collecting said data, the question about the data itself becomes relevant. What data should the SOC get, how much data should it get, and from where? *Professor_ Cybersecurity_ Advisor* states:

> "*Monitoring equals data, so monitoring is about getting the right set of data from the right parts of the OT system. Not as much as possible, but the right dataset.*"

Having the right dataset collected from sensors of different parts of the OT environment and having frequent talks with the stakeholders to understand the context further are the next steps for the SOC to work with this data. To contextualize all that information can be taxing, and as *SOC_ Team_ Lead_ and_ Researcher* suggests having a "context broker", saying:

> "[...] *context brokers', and it's an encapsulation of that complexity, but it allows you to ask a context broker and get the condition there and then, and that means that you create an indicator. And when this happens in an OT system or IT, you can say, "That's it." But it's not "it" necessarily, right? But what happens then is that you often have to start backtracking, i.e., you're missing the rest of the context on that indicator. So this "context broker" that I'm talking about gives you that information right away.*"

For the SOC to have a context broker that is fed from the dataset collected, as to get the SOC analysts to increase their understanding and knowledge of the system, *Senior_ OT_ Analyst* points out a crucial point, stating:

> "*You need to understand your tool and tooling and you need to understand the customer, the operating system and it's a whole stack of things that you need to understand.*"

When all is said and done, the SOC analysts need to understand the tool that they are working with. When data is collected, contextualized in the context broker, and presented, the analysts have to understand what they are looking at. Additionally, *OT_SOC_Team_Lead* highlights this further, explaining how data from all the customer's sensors must abide by this contextualization, saying:

> "[...] *basically have customers that have installed an OT security solution that's being Nozomi Network, Cisco Cyber vision, this type of things. From there, we take the data that those products are generating and we parse them into common fields so that we can use global dashboarding.*"

Therefore, the context broker that encapsulates this complexity of data, as collected from the different OT security solutions, must be presented to the SOC analyst in such a way that it is understandable.

The respondents all point out how the OT environment has some form of IT integration, not in the systems and processes themselves, but plugged onto it for optimization purposes. The equipment in the environment may serve practically the same functions, as servers and switches are "the same". Even if that is the case, the OT environments themselves are vastly different across sites and industries, as the environments are often heavily tailored to specific processes. Additionally, respondents highlighted the importance of communication and cooperation with the customers when dealing with data and information collection, giving examples of how the SOC has frequent meetings and status reports to update its knowledge base. In addition, the respondents make it very clear that data that is collected from the different OT security solutions must provide a dataset from the environment that is contextualized, where giving examples of a "context broker." Lastly, the essence of the respondents' answers makes it very clear that documentation, communication, and cooperation are needed when dealing with data collection and understanding the environment. The SOC is dependent on the customer for this information, the more knowledge the SOC has of the customer's environment, the better they will be at protecting it.

4.1.3 Actors, Entities, and Structure

In addition to separating the IT and OT domains in terms of characteristics and technological differences, respondents also distinguish between the actors and entities within the two domains. Denoting the distinct, specialized, and context-dependent nature of OT through descriptions of roles and entities, organizational structure, processes, and other unique traits that set the domains apart. The *Senior_Cybersecurity_Advisor* mentions the need for specialized and OT-specific roles, stating:

> "*We wouldn't have an OT CISO, most have an IT CISO. On the OT side, you would have OT resources, either process engineers or purely OT maintenance resources who are skilled in the OT systems that they use in their processes.*"

The *Senior_OT_Analyst* adds to this, accentuating the specialized and knowledge-dependent nature of OT by expressing that external actors would struggle to understand the processes and intricacies of OT systems:

> "*I've just seen a few different industries [and] there's a lot of commonalities, but when you get lower into the [industrial processes], that's where all of the special sauce is, and that's where most IT security people and certainly anybody who hasn't worked in IT security gets lost because you have to be a process engineer.*"

This point is furthered by the *Senior_IT&OT_Advisor*. When addressing how the SOC can respond to a cyber incident affecting an OT environment, the *Senior_IT&OT_Advisor*

highlights the need for cooperation and coordination between the domains to establish shared SA, stating:

> "*Then it becomes hard to act on, you may need to pair process engineers or [someone with] process understanding with a SOC operator to correctly triage or select the right path ahead, "What is the smart thing to do here?". It's a situational image that you need to construct over time together with the SOC service.*"

With experience from working within an OT SOC, the *OT_SOC_Team_Lead* supports the need for cross-domain collaboration, specifically mentioning the SOC interacting with the CR:

> "*The thing is that the people we talked to from the Security Operation Center, we would be better off, in my opinion, talking to, as you said there, the control room and the operators.*"

Adding to this, the *Professor* talks about how a SOC they're familiar with operates when monitoring an OT environment. Describing how the SOC interacts and collaborates with the customer:

> "*The SOC in [Organization], which deals with security, they're not involved in operating anything. The only thing they're doing [during operations] is cooperating with the various environments to understand when they have discovered something, and then they collaborate with the environments to try to understand what has happened. Attempting to retrieve more information, attempting to ask, "What does this mean?", attempting to find the right expert.*"

When talking about who should be contacted when an unexpected event occurs, the *SOC_Team_Lead_and_Researcher* mentions field engineers and accentuates the importance of individuals who are physically present and have physical access to the OT environment:

> "[...] *field engineer. Those who understand and commission these systems. These are the guys [the SOC] should talk to. If you're in the CR and you have a signal you can't trust, you need to call someone who can step out and manually verify the pressure of a tank and read that it says such and such.*"

The *Senior_Security_Researcher* also brings up engineers, exemplifying how senior or principal engineers can provide specialized and important information about their environment:

> "[...] *a lead engineer or principal engineer, or whatever you'd call it, it would be some sort of like engineer that's in a senior position that is responsible for the actual day-to-day management or safety.*"

> "[...] *in [OT] environments where I've dealt with setting up SOCs and setting up instances like this, I've spent hours with the principal engineers of the environment going "OK what is this Mac address?" "What is this IP address?*"

Third parties, suppliers or OEMs, also play an important role when dealing with OT. The *SOC_Team_Lead_and_Researcher* specifies that the suppliers play a key role and are essential to acquiring knowledge about OT systems, especially in larger environments:

> "[...] *you're dependent on getting a hold of the person that knows the system. If you have multiple systems, you will be dependent on a third party, and that is likely a supplier. These suppliers are also a part of the puzzle. At some point, they begin to have a central role because it is often they who commission the systems and have the knowledge.*"

The *Senior_ Cybersecurity_ Advisor* also brings up OEMs as an important entity within OT, briefly mentioning their position in the industrial process and system information hierarchy in the Oil & Gas sector:

> "*In Oil & Gas, you would have the platform chief, then the OEM which is the on top in terms of processes out there.*"

In terms of roles, the *Senior_ Security_ Researcher* mentions how senior management has domain equivalents:

> "[...] *the equivalent in terms of the organization structure would probably be the Chief Information Security Officer, the Chief Technical Officer.*"

Later, when discussing the organizational decision-making structure and information flow during IR, the *Senior_ Security_ Researcher* provides some insight as to who is involved and who communicates with whom. Denoting the C-suite senior management and head of IR as strategic actors, the level 3 analyst and plant manager as tactical resources, and briefly mentioning actors physically present in the OT environment:

> "*Chief Safety Officer is more of a strategic position and plant manager is more of a tactical position. I would personally swap those because like security leadership team, you're going to have like CISO, and you're like head of incident response and you want them talking to the Chief Safety Officer. They would be talking at C-Suite board level and then the Level 3 analyst would probably be speaking to the plant manager. The person that's like actually on the plant floor that's doing.*"

On the same topic, the *SOC_ Team_ Lead_ and_ Researcher* gives an abstract description of the actors and hierarchy from the CR to the higher decision-making levels and emphasizes the importance of communicating across the various levels. The *SOC_ Team_ Lead_ and_ Researcher* also talks about how the potential impact of a disruptive event on OT requires senior management to step in and manage the situation:

> "*Regarding the operators, there is often a leader of that department or a section of the production, and then you often have a leader on top of that before there is another manager on some level. I believe that it is important to establish good communication between these levels. Then we're discussing the incident response part from the traditional IT approach, but on the OT side, I believe that there is a bit more chaos and, additionally, that there is an entirely different impact, so I kind of think that the top management needs to step in to make decisions.*"

In contrast to their own statement and the *SOC_ Team_ Lead_ and_ Researcher's* statement, the *Senior_ Security_ Researcher* argues that senior management or the C-Suite should not directly participate during IR:

> "*Generally, when someone's like a C-Suite level, like a chief- anything, they are so far removed from actual processes and actual understanding [of] what's going on that they're almost ineffective.*"

On a more general note, when discussing the general organizational structure during OT IR, the *Senior_ OT_ Analyst* find that the different decision-making levels aid in creating an understanding of how the different actors understand the business side of the operations:

> "*I like the idea that [the IT and OT side is] split up [into operational, tactical, and strategic levels] because there has to be somebody who has a higher level of understanding that understands the business side.*"

The *Professor* describes how the SOC should communicate with the OT organization, underlining that there should be a single initial point of contact that the SOC relies upon for sharing and receiving information:

> "*[The SOC] should contact whoever is responsible, often the shift leader. The person responsible in the customers [control room]. There is always one person in charge. The person on duty can make certain decisions, and it is always that person who calls others, so this would be the person [the SOC] would rely on* [...]"

This concept of the SOC having a single point of contact within the CR or in the OT organization that manages the information flow between other OT stakeholders, in general, is supported by the *OT_SOC_Team_Lead*, which states that:

> "*We have a guy who knows the guys inside the factory, so he is acting as a catching dispatch, and he is dispatching to the asset owners [at the end of the chain].*"

The *OT_SOC_Team_Lead* also adds:

> "*We send the customer a list for each service that we provide, and he needs to fill in who we need to contact per site.*"

Additionally, the *OT_SOC_Team_Lead* mentions that they utilize a ticketing system to communicate with the customers and make approval-based decisions. The *OT_SOC_Team_Lead* continues, emphasizing the importance of information sharing and communication with the customer to understand what is actually happening in their OT environment:

> "*This is where it becomes more important to talk to your customer because, quite frankly, on [the OT SOC's] side, until we actually have the answer from the customer, it just means nothing. It's just like we have a BACnet event.*"

On the topic of communication and information, the *OT_SOC_Team_Lead* also highlights documentation as a crucial part of the information flow and knowledge sharing:

> "*Something that is actually properly configured, documentation being available about the diagrams, these types of things so that we can know what we are actually looking at.*"

SOC_Analyst_2 adds to this, making it clear that due to the real-time and safety characteristics of OT, they feel a need to have playbooks or documentation on how to respond to certain events:

> "*It's protocols and routines. If probe X detects a 5 degree drop in temperature, then "this is supposed to happen," and we should respond "like this". In the same way, [the control room] has a large document stating what to do if "x occurs", I think we should have the same.*"

When asked who gets contacted or what the chain-of-command is in the event of a cyber incident in an OT environment, the *Senior_Security_Researcher* also highlights documentation and playbooks. The *Senior_Security_Researcher* lists a series of questions that need to be answered then, saying:

> "*All of these things would massively need to be considered, and it's something that you'd have in place. But I mean, it's basically consult the documentation, the playbooks at that point.*"

The *Senior_OT_Analyst* provides reasoning as to why there is a need for information sharing and cooperation between the different actors and entities in the IT and OT domains:

> "[...] *so the key thing is nowadays, of course, all of the OT is connected to IT because of, you know, if you're sharing data out, you have the predictive maintenance side, but that's relatively new. The OT process in itself, even though it's isolated, relies on inputs from IT and then sharing that OT process information up and out into the IT side of things.*"

The respondents commonly believe that different specialized actors in both domains need to collaborate and coordinate their efforts through information sharing. Specifically for OT, the respondents mention process, field, and principal engineers, CR operators, Original Equipment Manufacturers (OEM) or suppliers, the Chief Technical Officer (CTO), and the Chief Safety Officer (CSO) as key actors. Additionally, they provide examples of how collaboration and communication during IR could be structured, with a common opinion being that the SOC should utilize the CR as their single point of contact and source of information. Respondents also commonly agree that it is a good idea to separate the operational, tactical, and strategic levels and that there should be necessity-based communication between the actors on the different decision-making levels. Communication between the domains is essential for both sides to gain important knowledge, insight, and context when needed. Lastly, respondents highlight documentation as a key source of information and guidance, with brief mentions of calling or using ticketing systems.

4.1.4 Incident Preparation

Across all respondents, a shared conviction is that the preparation phase is the most important in enabling the SOC to become situationally aware when monitoring OT environments. With preparation, the respondents refer to everything prior to the SOC monitoring and responding to events and incidents. Holistically, this covers knowledge, understanding, awareness, and context, providing the SOC with the prerequisites necessary to establish and maintain CSA when working with OT environments. We have found four essential elements commonly mentioned by the respondents: documentation, communication, training, and baselining and alert conditioning. The *Senior_Engineer* gives an example, from experience, of why preparation is essential when someone from IT security is doing work in the OT domain:

> "*The external [IT security] company comes in. They don't understand the business. They don't understand the industry. They only understand cybersecurity, and it kind of never really works as well as it should.*"

By illustrating how a computer can be a critical asset in OT, the *SOC_Team_Lead_and_Researcher* exemplifies how the context of a device can change depending on the environment in which it operates. What could be considered a non-essential device in IT requires different knowledge, understanding, and perspective when dealing with it in the context of OT:

> "*Those systems require an entirely different approach, that in itself contributes to constructing a certain understanding, in that you need to bring that perspective. [...] It's about competence, understanding, and "Yes, it's actually a computer". It's just that [the computer] has a central and critical role, then you probably wouldn't respond because you're not always supposed to.*"

The *Senior_Security_Researcher* also mentions the need for context switching when dealing with OT. Explaining that the SOC needs to assess issues from more than one perspective to understand the implications of an event fully:

> "*So, you'd want to know exactly what that is doing, and you'd also want something that is outside of this single pane of glass, kind of SOC instance to know what the*

> *context of that is in an engineering capacity, is it something that's being targeted that is really not a big problem in the OT environment?"*

SOC_Analyst_4 brings understanding and knowledge into the context of SA from the perspective of a SOC analyst. When discussing OT and SA in SOCs, *SOC_Analyst_4* provides a good description of SA, accentuating understanding and that knowledge has an impact on analysis and response:

> "*[SA] is the degree of understanding you have for a situation you have encountered. The knowledge you have to be able to analyze the situation and possibly what the consequences of the situation might be if you handle it like this or like that.*"

The need for sufficient knowledge and understanding of what you are monitoring is made clear by *SOC_Analyst_2*, which states:

> "*As a security analyst, what are you really looking at? What is it? What device is named XABC? What does this device do? I think that this is important to understand.*"

Adding to this is the *OT_SOC_Lead*, describing briefly how knowledge affects OT SOC operations, stating:

> "*The more you know about a customer's environment, the easier it is to protect because the faster you can be at protecting it.*"

Documentation was the most prevalent method or source of knowledge and context mentioned by the respondents throughout the interviews. Respondents regularly talked about documentation as a source for various types of information. *SOC_Analyst_3* explains how asset or network documentation facilitates understanding and can act as important assurance for multiple stakeholders. *SOC_Analyst_3* describes a scenario that clarifies the role of documentation in terms of context and customer environment insight:

> "*I think that it's very important for the person responsible for the customer and the customer that the SOC is provided with a mapped network to understand what we are monitoring so that we don't receive a random alert for company X where it says "ICS write" and we have no idea what it's writing to, right? We don't have any documentation on this.*"

The *Senior_OT_Analyst* also specifically mentions asset knowledge:

> "*[The SOC] need[s] to know a lot about the assets and the connected assets.*"

The *OT_SOC_Lead* also brings up a list or documentation as the source information on who to contact when the SOC needs additional information:

> "*We also have a very important contact list of the guys that we know at the customer.*"

Why documenting a list of OT personnel to contact is important is highlighted by the *Senior_Security_Researcher*, which makes it clear that it can be difficult to locate the right person or the necessary expertise on an ad-hoc basis:

> "*The one thing that I find really annoying about any OT organization is that no one has any idea on how to manage the structure of the organization, the security staff? Every time I've gone into an organization, it's like, OK, who's reporting to what? Like, who's got responsibility for this kind of thing?*"

Furthermore, by posing a series of questions, the *Senior_IT&OT_Advisor* outlines how documentation can provide valuable and timely knowledge on how to respond and what to do when an unexpected event occurs:

> "*[The SOC and the CR] need [information on] more like: How do we handle it? Do we need more help? Who should be involved? Have we notified those whom we should notify? What are the possible consequences? More of this. Should we be on general alert, or do we manage this within regular office hours? Should the entirety of the company be on general alert, like, what are we supposed to do?*"

The *Professor* highlights why preparation and established procedures are an essential element during an incident or emergency in terms of the human aspect:

> "*The human mind can't handle [the stress of an emergency over an extended period of time], so that's why [the CR] have procedures detailing how to share the right amount of information to enable other [CR operators] to "hit the ground running.*"

Preparing the SOC in terms of collaboration and communication is another theme that respondents address. The *Senior_IT&OT_Advisor* provides a good example of why there is a need for prepared and established processes for collaboration and communication, stating:

> "[...] *it is not a given that the SOC has decision-making authority to influence what the CR does anyway; it would likely be another person who is responsible for the operations that would make that decision.*"

The *SOC_Lead_and_Reseracher* furthers the *Senior_IT&OT_Advisor's* line of reasoning:

> "*There is often someone who is an expert in these systems or has more experience that you need to know. It takes time to find this in an organization. It's not guaranteed. Additionally, it is often that person that reaches out to suppliers.*"

Establishing procedures for when and who to contact is already a common practice in OT organizations as indicated by the *CERT_Specialist*:

> "*Most of [the CR operators] would basically call for help. But they are aware that they need to call for help, that they cannot help themselves. So, this is the procedure, to call for help.*"

Understanding how to communicate is especially important due to the difference in domains and priorities, as stated by the *OT_Security_Consultant*:

> "*[IT and OT people] don't even speak the same language, and they do not trust each other. Because OT has another focus.*"

The *CERT_Specialist* provides some clarification, noting that IT actors need to understand and adapt how they communicate when speaking to OT actors, explaining:

> "[...] *translate [IT] information into understandable information. A lot of our members are not IT educated, they are not in the IT field, they are technicians.*"

Respondents indicate that the understanding of how to communicate and some level of domain insight is not solely based on resources and documentation, but also on training. From the OT perspective, the *Senior_Engineer* explains what prerequisites the SOC should have:

> "*I would like [the SOC] to understand what it is they're monitoring and understand how the business works, how it's designed, but not the proprietary information, just the process that it goes through.*"

Adding to this, the *Senior_IT&OT_Advisor* explains how training provides insight mentioned by the *Senior_Engineer*. Specifying that training is required to gain the domain understanding needed to monitor OT environments:

> "*Some training is necessary to be able to work with monitoring of OT environments in a good way. But I don't think it's impossible [for the SOC to monitor and respond to cyber incidents in OT environments]. It's not a big deal if you have good training, but you can't do it without the domain understanding, because then you'll just do it wrong.*"

The *Senior_IT&OT_Advisor* accentuates the importance of training on domain knowledge and understanding later in the interview, stating:

> "*What [the SOC] have to do is obviously train in the domain part and [gain an] understanding of the consequences of the events that can happen [in OT environments]. I think that part is very challenging. Very few people have that OT knowledge, regardless of whether they have the security understanding for it or not.*"

With experience from working and managing an OT SOC, the *OT_SOC_Team_Lead* is clear in that training is necessary for the SOC to know what they are doing, stating what analysts need training in:

> "[...] *the easy answer is the training. First of all, the training in the technology that we use, [how to respond to] events, but also the training in the customer environments.*"

However, the *Professor* makes the case that it isn't possible to train for every type of OT environment, saying:

> "*It's difficult for a SOC because [the analyst] can't learn, or [an analyst] can't become a process engineer in all the sectors that [the analysts] are supposed to deliver [services] to.*"

The final sub-theme on the topic of preparing the SOC is baselining the environment and alert conditioning. This was a recurring and important theme among the respondents, why this is important was concisely explained by the *Senior_Security_Researcher*:

> "*In an OT context, situational awareness, especially the first stage, is knowing what you've got and having visibility of what's going on.*"

While this may seem very similar to IT environments, the *SOC_Team_Lead_and_Researcher* offers clarification of the different domain alert perspectives and why baselining and alert conditioning is vital when monitoring OT environments:

> "*If you're sitting in an IT SOC, you should expect [to receive alerts]. But those sitting on the other side [in the CR] don't. And then I'm afraid that there will be too many false positives, which can implicate the OT environment. [...] you're afraid that noise from the IT environment can influence decisions made in the OT environment*"

This sentiment is supported by the *Senior_Cybersecurity_Advisor*, which specifies why baselining and alert conditioning is important, stating:

> "[...] *it's important that [the SOC] has an understanding of how to distinguish normal process operations from anomalies, that is, events that they don't want in the systems. Distinguish false positives from actual events.*"

When discussing what requirements the *Senior_IT&OT_Advisor* would set for a SOC that was going to monitor an OT environment, conditioning or tuning of data or alerts was highlighted:

> "*The most important requirement I would pose is that [the SOC] must tune and set up the logs in close collaboration with those who have domain knowledge of the OT system.*"

The *OT_SOC_Lead* offers some perspective on how baselining and alert conditioning affects OT-SOC operations, explaining:

> "*When everything is properly implemented, monitoring is quite easy, to be honest. It's just like "this never happened before, is it normal?". Yes or no, that's more or less your monitoring, but it takes a while to get there.*"

Respondents unanimously indicate that the preparation phase is the most crucial stage in facilitating CSA for SOC analysts and success in providing OT security services. While data may flow into the SOC's SIEM tools, a lack of the proper knowledge, understanding, contextualization, and awareness leaves analysts unable to monitor and respond to OT incidents correctly. The respondents are aware and make it evident that SOC analysts most often belong to cybersecurity in the IT domain and rarely have any relevant OT experience. Therefore, they state that SOC analysts must be provided with the prerequisites and insight necessary to comprehend the intricacies of the OT domain and customer environments. As stated by the respondents preparation includes four main elements: documentation, communication, training, and baselining and alert conditioning. Documentation is about providing analysts with a knowledge base that is accessible on demand and should include essential information such as system, network, and asset mappings, contact lists, and response and information-sharing processes and procedures. Communication is about knowing when and how to communicate with OT actors and speaking the domain language to facilitate trust and understanding. Respondents also bring up training as an essential aspect; training gives analysts knowledge, understanding, context, and awareness by providing training covering the OT domain, the technologies they use, how to respond, and customer environments. Furthermore, for OT SOC analysts to correctly monitor and react to events, they require a baseline of what is expected in a customer's environment and conditioned alerts to be able to distinguish between normal operations and anomalous conditions.

4.1.5 Incident Response

The respondents' answers indicate that their current role and background impact how they would approach and think of cyber-IR in OT environments. However, they propose similar ideas regarding the role of the SOC, MSSPs, and the OT asset owner during IR. Additionally, they provide descriptions of the various stages of the IR process, which clarify the role of the SOC in establishing shared SA and how the SOC acquires CSA. The first thing that happens is that the SOC receives an alert. The *OT_Security_Consultant* provides an example of how the SOC receives and confirms the information that they observe from the environment:

> "*The sensors collect traffic and send it to a central system like Guardian or Cyber Vision. The installation of such a [platform] doesn't mean a thing. [The SOC] first needs to see the information [from the environment], talk with the people involved who are working in the production lanes or in the cells, and verify the observed information* [...]"

Most respondents make it clear that when the SOC receives an alert, it can result in one of two possible outcomes. Either the event is benign and is whitelisted and added to the knowledge base, or the procedures for handling incidents are followed. The *OT_SOC_Team_Lead* describes how their OT-SOC approaches alerts:

> "*At the end of the day, that will be event management. It results in one of two different scenarios. It's either, yes, that's OK; put it into the whitelist, or it's an actual alert, and then we follow incident management.*"

Additionally, the *OT_SOC_Team_Lead* explain that their immediate response to an alert is never to perform actions that might directly interfere with the operational environment:

> "*We know everything is malicious; as the MSSP, we will never block [an event] right away because of our SA and OT understanding of the customer's environment [lets us know] that if it's blocked, something might actually stop working in the customer's [environment] right away.*"

IR in OT environments is in many ways similar to IR activities in other domains. However, it is more a question of having the knowledge required to understand the environment and implications of the incident as pointed out by the *Senior_IT&OT_Advisor*:

> "*[IR] always involves the same concepts and activities. [In OT], it's more about the competence that needs to be applied.*"

Additionally, in OT environments, input from various sources and different knowledge needs to be applied to verify that an adverse event has or is occurring. These systems exist and operate in the physical realm, as such, the most reliable source of information is to check the physical status of the environment, which is made clear by the *CERT_Specialist*:

> "*Alarms are just indicators that we have to dig down into in some way or another. We need to have evidence from the real world by actually going down [into the environment].*"

As such, the SOC is dependent on external expertise and verification of the physical attributes of the affected systems to gain the necessary CSA to accurately triage an incident in collaboration with on-site experts. The *Senior_Cybersecurity_Advisor* states that this is the case:

> "*It's important for the [SOC] operator to gain more knowledge of the incident and consider triaging if it is an emergency, or if it is something that you have to call process engineers or others to support and increase [SA].*"

Therefore, during IR, the CR should dedicate resources to cooperate and coordinate their efforts with the SOC to verify the occurrence and impact of a cyber incident on the OT environment as stated by the *SOC_Team_Lead_and_Researcher*:

> "*[The CR] is still supposed to function as a [CR] and operate, so [the SOC] can't necessarily disrupt that. [The SOC] always needs to consider that they need to do their job, but [the SOC] needs to have some part of [the CR's capacity], maybe 50%, to get some initial information about the condition of the systems and status and all that. This helps in establishing [SA].*"

With the continuous flow of incident-related information between the SOC and the CR, both entities often have a representative who receives information, interprets it, and shares need-to-know information with relevant stakeholders. The *Senior_OT_Analyst* specifically mention team leaders, stating:

> "*When you do [IR], and you're the team leader, because you're in between management and the technicians who are actually helping, your role is to sit in the middle and first understand and interpret all of the information and the actual situation on the ground.*"

Furthermore, IR in OT environments is dependent not only on actors from multiple pillars across the MSSP and the organization that owns the OT systems but also on third parties. The *SOC_ Team_ Lead_ and_ Researcher* gives an impression of how complex IR can be in terms of stakeholder involvement, stating:

> "*We need to have a well-established channel of response towards suppliers. There might be multiple suppliers in the same system, and you need IT to investigate what has happened. They can operate autonomously on their own and start to map what has happened, and then you need to activate all the other actors and roles that are needed.*"

Due to the domain difference and the presumed gap in domain-specific knowledge and context awareness, respondents make it clear that the SOC's role is mainly to provide advice and support the OT organization during IR. The *Professor* explains:

> "[...] *give the customer in that situation, if you're a SOC, actionable advice. Because [the SOC] is not in engineering mode in OT yet, [the SOC] is more in a place where they receive advice and communicate with the customer, and then you help the customer to carry out said advice.*"

The *Senior_ Cybersecurity_ Advisor* aids in clarifying the role of the SOC in OT IR:

> "*A SOC service can contribute to enriching the situational picture and the changes that could have happened, providing decision support and making decisions simpler for those in crisis and preparedness in the management.*"

The SOC's job is to monitor, detect, and share need-to-know information with the CR and the cyber-IR team to enable them to do their job correctly. All entities and actors should share the information necessary for them to complete their tasks, requiring the CR to share information with the SOC such that they can establish and maintain CSA. The *Senior_ Engineer* exemplifies how information sharing should work during OT IR, stating:

> "*If you're asking me what should be shared, it should be enough information that the people that are investigating it can do their job. So, if it's a breach that causes an incident from a functional point of view, then the functional people should have enough information to go about their job and get the plant back and running. And then the other people that need to investigate the other parts of the breach may get their sort of information. So, it's kind of a need-to-know basis* [...]"

Respondents often state that incidents in OT environments have a bigger impact on the organizations in which they happen and are more demanding than incidents that only impact IT. They also require another type of response and knowledge, which highlights why the SOC acts as a supporting actor in what is a comprehensive multi-actor response effort. The *Senior_ IT&OT_ Advisor* clarifies:

> "*A difference between IT and OT is that all of OT is much closer to the business side and the core business activities. If there is an incident in the OT environment, it is very rarely only a cybersecurity incident.*"

> "[...] *if it's [an incident] within the OT world, then it's often resorting to the contingency plan, which often goes beyond cybersecurity and into regular incident management.*"

While some respondents have made it clear that OT is both embedded with and, to a certain degree, dependent on IT, they also make it clear that IT and OT are separate domains that require different approaches to cyber-IR. The *Professor* illustrates this by describing what a response from the CR could look like in the event of a malicious cyber event:

> "*Often resorting to what's stated in [IEC] 62443, like going into Island Mode. You need to set up your network in such a way that you can cut the umbilical cord that's connected to the firewall.*"

The interviews show that the SOC retains a less active supporting role in OT IR than in a similar situation within the IT domain. Respondents often refer to domain knowledge, environment context, and the close relationship between OT and core business processes as reasons why the SOC retains a support and information-sharing role. The main objective of the SOC is to facilitate team SA among actors by sharing events and need-to-know information with the CR and other relevant stakeholders. Additionally, respondents indicate that IR and information-sharing are initially triggered by the SOC receiving an alert or the CR observing some operational anomaly. When the SOC gets an alert, the CR applies its domain knowledge and insight into the OT environment to provide operational context. The CR can also prompt on-site personnel or process engineers to physically assess and verify what they cannot. Hence, CSA in the SOC depends on the CR and on-site personnel providing domain and environment-specific insight. As such, the SOC and the CR complement and aid each other in filling the knowledge gaps that result from separate domains, specializations, and priorities. Furthermore, due to the complexity and diversity of OT environments, respondents also bring up suppliers as essential actors during OT IR. Successful IR in OT environments depends on close collaboration and coordination of actors from multiple domains and organizations. While the domains may be tightly integrated, during IR, if unable to bring the OT environment into a safe state, operators may resort to disconnecting and separating the enterprise and operational networks or perform a shutdown.

4.1.6 Post-Incident Activities

As the incident and situation have been handled by the IR team and CR on both domains, the post-incident activities will take effect. The post-incident activities themselves can vary depending on the incident, but as respondents have previously stated, if a cyber-incident occurs in an OT environment, it can also affect the physical domain. As such, there are two angles to what happens post-incident, from the OT perspective and the SOC. The *OT_SOC_Team_Lead* goes on to describe their OT SOC's workflow on how they handle the post alert/incident, briefly saying:

> "[...] *when we know that context, next time if the context is the same, we know what to do with it.*"

When doing incident management in their OT SOC, the *OT_SOC_Team_Lead* highlights the importance of documentation after an alert and incident. Their workflow is centered around experience and documentation-based knowledge. When an alert triggers that are familiar or recognizable, they know what to do with it. If not, he continues:

> "*So that next time we see that [alert or activity], we learn, we build it into our knowledge base, and next time we see that we know how to act quickly.*"

This is related to incident management and handling alerts in the SOC on a daily basis. However, the essence of incident management and post-incident activities relies on the same notion of documentation and learning, building your knowledge base of the environment. When an incident occurs, the SOC automatically or quickly handles or escalates it. If it then goes through the entire incident cycle and reaches the post-incident activity, the *OT_SOC_Team_Lead* later adds and continues saying:

> "[...] *we go back into the cycle of; now we know, now we update the knowledge, as we will know for the next time.*"

On the OT side, the *Senior_ Engineer* explains how, from a field engineer perspective, when an OT organization has an incident in their environment, what are the steps after the incident? He highlights the importance of awareness and training for the people involved, stating:

> "[...] *what do they [organization] do afterwards? Do they learn from the breach and then realize that they put all these steps in place? It's not just about making it as secure as possible after that. It's then looking at what happened and then seeing if the [employees/engineers] were aware of what was going on. If not, do they need more training? Do they need more technical supervisors instead of administrative supervisors? So again, it would depend on what the breach was and how severe it was.*"

The difference in post-incident activities between the two domains is that the OT world deals with physical environments and systems. As such, OT personnel need training and understanding incidents on a different level than a SOC. The OT SOC will frequently discuss the customer's environment and incidents, constantly documenting and updating the information so that they know what to do in every given situation.

In our findings, experienced respondents highlight the various challenges and intricacies of OT-SOC IR and provide essential insight to understand how MSSPs could be operationalized and how the SOC can establish and maintain CSA during OT IR. In accordance with the literature, respondents separate IT and OT, highlighting safety, real-time, and contrasting views of the CIA triad as fundamental differences. However, their statements also make it clear that even though the domains may be separate, they are highly interconnected and mutually dependent on each other. This becomes increasingly apparent when the respondents describe OT environments and how data can be collected about and how to understand the state of the environment. Additionally, separated by domain knowledge, priorities, and environment-specific insight, the respondents differentiate entities and actors in the IT and OT domains, describing a complex and person-dependent OT environment with response and reporting structures that vary depending on the sector and environment. Furthermore, as the foundation that facilitates effective OT-SOC IR and CSA, pre-incident activities or IM is accentuated by the respondents as the most crucial stage. In IR, respondents highlight the importance of cooperation and coordination through continuous communication and information-sharing so that both sides can fully comprehend the situation. Post-incident, respondents state that both the IT and OT sides need to learn and update their knowledge based on the event, using insight to get a shared understanding of the situation and create awareness of similar future scenarios. In the following chapter, we utilize the findings derived from the interviews with various domain experts and present our insights as a framework for CSA in OT-SOC IR.

Chapter 5

Discussion and Summary of Findings

This thesis aims to examine how the SOC provides security services to owners and maintainers of OT environments. By investigating OT cybersecurity and IR, CSA, and the SOC, we seek to expand upon the SA framework for SOC IR (Figure 1.1) presented by Andreassen et al. (2023) to visualize how SOC analysts obtain CSA of events that occur in the physical world. Thereby mapping and creating an understanding of how MSSPs are operationalized to provide OT security operations as a service and how the SOC can acquire and maintain CSA when OT environments are incorporated into its operations.

By applying a deductive exploratory approach supported by interpretive elements, we have constructed a theoretical lens that has been used to create a theory-informed narrative through explanation-building. This resulted in developing an understanding and the subsequent expansion of the SA in SOC IR framework by Andreassen et al. (2023) into a conceptual multi-domain CSA framework for OT-SOC IR. In the following section, we present and explain the framework, discuss the findings, and answer our research questions.

5.1 A Dynamic Framework For Cyber Situational Awareness in OT-SOC Incident Response

Using theory and empirical data, we have expanded upon and adapted the work of Andreassen et al. (2023) and constructed a conceptual framework modeling CSA in OT-SOC IR (Figure 5.1). The framework is based on A Dynamic Framework Highlighting Situational Awareness in Cyber IR (Figure 1.1) by Andreassen et al. (2023) and applies Collective Intelligence theory (Figure 2.17) and Endsley's (1995) theory of Situation Awareness of the Environment (Figure 2.16) to map and create an understanding of CSA and SA in a cross-domain and multi-actor environment. Additionally, the framework draws upon aspects from Situation-Awareness in Cybersecurity Incident Response (Figure 2.18) by Ahmad et al. (2021) to better highlight the intricacies of SA in IR and the Purdue model (Figure 2.19) as presented by Onshus et al. (2022) to distinguish the two domains. As we consider their representation to be an accurate depiction of the IT domain during SOC IR, the IT section of the framework is based on the work of Andreasen et al. (2023) and adapted, using theory and empirical data, to fit the context of OT-SOC IR. In addition, the OT side is the direct result and amalgamation of theory and empirical data and has been modeled to fit the structure of the IT domain. As such, from a systematic review of the current body of knowledge and 11 interviews with 14 industry professionals, we have developed a conceptual framework that models the process of CSA in OT-SOC IR.

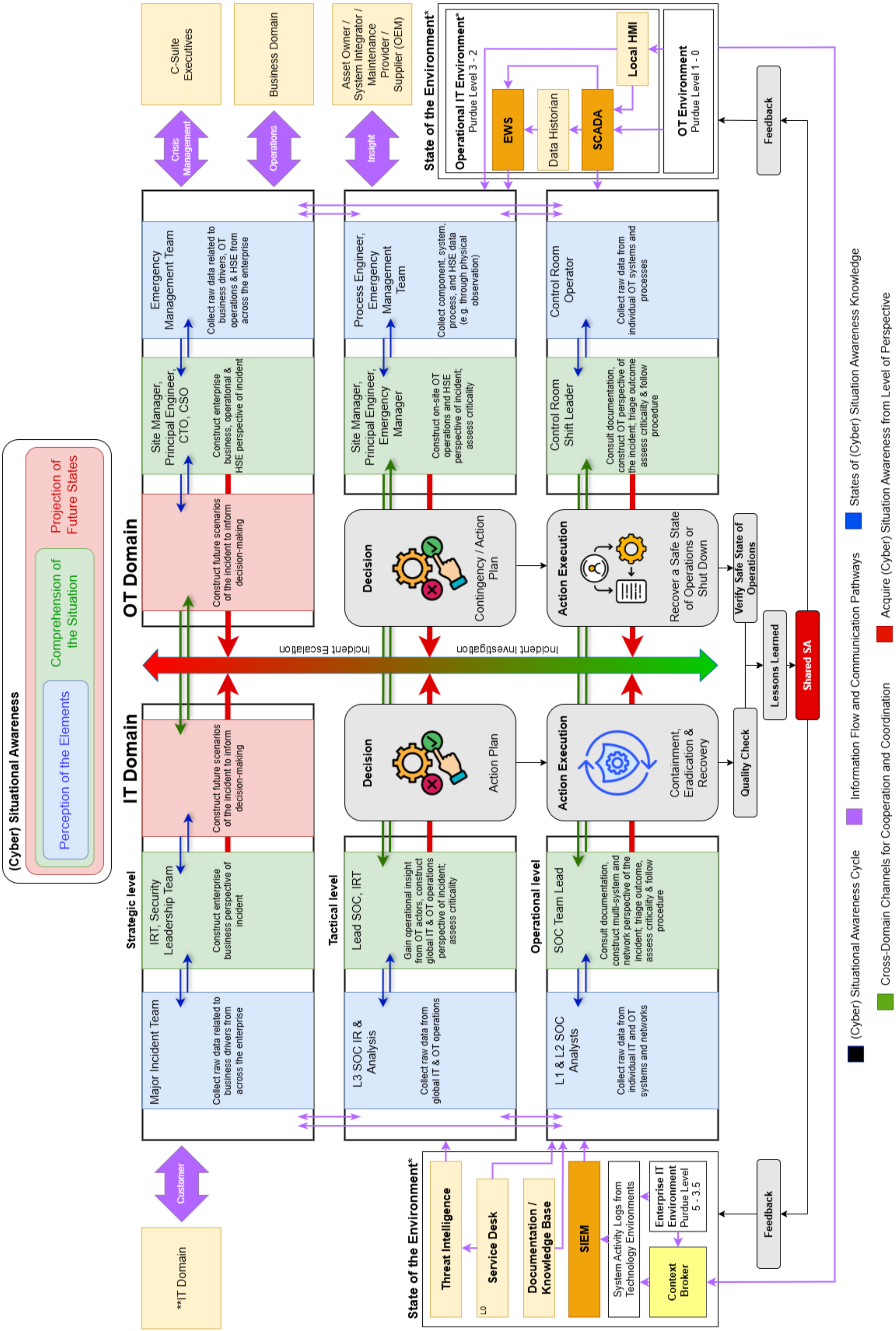

(Cyber) Situational Awareness
Perception of the Elements
Comprehension of the Situation
Projection of Future States
IT Domain
OT Domain
Strategic level
Tactical level
Operational level
**IT Domain
Customer
C-Suite Executives
Crisis Management
Business Domain
Operations
Asset Owner / System Integrator / Maintenance Provider / Supplier (OEM)
Insight
Major Incident Team
Collect raw data related to business drivers from across the enterprise
IRT, Security Leadership Team
Construct enterprise business perspective of incident
Construct future scenarios of the incident to inform decision-making
Construct future scenarios of the incident to inform decision-making
Site Manager, Principal Engineer, CTO, CSO
Construct enterprise business, operational & HSE perspective of incident
Emergency Management Team
Collect raw data related to business drivers, OT operations & HSE from across the enterprise
L3 SOC IR & Analysis
Collect raw data from global IT & OT operations
Lead SOC, IRT
Gain operational insight from OT actors, construct global IT & OT operations perspective of incident; assess criticality
Decision
Action Plan
Decision
Contingency / Action Plan
Site Manager, Principal Engineer, Emergency Manager
Construct on-site OT operations and HSE perspective of incident; assess criticality
Process Engineer, Emergency Management Team
Collect component, system, process, and HSE data (e.g. through physical observation)
L1 & L2 SOC Analysts
Collect raw data from individual IT and OT systems and networks
SOC Team Lead
Consult documentation, construct multi-system and network perspective of the incident; triage outcome, assess criticality & follow procedure
Action Execution
Containment, Eradication & Recovery
Action Execution
Recover a Safe State of Operations or Shut Down
Control Room Shift Leader
Consult documentation, construct OT perspective of the incident; triage outcome assess criticality & follow procedure
Control Room Operator
Collect raw data from individual OT systems and processes
Incident Escalation
Incident Investigation
Quality Check
Lessons Learned
Shared SA
Verify Safe State of Operations
Feedback
Feedback
State of the Environment*
Threat Intelligence
Service Desk
L0
Documentation / Knowledge Base
SIEM
System Activity Logs from Technology Environments
Enterprise IT Environment Purdue Level 5 - 3.5
Context Broker
State of the Environment*
Operational IT Environment* Purdue Level 3 - 2
EWS
Data Historian
SCADA
Local HMI
OT Environment Purdue Level 1 - 0
■ (Cyber) Situational Awareness Cycle
■ Information Flow and Communication Pathways
■ States of (Cyber) Situation Awareness Knowledge
■ Cross-Domain Channels for Cooperation and Coordination
■ Acquire (Cyber) Situation Awareness from Level of Perspective

Figure 5.1: A Dynamic Framework for Cyber Situational Awareness in OT-SOC Incident Response.
*A simplified generalization, not a complete representation and may depend on the configuration of the environment.
**Exists if the OT organization (customer) employs IT personnel.

As an extension of the SA for SOC IR framework (Figure 1.1) by Andreassen et al. (2023), many of the elements used in the CSA framework (Figure 5.1) will be inherently similar to create understanding of CSA in OT-SOC IR. While the meaning of these elements are the same, the context in which they are applied differs. As such, the description of individual elements will not be comprehensive; instead, the focus will be on the unique contexts that apply in OT-SOC IR.

The framework is presented as a two-dimensional artifact depicting the IT domain on the left side and the OT domain on the right side along with domain-specific stakeholders integral to the cross-domain IR process, environments, and their interconnections. Actors, stakeholders, and their respective decision-making levels are mapped on the vertical plane and the three phases (perception, comprehension, and projection) of Endsley's (1995) process of SA on the horizontal plane. In both domains, the various levels of CSA and SA are denoted by color, where blue is the perception of the elements, green is the comprehension of the situation, and red is the prediction of future states. Additionally, the process from decision to feedback into the environment of Endsley's (1995) model is illustrated using grey boxes connected by black arrows. The framework features four kinds of dynamic behavior: information processing behavior (data-driven vs goal-driven), task behavior (escalation vs investigation), communication behavior (information flow and communication pathways), and cooperation and coordination behavior (cross-domain channels for cooperation and coordination) (Ahmad et al., 2021; Andreassen et al., 2023).

Information processing behavior that allows for progression through Endsley's (1995) 3 states of SA knowledge among actors internally is modeled using the dark blue arrows depicted in Figure 5.1. The dark blue arrows pointing toward the middle (right-facing in the IT domain and left-facing in the OT domain) indicate increased levels of CSA in the IT domain and SA in the OT domain from data-driven processes (moving from perception to comprehension to projection) (Ahmad et al., 2021). While both the IT and OT domain mostly utilize data that originate from IT, the OT domain is also dependent on data acquired through physical observation of the environment. Furthermore, the dark blue arrows pointing away from the middle (left-facing in the IT domain and right-facing in the OT domain) "*reflect that goal-driven processing, such as attention-focusing using existing mental models, can improve lower levels of [SA] (moving from projection to comprehension to perception)*" (Ahmad et al., 2021, p. 10). An example of goal-driven processing in the OT domain is using the projected failure of a process to better comprehend the situation and gather more data to identify a safe solution.

The red and green gradient arrow in the middle of the framework models task behavior. Moving toward the top (red) of the arrow represents situations where priority incidents are escalated in the decision-making hierarchy, from the CR or SOC to principal engineers and IRT and, finally, the security leadership team and the CTO and CSO (Ahmad et al., 2021). Moving toward the bottom (green) of the arrow represents situations where higher-level decision-makers require additional incident data or context from the CR, SOC, OT service providers, or physically from the environment (Ahmad et al., 2021).

Based on Andreassen et al. (2023), the larger purple arrows on the leftmost and rightmost sides are communication pathways to external actors. In the OT space, a component or system might have been manufactured, specified, and implemented by different entities, requiring engineers to engage with various external entities to obtain essential system insight (Humayed et al., 2017). Finally, the smaller purple arrows in the framework represent information flow and how different sources of knowledge and understanding distribute information between stakeholders, technologies, and environments (Andreassen et al., 2023).

The green arrows connecting the two domains represent cross-domain channels for cooperation and coordination. These connections are essential for CSA in OT-SOC IR, as they facilitate crucial information sharing and the successful mobilization and coordination of skills across the two domains. On the operational and tactical levels, cooperation and coordination occur when stakeholders retain a single or partial multi-domain comprehension of the situation. Cooperating and coordinating their comprehension with stakeholders in the other domain adds to and expands their current understanding of the situation. For the SOC, this adds incident context, enabling the correlation of digital indicators to events in the physical world through the interpretation of data that might otherwise be outside their current knowledge. In addition, information from the SOC could cause the CR to understand and attribute some operational anomaly to an event in the cyber domain. On the strategic layer, senior stakeholders share projections of the future states of the situation to inform decision-making and increase their comprehension of the broader impact of the incident on business, operations, and Health, Safety, and Environment (HSE).

The red arrows pointing toward the center represent the stakeholders' contributions on each decision-making level to CSA in IT and SA in OT relative to their frame of reference (Ahmad et al., 2021). From the control room on the operational level, the shift leader retains a broader, less detailed frame of reference, constructing a real-time state of local operations of OT systems and processes perspective. On the tactical level, the site manager, principal engineer, and emergency manager have a broader, more specialized, and highly detailed frame of reference and construct the local site operations and HSE perspective of the incident. On the strategic level, the site manager, principal engineer, CTO, and CSO have an encompassing frame of reference for constructing the incident's enterprise business, operations, and HSE perspective.

On the framework's lower left and right side (Figure 5.1), the *State of the Environment* represents the source of data collection for both the IT and OT domains. Following the Purdue model (Figure 2.19) as presented by Onshus et al. (2022), the environments have been separated into enterprise IT, operational IT, and OT. In the OT domain, the environment is split into the operational IT and OT environment. The operational IT environment on levels 3-2 incorporates assets and technologies that exist separately but are connected to the processes and are utilized in the operation and control of the OT environment. The OT environment on levels 1-0 represents the industrial processes and encompasses the assets concerned with process logic and the field devices that sense, manipulate, and interact with the physical world. Furthermore, the OT environment (Purdue 0-1) passes process data to local HMIs, enabling on-site personnel to gather data via physical observation and the SCADA system (Purdue 3-2). The SCADA collects and aggregates real-time data from the OT environment, enabling CR operators to monitor and control the environment's systems and processes. Additionally, the SCADA passes data to the data historian, a server for extended storage of process and event data. Data from the historian and SCADA system can then be accessed via the EWS, facilitating real-time and historical insight into the OT environment. Levels 5 to 3.5 in the IT domain represent the enterprise IT environment, encompassing all technologies not directly related to the operational environment. However, data from the operational IT (SCADA and data historian) and OT (process data) environments (Purdue 3-0) are collected and correlated with data from the enterprise IT environment by a context broker. The context broker integrates data from multiple IT and OT systems, retains a baseline of normal system activity, and creates a holistic view of data that facilitates the correlation of cyber incidents to events in the physical space (European Comission, 2024). Events that fall outside of the baseline are passed on to the SIEM as alerts, where SOC analysts can analyze and construct a picture of the incident and assess its criticality (Andreassen et al., 2023). Lastly, in the IT domain, the documentation or knowledge base acts as an essential source for knowledge such as asset overviews, network maps, contact lists, and response procedures, information that adds further context and understanding of the operational IT and OT environment.

The grey boxes and black arrows towards the middle of the framework (Figure 5.1) reflect the following process after reaching any of the three states of CSA or SA according to Endsley's (1995) theory of SA. Stakeholders utilize their current level of CSA or SA to make a decision, which in the OT domain is either resorting to an existing contingency plan for predicted incidents or the creation of an ad-hoc action plan based on the current state of SA. For action execution, the OT domain is concerned with reaching a safe state. Therefore, action execution results in taking steps to recover a safe state of operations, or if a safe operational state cannot be guaranteed or maintained, the affected systems are shut down. Following action execution is the verification of the system state of safety followed by lessons learned where the IT and OT domains share incident insight and information and achieve shared SA. The consequence of the selected action is then applied to the environment as feedback, changing the environment, "*this interaction with the real-world environment results in further modification of the operators mental model which directs further actions*" (Ahmad et al., 2021, p. 4).

When an alert is triggered in the SIEM due to activity that deviates from the context broker baseline, operational-level SOC personnel analyze the event, correlating IT and OT data to determine whether it affects the OT domain. In the event of an incident that involves the OT domain, the SOC personnel consult the knowledge base, determine whether the alert was triggered unintentionally or if there is an indication of malicious activity, triage the multi-system incident based on their comprehension, and contact the CR to acquire additional context and make them aware. Both team leaders cooperate and coordinate their efforts by sharing information from their domain perspective. If the CR is uncertain or determines that the incident could impact the OT environment, they will continue to monitor the OT environment, triage, and escalate the incident, requesting on-site personnel to check and verify their observations. Process engineers gather data through physical observation and additional insight from OT service providers, sharing the information with the CR, site manager, and principal engineer. From here, the site manager and principal engineer assess the operational and HSE situation and activate the IT IRT and the emergency management team. In the rare event of a major incident, the CSO and CTO are engaged, which can coordinate internal resources should the need arise. The strategic actors in both domains cooperate to construct an accurate multi-domain picture of future scenarios to inform decision-making. Subsequently, a decision is made, and the effect of the selected course of action on the state of the environment in both domains is observed to determine whether further action is required.

5.2 Discussion

This section will discuss the elements and characteristics that are unique to and distinguish CSA in OT-SOC IR from SA in IT-SOC IR. We will highlight the complexities and key differences between our framework (Figure 5.1) and the work of Andreassen et al. (2023) (Figure 1.1). Thereby making it clear how we have adapted and extended the framework of Andreassen et al. (2023) to fit the context of cyber incidents that affect the physical world. First, we will discuss how collective intelligence facilitates CSA and SA in the complex cross-domain and multi-actor environment of OT-SOC IR before addressing the distinct HSE perspective of the OT domain and how it impacts the CSA and SA process during IR. We will then discuss the people, processes, and technologies on the operational layer that act as the foundation for effective IR. Finally, we accentuate and discuss the broader complexities of cross-domain IR to garner an understanding of the interdisciplinary challenges and extensive efforts required for OT-SOC IR.

5.2.1 Collective Intelligence in OT-SOC IR

For incidents that encompass both the IT and OT domains, we argue that CSA in OT-SOC IR and the successful and timely resolution of incidents are dependent upon the creation of a CI among the stakeholders involved in the cross-domain response effort. Elements of the framework (Figure 5.1) can be placed into one or more categories as contributing factors to cognition, cooperation, or coordination, which facilitate CI and enable CSA in cross-domain and multi-actor environments. These elements have been derived from empirical data and are supported by literature as both key requirements to industrial IR and accommodate important challenges that impede the development of SOCs. The literature in Chapter 2.4.1 emphasizes domain knowledge of OT, cross-discipline integration, communication, and information sharing, and shared situational awareness as key requirements for cyber-IR in industrial environments. Additionally, the literature in Chapter 2.3.3 specifies challenges related to the collaboration of experts, integration of domain knowledge, and increasing technological complexity. In the following sections, we will provide examples from the framework, and rationale and expand upon how these elements facilitate CSA in OT-SOC IR.

Two of the challenges raised in Chapter 2.3.3 by Vielberth et al. (2020) concern the collaboration of experts and the integration of domain knowledge. When the scope of the SOC is expanded to include OT, the perspectives and domain knowledge of non-security experts, such as engineers, become crucial in dealing with the situations that arise (Vielberth et al., 2020). Coinciding with the literature, multiple respondents also highlighted the importance of input from OT stakeholders familiar with the environment's context and intricacies, specifically mentioning CR operators, on-site personnel, and engineers. The *Senior_ OT_ Analyst* specified that it is challenging for individuals without OT and environment knowledge to interpret and understand the data that originate from the industrial processes. Additionally, the *Senior_IT&OT_Advisor* added that SOC operators must cooperate with process engineers or someone with process understanding to correctly triage and select the right course of action. As a solution, most respondents mentioned communication, information sharing, procedures, and documentation as essential facilitators for cooperation and coordination. Documentation is represented in the state of the environment and provides the SOC with information on how to respond, who to contact, and how to communicate. While procedures are considered a part of the documentation, it is also defined as the final action of the *SOC Team Lead* and the *CR Shift Leader* before initiating communication (Figure 5.2). Communication and information sharing are reflected in the framework as the green arrows (Figure 5.2) connecting the domains and the purple arrows on the left and right sides.

On the operational layer, the green arrows connect the *SOC Team Lead* and the *CR Shift Leader*, enabling the SOC and CR to communicate and share information to gain crucial understanding and context. Information sharing between the SOC and the CR and continuous communication is essential in ensuring CSA, coordination, and operational efficiency during IR (Fink & Shulga, 2018; Pöyhönen et al., 2021). As such, the four elements in the framework - communication, information sharing, documentation, and procedures - facilitate CI by acting as essential enablers for cooperation and coordination and the successful and effective distribution of cognition elements, such as knowledge, understanding, context, and awareness. Lastly, these elements resolve the collaboration of experts and the integration of domain knowledge challenges presented by Vielberth et al. (2020) in Chapter 2.3.3 and fulfill two of the four key requirements for industrial cyber-IR response in Chapter 2.4.1, specifically cross-discipline integration and communication and information sharing.

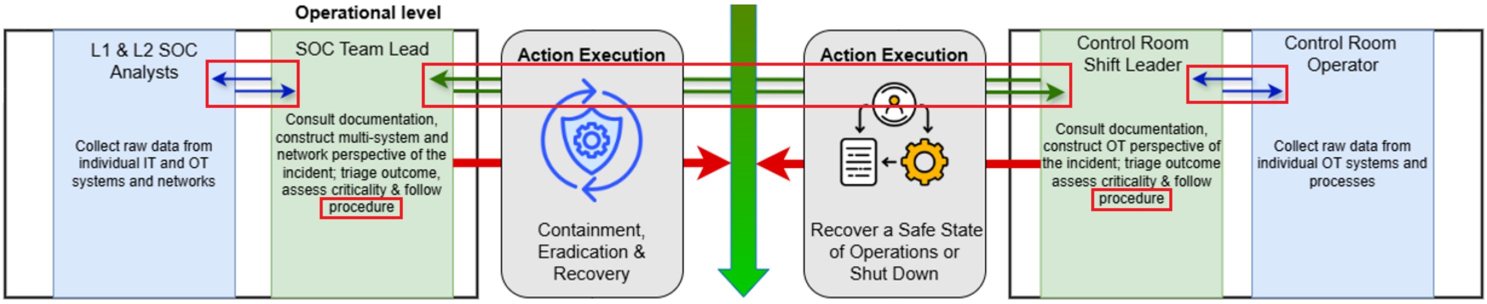

Operational level
L1 & L2 SOC Analysts
Collect raw data from individual IT and OT systems and networks
SOC Team Lead
Consult documentation, construct multi-system and network perspective of the incident; triage outcome, assess criticality & follow procedure
Action Execution
Containment, Eradication & Recovery
Action Execution
Recover a Safe State of Operations or Shut Down
Control Room Shift Leader
Consult documentation, construct OT perspective of the incident; triage outcome assess criticality & follow procedure
Control Room Operator
Collect raw data from individual OT systems and processes

Figure 5.2: Elements of Cooperation and Coordination in our framework of CSA in OT-SOC IR (Figure 5.1)

Findings from the interviews indicate a consensus among the respondents that domain knowledge and understanding are the most important and decisive features for the SOC to gain CSA and succeed in OT IR. Respondents specified general knowledge and understanding of operational technologies, the differences between IT and OT, individual customer environments, and safety. This correlates with the key requirement for industrial cyber-IR in Chapter 2.4.1, domain knowledge of OT. Due to the highly contextualized and varied nature of OT, without the right expertise, domain knowledge, and an understanding of the existing system requirements, the SOC won't be able to adequately assess the likely impact of an incident and the potential changes made to the OT system (Smith et al., 2021). While monitoring OT depends on visibility into the systems and processes that make up the environments, respondents clarified that a lack of essential knowledge and context would leave the SOC unable to interpret and understand the data from OT environments. To solve this issue, the CSA framework (Figure 5.1) integrates three key sources of information and knowledge that provide the SOC with essential context and understanding. These elements are the context broker, documentation, and communication and information-sharing channels with external actors. First, the context broker (Figure 5.3) provides the SOC with knowledge of the state of the OT environment, keeps a baseline of regular activity, and combines data from both environments to correlate cyber events to events in the OT environment. Additionally, the context broker allows for adding context data, such as assigning PLCs or RTUs to specific processes, providing a MAC address with a component name or description, and details on proprietary protocol communications unique to OT networks. The documentation and knowledge base contains knowledge on, amongst other things, network architecture, assets, response procedures, who to contact, and more (Figure 5.3). Lastly, communication and information-sharing channels with external actors, such as the CR and process engineers, enable the SOC to acquire necessary knowledge, context, and understanding from experienced individuals with domain and environment understanding on demand. Even if this knowledge is not cognitively held by the SOC analysts themselves, these elements are sources of shared information that can be accessed when needed to acquire the knowledge necessary to develop CSA. Combined, the context broker, documentation, and communication and information-sharing channels with external actors satisfy the domain knowledge of OT requirement in Chapter 2.4.1 and can be considered as a solution to the challenge of increasing technological complexity stated by Vielberth et al. (2020) in Chapter 2.3.3. Lastly, in CI these can be considered elements of cognition, sources of knowledge that enable the SOC to understand and become aware of the environment they are interacting with.

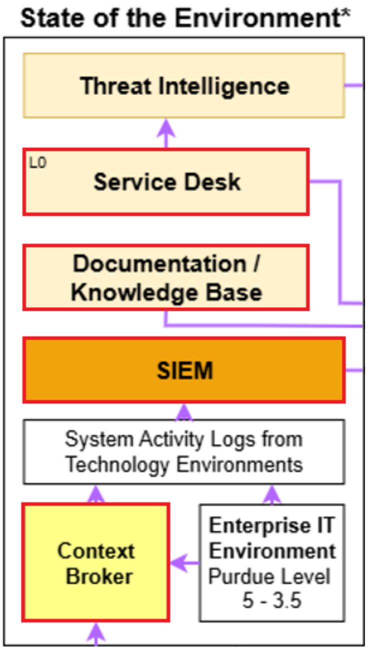

State of the Environment*
Threat Intelligence
L0
Service Desk
Documentation / Knowledge Base
SIEM
System Activity Logs from Technology Environments
Context Broker
Enterprise IT Environment Purdue Level 5 - 3.5

Figure 5.3: Elements of Cognition in our framework of CSA in OT-SOC IR (Figure 5.1)

Holistically, communication, information sharing, documentation, procedures, the context broker, and external actors can be considered as elements of cognition, cooperation, or coordination and facilitate the creation of a CI which enables CSA in the cross-domain and multi-actor environment of OT-SOC IR (Figure 5.4). In the framework (Figure 5.1), these elements compensate for the inherent differences between IT and OT, allowing the SOC to perceive the elements and comprehend situations that span the two domains. The merger of knowledge and experience from various stakeholders across the two domains as a result of CI is key to a successful OT IR (Smith et al., 2021). Additionally, cooperation, coordination, and cognition lead to synchronization of efforts and provide IR stakeholders in both domains with the CSA or SA necessary for their responsibilities. As such, CI facilitates the development of shared SA, accommodating the fourth and final key requirement of IR in industrial environments in Chapter 2.4.1. CI acts as the foundation for OT-SOC IR through the generation of a universally distributed, constantly enhanced, real-time intelligence among IR stakeholders which result in effective mobilization of skills and knowledge required to become situationally aware and resolve cross-domain incidents (Lévy, 1997).

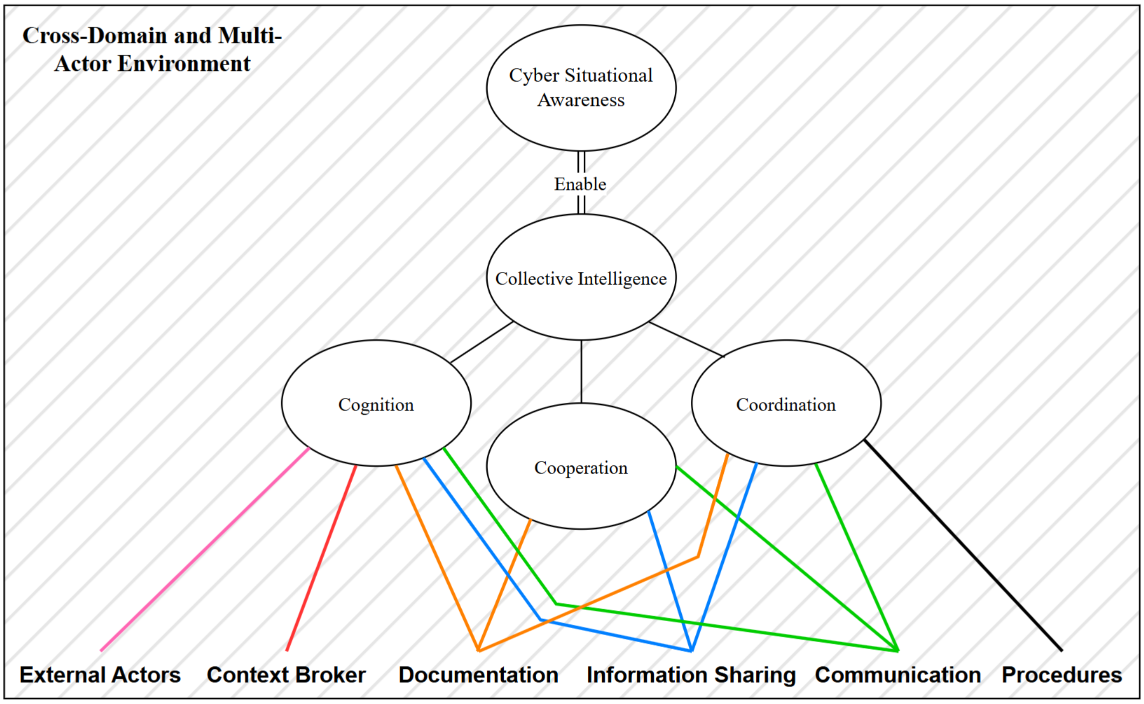


Figure 5.4: Elements of Collective Intelligence in OT-SOC IR

5.2.2 Health, Safety, and Environment

When a SOC deals with security monitoring and IR for an OT environment, HSE plays a role in how SOC analysts' CSA is impacted. Based on the qualitative research, interview respondents expressed opinions on how a SOC cannot directly respond to the OT environment. Blocking a connection from a PLC might cause pressure to rise and cause an explosion. As OT has safety as its most important aspect, this notion creates a challenging dynamic for the SOC when dealing with IR in this domain.

SOC analysts require adequate information, documentation, and domain knowledge in order to handle OT incidents sufficiently, according to the findings and backed up by the literature. As the *Senior_IT&OT_Advisor* explained in chapter 4.1.4, *"[The SOC and the CR] need [information on] more like: How do we handle it? Do we need more help? Who should be involved? Have we notified those whom we should notify? What are the possible consequences?"*. Vielberth et al. (2020) highlights the notion of complexity of a SOC when introducing OT and IT environments. When dealing with the complexity of the OT environment with security monitoring, to have HSE on top of everything, as highlighted by the interviews, *"The CIA triangle, for example, is supposed to be reversed in OT. I'm not entirely sure that's true. It's another way of seeing it, but everybody says it's in reverse in OT. No, it's just that you have the safety on top of everything"*. The challenge for a SOC is its security operations while attempting to increase its CSA at all times while dealing with safety-critical systems. Consequently, IR in the OT environment must always cater to safety.

The CSA framework (Figure 5.1) highlights the workflow across organizational levels and domains when an OT-SOC deals with IR. The roles on the tactical level all have their part to play in the HSE data collection when dealing with IR. As such, the people, processes and technologies that are included, to eventually where the CR and SOC share information cross-domain to ascertain the situation where the criticality of a (cyber) incident might heavily impact HSE; the *Professor* expressed *"You can never let people die. It's completely out of the question. Safety first, [the] environment second."* This alone is a crucial aspect of what impacts SOC analysts' CSA in understanding the OT domain and its environment;

the consequences can lead to physical harm. The literature and the respondents of the interviews make this abundantly clear. The *OT_SOC_Team_Lead* expressed in the interview how "[...] *the more you know about a customer's environment, the easier it is to protect and the faster you can be at protecting it.*"

Incident Response in the context of dealing with Health, Safety, and Environment in OT IM from a SOC perspective means that analysts working there must have the right tools and adequate information from the right sources to make the right decisions and information to pass along during an IR cross-domain and organizational levels. This is the crucial point of how HSE impacts a SOC's CSA, understanding, knowledge, and documentation, as highlighted in the framework, as well as the communication pathways between entities, processes, and technologies.

5.2.3 The Operational Level

The foundation of effective incident response boils down to the people, processes, and technologies in which a SOC operates. The core elements must be in place for an MSSP to do its security operations effectively. These elements, as previously discussed regarding CI, fundamentally build CSA and enable the foundation for effective IR. The operational level, as shown in Figure 5.5, comprises essentially two roles in each domain: SOC analysts and CR operators. In collaboration with the process engineer, the information flow originates from the OT environment, and the CR operators will establish an understanding of an alert that triggers in the CR. Consequently, this will also trigger on the SOC side through the Context Broker, where the two roles will communicate and share information to establish and increase CSA.

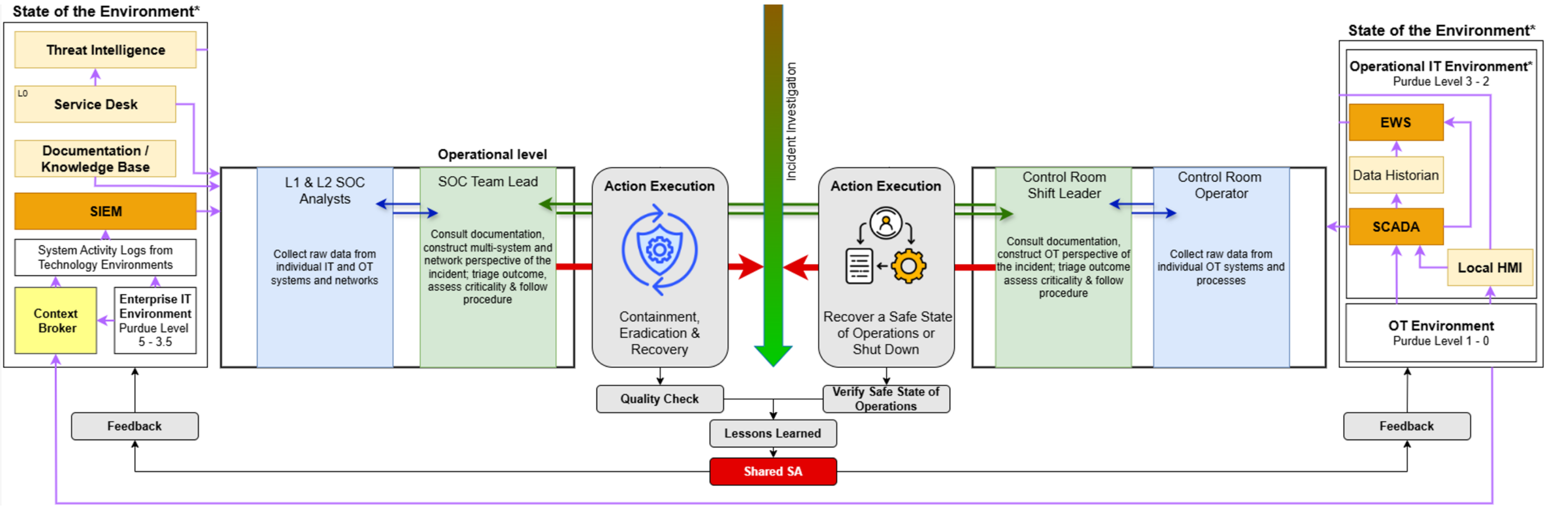

State of the Environment*
Threat Intelligence
L0
Service Desk
Documentation / Knowledge Base
SIEM
System Activity Logs from Technology Environments
Context Broker
Enterprise IT Environment Purdue Level 5 - 3.5
Operational level
L1 & L2 SOC Analysts
Collect raw data from individual IT and OT systems and networks
SOC Team Lead
Consult documentation, construct multi-system and network perspective of the incident; triage outcome, assess criticality & follow procedure
Action Execution
Containment, Eradication & Recovery
Incident Investigation
Action Execution
Recover a Safe State of Operations or Shut Down
Control Room Shift Leader
Consult documentation, construct OT perspective of the incident; triage outcome assess criticality & follow procedure
Control Room Operator
Collect raw data from individual OT systems and processes
State of the Environment*
Operational IT Environment*
Purdue Level 3 - 2
EWS
Data Historian
SCADA
Local HMI
OT Environment
Purdue Level 1 - 0
Quality Check
Verify Safe State of Operations
Lessons Learned
Shared SA
Feedback
Feedback

Figure 5.5: The Operational Level of the CSA for OT-SOC IR Framework

At the core of all OT-SOC IR resides the concept of baseline. An unforeseen incident or alert that deviates from the norm, and the data that originates from this event gets passed through the Context Broker. This results in contextualized data, which leads to increased understanding. Furthermore, in every event, the SOC greatly relies upon documentation. As respondents from the interviews made clear, when an incident or alert occurs, they update the documentation, detailing the event by logging new information. Additionally, the CR assists in this process by sharing information from the process engineers, who have a more detailed frame of reference than the CR. As Figure 5.1 highlights in the tactical section on the OT domain, the process engineers will have contact with the 3rd party suppliers. With this, in-depth information will be gathered and shared with the CR, which in turn will be shared with the SOC. This information flow enables a heightened CSA, as the data and information from the process, incident, and context of the environment are understood by all parties cross-domain, as the SOC will share its IT-related information.

The resulting factor is a comprehension of the situation. The MSSP is operationalized alongside the OT domain, collecting contextualized data via their technologies and tools, i.e. Context Broker and SIEM, and through documentation and collaboration. Smith et al. (2021) underlines this by highlighting the importance of cross-domain cooperation, saying: "*Cyber IR within ICS is characterized by high levels of uncertainty and unpredictability and requires a multi-disciplined team that encompasses personnel business operations, OT, IT, security operations [...] to be effective.*" Therefore, the operational level's people, processes, and technologies are the foundation for an effective IR with a SOC.

5.2.4 The Complexity of Cross-Domain Incident Response

Highlighted by theory in Chapter 2.4.1, IR in industrial environments is a complex and extensive process that requires collaboration between multi-disciplined stakeholders from several domains (Smith et al., 2021). Different technologies and priorities make cross-domain IR a challenging endeavor that is dependent on highly specialized and contextualized knowledge. Comparing the work of Andreassen et al. (2023) in Figure 1.1 with the proposed framework in Figure 5.1 illustrates the extensive nature of the issue and accentuates the importance of shared SA in OT-SOC IR. While the SOC might be operationalized the same internally in terms of people, the technological environment, processes, and external dependencies are significantly different when OT is incorporated into its scope.

As indicated by both theory in Chapter 2.4.1 and the respondents, availability requirements and the safety-critical nature, combined with the highly contextualized and diverse nature of OT systems, make the SOC dependent on operators and maintainers as well as third-party OT service providers. While the CR acts as the SOC point of contact, their role makes their frame of reference broad and less detailed than that of process engineers. This makes the CR dependent on on-site personnel to discern and understand the full scope of operational anomalies. Process engineers retain a smaller but detailed frame of reference relative to the CR as they are concerned with the individual components and systems that make up the processes. While process engineers understand the processes, they often require input from external OT service providers to fully grasp the intricacies of the OT systems. This is just one example of how rigorous the information-gathering and incident response process can be during OT-SOC IR. Showcasing how incidents that start with the SOC could require input from multiple different entities to arrive at a resolution.

Respondents denoted preparation in terms of domain knowledge, speaking the domain language, and preparing the right processes, procedures, and insight into the environment for IR as essential for the success of the SOC in dealing with OT. Processes are generally documented as procedures detailing what needs to be done and how to do it. Additionally, the SOC needs to speak the domain language when sharing information with the CR or OT actors in general. When a cyber-incident occurs, the SOC needs to communicate why it is important and how this could impact the OT environment to garner support from OT stakeholders. Training and documented processes and procedures facilitate some preliminary understanding of how to communicate across the domains. An example of domain language can be found in the framework, on the strategic level the IT domain communicates with the customer's IT department. Additionally, the importance of planning and having procedures in place is indicated by the contingency plan in the decision on the OT side of the framework. "*Regardless of the cause of the situation, incident response planning produces contingency plans to manage the negative impacts on critical equipment and operations. ICS operators typically have plans in place for loss of essential power, supplies, and output, but it is only recently that these plans have started to consider cyber impact.* (Smith et al., 2021, p. 2). While the MSSP and SOC remain the same internally, the environment in which they operate drastically changes with the inclusion of OT into its scope. To address this, the respondents and literature emphasize the importance of IM or preparing the SOC in dealing with OT. Elements in the framework, such as documentation, procedures, cross-domain communication, and information sharing are elements that represent the result of sufficient incident response planning or IM. In close collaboration with actors from the OT domain, the MSSP and SOC need to develop procedures for IR, points of communication between the SOC and the OT asset owner, and documentation. Planning and preparation provide the SOC with the foundation needed to obtain CSA and handle the complexities of cross-domain IR.

Chapter 6

Conclusion

In this study, we explored the concept of OT-SOC IR and sought to understand how physical real-time, high-availability, and safety-critical operational technologies change the SOC when integrated into its scope. Using collective intelligence theory (Malone & Bernstein, 2015) and Endsley's (1995) theory of SA, we have expanded on the work of Andreassen et al. (2023) and created a conceptual framework that models CSA in OT-SOC IR. Holistically, the framework maps and represents how people, processes, and technologies are operationalized across MSSPs and OT organizations in cross-domain IT and OT cybersecurity detection and response. The framework follows the SA cycle and illustrates how the different elements facilitate effective decision-making during cross-domain IR. Illustrating how people, processes, and technologies work across the IT and OT domains and on different decision-making levels to support or enable the perception, comprehension, and projection of a combined IT and OT environment to construct shared SA. Detailing how the increased socio-technological complexity of the combined IT and OT environment makes IR stakeholders in either domain mutually dependent on each other in obtaining SA. In OT IR, the SOC relies on numerous sources of knowledge and context to acquire CSA and enable the correlation of cyber incidents with events that impact physical operations in OT environments. Similarly, stakeholders in the OT domain depend on the SOC to acquire SA by identifying and making them aware of cyber incidents that impact operational availability and safety. Making cross-domain IT and OT IR a continuous exercise in cooperation and coordinating domain knowledge, skillsets, and priorities to obtain a collective IR intelligence and shared SA.

Expanding the scope of MSSPs to include OT security operations as a service does not necessitate a change in how people are operationalized. However, the technological environment in which they operate, their processes, and external dependencies change significantly. OT is a fundamentally different category of technology that makes MSSPs dependent on sources of knowledge and context, such as documentation, the context broker, and communication and information-sharing channels with the owner or maintainer of the OT environment, to sufficiently perceive and comprehend the intricacies of the industrial environment and its processes. Additionally, due to OT's high availability and safety-critical context, MSSPs retain a less active, supportive information-sharing role. This is reflected in their processes, which in OT environments are not to contain, eradicate, and recover but to provide the OT stakeholders with information on anything that might impact the operational integrity and compromise safety. Additionally, during IR, the MSSP and the SOC depend on external actors to acquire and retain CSA. Information on what is happening in industrial networks and systems requires domain knowledge and often physical observation from on-site personnel. Consequently, CSA depends on communication and information sharing with external OT actors familiar with the environment, processes, and context.

6.1 Contribution

Our work contributes to cyber situational awareness and situational awareness theory in the context of cross-domain cybersecurity incident response in industrial environments. We add to and further the understanding of how MSSPs and SOCs correlate cyber incidents to events in the physical environment and develop CSA by expanding on the work of Andreassen et al. (2023). We also apply and expand upon established theories in the context of cybersecurity operations and industrial environments, using Endsley's (1995) theory of Situation Awareness and Collective Intelligence theory in the OT and cybersecurity domains to explain CSA in OT-SOC IR. The presented framework emphasizes how MSSPs and SOCs develop CSA in a complex cross-domain environment but also provides insight and contributes to understanding how OT actors fully obtain SA during a cyber-IR and how shared SA is generated in cross-domain cybersecurity operations. Additionally, we create an understanding of how people, processes, and technologies are operationalized across domains during cyber-IR in OT environments. Our work also contributes to the current knowledge of control rooms in the OT domain. Finally, our work contributes to the body of knowledge on SOC processes and IR, CSA and covers a gap in the literature on CSA in OT-SOC IR.

6.2 Limitations

Four main limitations apply to this study and should be addressed. Firstly, during our SLR, we found that there is no literature on CSA in OT-SOC IR. While there is an extensive body of knowledge on the surrounding topics, we could not identify any literature considering CSA in the context of OT-SOC IR. Consequently, the work proved to be more resource-intensive and demanding than we initially thought. Therefore, limited by time and resources, we know that this study might not be sufficiently comprehensive and that additional work is required to fill the research gap on CSA in OT-SOC IR. Secondly, limited and dated literature covering control rooms made comprehending their role, function, and processes challenging. This made us dependent on respondent insight and understanding to further the knowledge of and adequately comprehend the CR as an entity, its role in OT-SOC IR, and its contribution to the development of CSA. Third, to get a more accurate and nuanced perspective of the challenges of cyber-IR in OT environments, we should have included more than one engineer or on-site respondent in our interviews. Technical on-site personnel who work on OT and CPS possess operational and safety knowledge that could prove essential and significantly improve the framework. Lastly, based on literature and empirical data, the framework models CSA in OT-SOC IR from the perspective of a single ideal incident scenario. While the framework offers a theoretically ideal solution, we acknowledge that it may not be the easiest solution to implement in a real-world MSSP, SOC, or OT setting.

6.3 Future Work

While the thesis addressed CSA in OT-SOC IR, some limitations remain, prompting opportunities for future work. Specifically, the framework is a result of theory and practitioner input and remains theoretical in nature. To ensure its real-world applicability, the framework should be empirically and practically validated in a MSSP and OT environment. We propose that researchers engage with OT personnel on-site and on the various decision-making levels and conduct iterative scenario-based testing or simulations. Additionally, future work should address this study's four limitations to further improve upon the framework and acquire a better understanding of CSA in OT-SOC IR. Generally, we find a lack of recent and relevant literature on SOCs in the context of OT. We therefore encourage researchers to investigate the topics of OT-SOCs, CSA in OT-SOCs, and cybersecurity monitoring of high availability and safety-critical environments.

Bibliography

Afry. (2023). Et av bransjens mest avanserte kontrollrom optimaliserer produksjonen ved elkems anlegg i bremanger. *Afry.* https://afry.com/no-no/aktuelt/nyhetsside/et-av-bransjens-mest-avanserte-kontrollrom-optimaliserer-produksjonen-ved-elkems

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Akbarzadeh, B. A., & Katsikas, S. (2022). Unified it&ot modeling for cybersecurity analysis of cyber-physical systems. *IEEE Open Journal of the Industrial Electronics Society*, *3*, 318–328. https://doi.org/10.1109/OJIES.2022.3178834

Alvesson, M., Sandberg, J., & Einola, K. (2022). Reflexive design in qualitative research. In U. Flick (Ed.), *The sage handbook of qualitative research design* (pp. 23–40). SAGE Publications.

American Psychological Association. (n.d.). Apa dictionary of psychology: Cognition [Accessed: 10.04.2024]. https://dictionary.apa.org/cognition

Andreassen, J., Eileraas, M., Herrera, L. C., & Noori, N. S. (2023). Increase: A dynamic framework towards enhancing situational awareness in cyber incident response. In T. Gjøsæter, J. Radianti, & Y. Murayama (Eds.), *Information technology in disaster risk reduction* (pp. 230–243). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-34207-3_15

Armellin, A., Gaggero, G. B., Cattelino, A., Piana, L., Raggi, S., & Marchese, M. (2023). Integrating ot data in siem platforms: An energy utility perspective. *2023 International Conference on Electrical, Communication and Computer Engineering (ICECCE)*, 1–7. https://doi.org/10.1109/ICECCE61019.2023.10442554

Ashibani, Y., & Mahmoud, Q. H. (2017). Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, *68*, 81–97. https://doi.org/10.1016/j.cose.2017.04.005

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138–151. https://doi.org/https://doi.org/10.1016/j.im.2013.11.004

CISA. (2021). Cyber-attack against ukrainian critical infrastructure [Accessed: 23.05.2024]. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

Dimitrov, W., & Syarova, S. (2019). Analysis of the functionalities of a shared ics security operations center. *2019 Big Data, Knowledge and Control Systems Engineering (BdKCSE)*, 1–6. https://doi.org/10.1109/BdKCSE48644.2019.9010607

Dragos. (2023). Bridging the it-ot cybersecurity gap: Strengthening ot cybersecurity with advanced soc capabilities. https://www.dragos.com/blog/bridge-ot-it-cybersecurity-gap/

Dragos. (2024). Ot cybersecurity: The 2023 year in review. https://hub.dragos.com/hubfs/312-Year-in-Review/2023/Dragos-2023-Year-in-Review-Full-Report.pdf?hsLang=en

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

European Comission. (2024). Cef context broker [Accessed: 24.05.2024]. https://joinup.ec.europa.eu/collection/egovernment/solution/cef-context-broker

Evesti, A., Kanstrén, T., & Frantti, T. (2017). Cybersecurity situational awareness taxonomy. *2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8. https://doi.org/10.1109/CyberSA.2017.8073386

Fink, G. A., & Shulga, Y. (2018). Helping it and ot defenders collaborate. *2018 IEEE International Conference on Industrial Internet (ICII)*, 188–194. https://doi.org/10.1109/ICII.2018.00036

Flick, U. (2022). Setting the agenda – roles of design(ing) in qualitative research. In U. Flick (Ed.), *The sage handbook of qualitative research design* (pp. 1–18). SAGE Publications.

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – a systematic review of the literature. *Computers & Security*, *46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Furrer, F. J. (2022). Safety, security, and risk. In *Safety and security of cyber-physical systems: Engineering dependable software using principle-based development* (pp. 89–186). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-37182-1_4

Habib, M., & Chimsom, C. (2022). Cps: Role, characteristics, architectures and future potentials [3rd International Conference on Industry 4.0 and Smart Manufacturing]. *Procedia Computer Science*, *200*, 1347–1358. https://doi.org/10.1016/j.procs.2022.01.336

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods* (2nd ed.). SAGE Publications.

Hiltz, S. R., & Turoff, M. (1978). *The network nation human communication via computer* (1st ed.). Addison-Wesley.

Humayed, B. A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security — a survey. *IEEE Internet of Things Journal*, *40*, 1802–1831. https://doi.org/10.1109/JIOT.2017.2703172

Kanamaru, H. (2020). Requirements for it/ot cooperation in safe and secure iacs. *2020 59th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE)*, 39–44. https://doi.org/10.23919/SICE48898.2020.9240295

Kayan, B. H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of industrial cyber-physical systems: A review. *ACM Computing Surveys*, *54*, 1–35. https://doi.org//10.1145/3510410

Kitchenham, B., & Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. *2*.

Lévy, P. (1997). *Collective intelligence mankind's emerging world in cyberspace* (1st ed.). Perseus Books.

Lu, T., Lin, J., Zhao, L., Li, Y., & Peng, Y. (2014). An analysis of cyber physical system security theories. *2014 7th International Conference on Security Technology*, 19–21. https://doi.org/10.1109/SecTech.2014.12

Malone, T. W., & Bernstein, M. S. (2015). Handbook of collective intelligence. In T. W. Malone & M. S. Bernstein (Eds.). MIT Press.

Malone, T. W., Laubacher, R., & Dellarocas, C. N. (2009). Harnessing crowds: Mapping the genome of collective intelligence. *MIT Sloan Research Paper No. 4732-09*, 1–20. https://dx.doi.org/10.2139/ssrn.1381502

Matthews, E. D., Arata, H. J., & Hale, B. L. (2016). Cyber situational awareness. *The Cyber Defense Review*, *1*(1), 35–46. Retrieved February 19, 2024, from http://www.jstor.org/stable/26267298

Moore, S. (2021). Gartner predicts by 2025 cyber attackers will have weaponized operational technology environments to successfully harm or kill humans. *Gartner*. https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

Myers, M. D. (1997). Qualitative research in information systems. *MIS Quarterly*, *21*, 241–242. https://doi.org/10.2307/249422

Myers, M. D., & Newman, M. (2007). The qualitative interview in is research: Examining the craft. *Information and Organization*, *17*, 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Niederman, F., & March, S. (2019). The "theoretical lens" concept: We all know what it means, but do we all know the same thing? *Communications of the Association for Information Systems*, *44*, 1–33. https://doi.org/10.17705/1CAIS.04401

Nyre-Yu, M., Gutzwiller, R. S., & Caldwell, B. S. (2019). Observing cyber security incident response: Qualitative themes from field research. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *63*(1), 437–441. https://doi.org/10.1177/1071181319631016

Onshus, T., Bodsberg, L., Hauge, S., Jaatun, M. G., Lundteigen, M. A., Myklebust, T., Ottermo, M. V., Petersen, S., & Wille, E. (2022). Security and independence of process safety and control systems in the petroleum industry. *Journal of Cybersecurity and Privacy*, *2*(1), 20–41. https://doi.org/10.3390/jcp2010003

Piggin, R. S. H., & Boyes, H. A. (2015). Safety and security — a story of interdependence. *10th IET System Safety and Cyber-Security Conference 2015*, 1–6. https://doi.org/10.1049/cp.2015.0292

Pöyhönen, J., Rajamäki, J., Nuojua, V., & Lehto, M. (2021). Cyber situational awareness in critical infrastructure organizations. In T. Tagarev, K. T. Atanassov, V. Kharchenko, & J. Kacprzyk (Eds.), *Digital transformation, cyber security and resilience of modern societies* (pp. 161–178). Springer International Publishing. https://doi.org/10.1007/978-3-030-65722-2_10

Ragin, C. C., & Amoroso, L. M. (2019). *Constructing social research* (3rd ed.). SAGE Publications.

Sarker, S., Xiao, X., Beaulieu, T., & Lee, A. S. (2018). Learning from first-generation qualitative approaches in the is discipline: An evolutionary view and some implications for authors and evaluators (part 1/2). *Journal of the Association for Information Systems*, *19*, 752–774. https://doi.org/10.17705/1jais.00508

Sarkis-Onofre, B. R., Catalá-López, F., Aromataris, E., & Lockwood, C. (2021). How to properly use the prisma statement. *Systematic Reviews*, *10*, xiii–xxiii. https://doi.org/10.1186/s13643-021-01671-z

Scopus. (n.d.). Analyze search results: Documents by year [Accessed: 02.06.2024]. https://www.scopus.com/term/analyzer.uri?sort=plf-f&src=s&sid=cd25d905e425e97f8c4a59e159040801&sot=a&sdt=

a&sl=277&s=%28ALL%28%22operational+technology%22+OR+ot%29+AND+ALL%28%22security+operation+center%22+OR+%22security+operations+center%22+OR+%22security+operation+centers%22+OR+%22security+operations+centers%22+OR+soc%29+AND+ALL%28%22incident+response%22%29+AND+ALL%28%22cyber+situational+awareness%22+OR+%22cyber+situation+awareness%22%29%29&origin=resultslist&count=10&analyzeResults=Analyze+results

Shafi, Q. (2012). Cyber physical systems security: A brief survey. *2012 12th International Conference on Computational Science and Its Applications*, 146–150. https://doi.org/10.1109/ICCSA.2012.36

Smith, R., Janicke, H., He, Y., Ferra, F., & Albakri, A. (2021). The agile incident response for industrial control systems (air4ics) framework. *Computers & Security*, *109*, 102398. https://doi.org/10.1016/j.cose.2021.102398

Stake, R. E. (1995). *The art of case study research*. SAGE Publications.

Steyvers, M., & Miller, B. (2015). Cognition and collective intelligence. In T. W. Malone & M. S. Bernstein (Eds.), *Handbook of collective intelligence* (1st ed., pp. 119–132). MIT Press.

Tadda, G. P., & Salerno, J. S. (2010). Overview of cyber situation awareness. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.), *Cyber situational awareness: Issues and research* (pp. 15–35). Springer US. https://doi.org/10.1007/978-1-4419-0140-8_2

Telenor. (n.d.). Telenor sikkerhetssenter. https://www.telenor.no/bedrift/sikkerhetstjenester/sikkerhetssenter/

The Norwegian National Security Authority. (2024). Risiko 2024. https://nsm.no/regelverk-og-hjelp/rapporter/risiko-2024

Thomas, J., & Harden, A. (2008). Methods for the thematic synthesis of qualitative research in systematic reviews. *BMC Medical Research Methodology*, *8*. https://doi.org/10.1186/1471-2288-8-45

Tight, M. (2022). Designing case studies. In U. Flick (Ed.), *The sage handbook of qualitative research design* (pp. 399–413). SAGE Publications.

Tuptuk, N., & Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, *47*, 93–106. https://doi.org/10.1016/j.jmsy.2018.04.007

Vielberth, M., Bohm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE*, *8*, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514

Vincente, K. J., Roth, E. M., & Mumaw, R. J. (2001). How do operators monitor a complex, dynamic work domain? the impact of control room technology. *International Journal of Human-Computer Studies*, *54*, 831–856. https://doi.org/10.1006/ijhc.2001.0463

Web of Science. (n.d.). Analyze results, bar chart of publication years [Accessed: 02.06.2024]. https://www.webofscience.com/wos/woscc/analyze-results/be83eebf-4d21-4bcb-b0ab-915ac5c5736b-ef18b235

Webster, B. J., & Watson, R. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, *26*, xiii–xxiii. https://www.jstor.org/stable/4132319

Williams, T. J. (1994). The purdue enterprise reference architecture. *Computers in Industry*, *24*(2), 141–158. https://doi.org/10.1016/0166-3615(94)90017-5

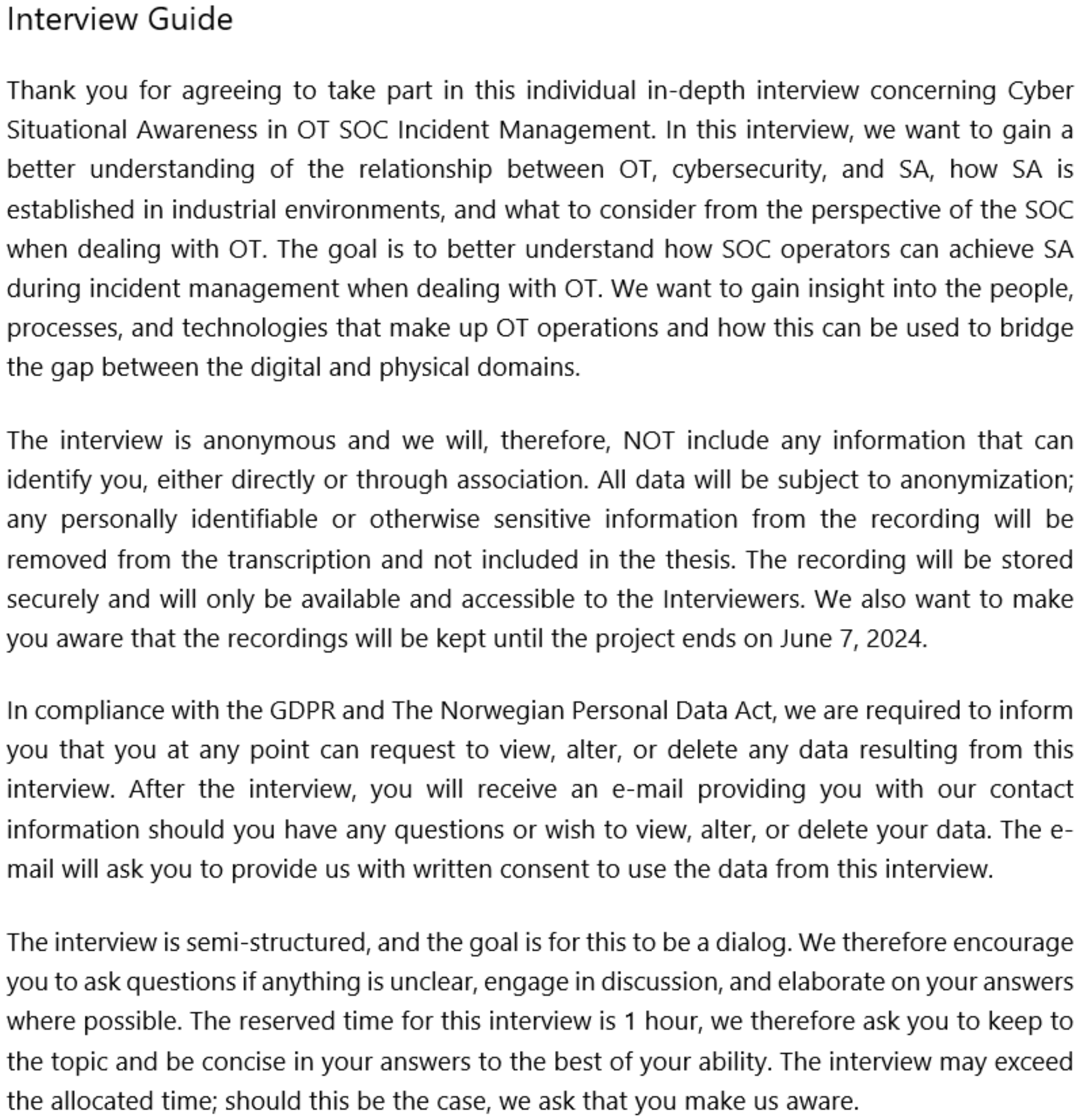
Woolley, A. W., Aggarwal, I., & Malone, T. W. (2015). Collective intelligence in teams and organizations. In T. W. Malone & M. S. Bernstein (Eds.), *Handbook of collective intelligence* (1st ed., pp. 143–160). MIT Press.

Xiao, B. Y., & Watson, M. (2017). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, *39*, 93–112. https://doi.org/10.1177/0739456X17723971

Yin, R. K. (2018). *Case study research and applications design and methods* (6th ed.). SAGE Publications.

Appendix A

Interview Guide



Interview Guide

Thank you for agreeing to take part in this individual in-depth interview concerning Cyber Situational Awareness in OT SOC Incident Management. In this interview, we want to gain a better understanding of the relationship between OT, cybersecurity, and SA, how SA is established in industrial environments, and what to consider from the perspective of the SOC when dealing with OT. The goal is to better understand how SOC operators can achieve SA during incident management when dealing with OT. We want to gain insight into the people, processes, and technologies that make up OT operations and how this can be used to bridge the gap between the digital and physical domains.

The interview is anonymous and we will, therefore, NOT include any information that can identify you, either directly or through association. All data will be subject to anonymization; any personally identifiable or otherwise sensitive information from the recording will be removed from the transcription and not included in the thesis. The recording will be stored securely and will only be available and accessible to the Interviewers. We also want to make you aware that the recordings will be kept until the project ends on June 7, 2024.

In compliance with the GDPR and The Norwegian Personal Data Act, we are required to inform you that you at any point can request to view, alter, or delete any data resulting from this interview. After the interview, you will receive an e-mail providing you with our contact information should you have any questions or wish to view, alter, or delete your data. The e-mail will ask you to provide us with written consent to use the data from this interview.

The interview is semi-structured, and the goal is for this to be a dialog. We therefore encourage you to ask questions if anything is unclear, engage in discussion, and elaborate on your answers where possible. The reserved time for this interview is 1 hour, we therefore ask you to keep to the topic and be concise in your answers to the best of your ability. The interview may exceed the allocated time; should this be the case, we ask that you make us aware.

Person

1. What is your current professional role and experience in the field you work in?
2. What are your daily work tasks/responsibilities?
3. How would you characterize your organizations type of business activities?
4. What is your relationship with Operational Technology and Cybersecurity?

Situational Awareness

1. Are you familiar with Situational Awareness or Cyber Situational Awareness and what do they mean to you?

   SA & CSA Explanations

   Situational Awareness is a term concerned with an individual's state of knowledge of a situation, or their ability to perceive, understand, and effectively respond to said situation. Situational Awareness is made up of three different stages: The first is for the individual to perceive or collect information about the situation, asking "What are the current facts?". The second stage is for the individual to interpret and understand the information, asking "What is actually going on?". The third stage is using the information and understanding of the situation to predict what could happen, asking: "What is most likely to happen if…?". Once an individual has achieved some level of Situational Awareness, he/she uses it to as a foundation on which to make a decision before some action is performed. As an example, a firefighter turning up to a fire will first observe the situation and collect information, then the firefighter will apply his training, experience, and opinions on the information to understand what is going on. Then the firefighter will use his understanding to predict future scenarios, using this information to select the next course of action to best solve the situation. Cyber Situational Awareness is a term mainly used in IT security which is SA limited to digital technologies and networked systems, or the "cyber" environment. Meaning that Cyber Situational Awareness is Situational Awareness applied in the digital domain.

2. What is your understanding of / thoughts on the concept of situational awareness in cyber incident response / cyber incident management / cybersecurity operations?

Operational Technology

1. Based on a sector you're familiar with, such as Oil & Gas, power generation, or manufacturing, or from a general perspective, what can you tell us about how OT environments are operated and managed?
2. What can you tell us about industrial control centers?
3. How does a control center operator establish situational awareness?
4. How is an adverse event handled in OT environments, what is the Standard Operating Procedure?
5. What do you know about cyber-vulnerabilities in OT?
6. In your opinion, what are the most prominent challenges related to cybersecurity incidents in OT environments?

Security Operations Center & Incident Management

1. What are your thoughts on cybersecurity monitoring of OT environments and situational awareness in a Security Operations Centers?
2. What would you do, or what is the SOP for incident management in a cybersecurity incident in an OT environment?
3. How can we correlate cyber events to events in the physical world?
4. Let's say you work in a remote monitoring facility, and you receive an alert that an adverse event has occurred, what information do you require, and from where, to be able to make an adequate decision?
5. Which aspects or characteristics in OT have the biggest impact on Cyber Situational Awareness, why?
6. In the event of a cybersecurity incident in an OT environment, what is the chain of responsibility, who gets contacted?
7. Within your experience how is and what information is typically shared within an OT hierarchy chain, regarding an operational anomaly effecting a process?
8. What requirements would you set for a Managed Security Service Provider or Security Operations Center that is going to monitor and respond to cybersecurity-incidents in OT infrastructure?