Østfold University College

MASTER'S THESIS

Educating ICS Cybersecurity Professionals
A Comparative Study of Graduate Level Curricula
& Industry Needs

Stine Aurora Mikkelsplass
15.06.2023

Master in Applied Computer Science
The Faculty of Computer Science, Engineering and Economics

Educating ICS Cybersecurity Professionals

A Comparative Study of Graduate Level Curricula and Industry Needs

Master Thesis in Applied Computer Science

Stine Aurora Mikkelsplass

Department of Computer Science and Communication
Østfold University College
Halden
15th June 2023

Abstract

Industrial Control Systems (ICS) present unique and complex challenges in the evolving cybersecurity landscape. The convergence of Information Technology (IT) and Operational Technology (OT) domains has underscored the need for a comprehensive understanding of how these disciplines intersect within ICS. This study aims to delve into the complexities of IT and OT collaboration in the context of ICS cybersecurity.

To begin the study, a comprehensive curriculum map of the Graduate Reference Curriculum for Software Engineering (GSwE2009) and the Graduate Reference Curriculum for Systems Engineering (GRCSE) is performed to uncover potential gaps and overlaps in the educational frameworks of these domains. It reveals the differences between knowledge acquisition and application within the IT and OT fields.

Next, interviews were conducted with experienced professionals from IT and OT backgrounds using a qualitative approach to gather in-depth, experiential insights about their collaboration in real-world ICS environments. The discussions revealed intriguing aspects of their respective habitus, the ingrained behaviours, attitudes, and dispositions nurtured through shared experiences and environments. The findings have been analysed in the light of Bourdieu's concept of habitus, illuminating how these professionals navigate the intricacies of ICS cybersecurity and how their collaborative dynamics shape the outcomes.

This thesis unveils that while the IT and OT domains each bring distinct competencies, fostering effective collaboration between them is paramount for enhancing ICS cybersecurity. It underscores the need for a paradigm shift, moving from a silo approach to a collaborative framework where knowledge and skills from both disciplines can be applied collaboratively. In addition, this study demonstrates the importance of cross-disciplinary competencies and mutual understanding between IT and OT professionals.

Acknowledgements

I would like to thank my supervisor Prof. Ricardo Colomo-Palacios at Østfold University College, and my co-supervisor John Eidar Simensen at the Institute for Energy Technology, for their advice, discussions and support on this report. Thanks to Bjørn Axel Gran and Per-Arne Jørgensen for allowing me to complete my master's degree while working at IFE. In addition, I would like to thank my colleagues for their encouragement along the way, and especially Sizarta for his help in completing this report.

More than anything, I would like to thank my family for their patience and support and for motivating me along the way. To my husband Anoop, for his love and care, and to my kids Oliver and Edwin, who fill my life with joy and laughter.

Preface

Cybersecurity is about people. Humans are the central component of performing operational, tactical and strategic actions and decisions. Risk analyses, security measures, and system security are all performed for, and by, people. It is also people who attempt to circumvent security measures, either intentionally or unintentionally. Though humans are often regarded as the weakest link in cybersecurity, there is something to be said about how cybersecurity issues and challenges are communicated between cybersecurity professionals and other personnel, as well as to society as a whole. Language matters, and cybersecurity semantics are far from a *lingua franca*.

Having previous degrees in both computer engineering and cultural studies, this thesis was explored, analysed and discussed from an interdisciplinary perspective. It was written while I worked as an engineer and researcher at the Institute for Energy Technology, an environment that houses a diversity of academic disciplines and people. This provided me with the ideal environment to contemplate how understanding and communication create the foundation for cooperation, the key to success in any endeavour.

This thesis aims to explore industrial cybersecurity in the context of *people, processes and technology*, the fundamental basis of any industrial environment.

Stine Aurora Mikkelsplass
Halden, 15th June 2023

Contents

List of Figures

List of Tables

Acronyms

AI Artificial Intelligence. 7

CIO Chief Information Officer. 36

CISO Chief Information Security Officer. 1

CPS Cyber-Physical Systems. 1

GRCSE Graduate Reference Curriculum for Systems Engineering. 7, 12, 13, 23, 45

GSwE2009 Graduate Software Engineering 2009: Curriculum Guidelines for Graduate Degree Programs in Software Engineering. 7, 12, 13, 23, 45

HMI Human-Machine Interface. 6

ICS Industrial Control System. 1, 5, 7, 14

IDS Intrusion Detection System. 7, 40

IFE Instiute for Energy Technology. 15, 53

IIoT Industrial internet of things. 6

INCOSE International Council on Systems Engineering. 2

IT Information Technology. 1, 5

KA Knowledge Area. 8, 12, 13, 23

ML Machine learning. 7, 27

OT Operational Technology. 1, 5

PLC Programmable logic controller. 6

QCA Qualitative Content Analysis. 17, 35

RTU Remote Terminal Unit. 6

SaSIWG Systems and Software Interface Working Group. 2

SCADA Supervisory Control and Data Acquisition. 6

SE Systems Engineering. 1, 7, 14

SEBoK Systems Engineering Body of Knowledge. 13

SOC Security Operations Centre. 1, 38, 48

SwE Software Engineering. 1, 7, 14

SWEBOK Software Engineering Body of Knowledge. 13

Chapter 1

Introduction

Fundamental support functions and services in modern society, such as water treatment, transportation, and energy systems, rely upon Industrial Control System (ICS). A standard ICS was originally a proprietary, isolated entity with specialised hardware and software significantly different from traditional Information Technology (IT) systems. Physically, these components were secure and not connected to IT networks. As ICS adopted IT solutions for enhanced connectivity and remote access, their resemblance to IT systems grew (Stouffer et al., 2015).

While ICS shares many fundamental characteristics with traditional information processing systems, the differences arise because logic executing in ICS directly affects the physical world. It is important to note that these characteristics include significant risks to human health and safety, severe environmental damage, serious financial issues such as production losses, negative effects on a nation's economy, and compromises of proprietary information and significant financial issues. ICS have unique performance and reliability requirements and often utilise operating systems and applications that may be considered unconventional to typical IT personnel (Stouffer et al., 2015).

Unlike ICS cybersecurity, IT cybersecurity has a long history of frameworks, guidelines, and standards for managing its systems. As a result, the recruitment and organisation of professionals for ICS cybersecurity teams is often the responsibility of IT professionals, such as information security managers or Chief Information Security Officer (CISO) (Michalec et al., 2022; Stouffer et al., 2015). Fortinet (2022) reports that 52% of OT security professionals state that all monitoring and tracking of OT activities is done by the same Security Operations Centre (SOC) that safeguards a company's information technology, i.e., IT professionals. The same report indicates that 79% of OT security professionals anticipate that OT security will soon fall under the CISO responsibilities in the near future, further underlining the importance of IT professionals in ICS security. Consequently, IT professionals are crucial for successfully implementing and managing ICS security, and their involvement in this process will likely increase as ICS environments become increasingly digitised.

As these systems become more complex and interdependent, there is a need for cybersecurity professionals who understand both the IT and the Operational Technology (OT) environment. Recent literature states that there currently is a lack of skill and competence in this area, as well as significant challenges related to educating and developing the workforce needed to secure critical industrial systems (Corallo et al., 2022; Kuttolamadom et al., 2020; Malatras et al., 2019; Maleh, 2021; Ngambeki et al., 2022; Siemers et al., 2021).

Software is a fundamental part of modern engineering systems, also called Cyber-Physical Systems (CPS). As such, Software Engineering (SwE) and Systems Engineering (SE) are both fundamental to the maintenance and development of complex systems (Pyster, Adcock et al., 2015;

Sheard et al., 2019). However, despite their significant roles in the fast-developing industry, the relationship between SwE and SE is not well defined (Pyster, Adcock et al., 2015). This issue has been debated since the 1990s (Armstrong & Pyster, 1997; Wray, 1993), and as recently as 2018, the International Council on Systems Engineering (INCOSE) started a working group exclusively to meet these challenges, the Systems and Software Interface Working Group (SaSIWG) (Sheard. et al., 2018a).

Research Questions

The work presented in this thesis aims to contribute to understanding the industry needs and challenges in ICS cybersecurity compared to the competence provided by graduate level curricula. The research questions are as follows:

RQ1: What are the skills and competencies required for ICS cybersecurity professionals, and how do they align with the graduate curriculum for IT and OT professionals?

RQ2: What are the industry needs for skills and competencies in ICS cybersecurity, and how do IT-OT teams collaborate in the industry today?

RQ3: Identify potential gaps between the industry and academia by comparing findings from RQ1 and RQ2.

RQ1 focuses on the skills and competencies required for ICS cybersecurity professionals and how they align with graduate curriculums for IT and OT professionals. Interview questions related to participants' years of cybersecurity experience, educational background, and queries about the typical tasks for IT, OT, and IT-OT cybersecurity roles, as well as typical skills and competencies for these roles, provide the data for RQ1. It is further enhanced by the participant's view of the structure of ICS cybersecurity education and the essential skills required in their company. This question also explores how and when IT and OT personnel collaborate, further augmenting the insights for RQ1.

RQ2 seeks to understand the industry's needs for skills and competencies in ICS cybersecurity and how IT-OT teams collaborate in the industry today. Almost all interview questions, except those solely focused on the individual's background, contribute to RQ2. Specifically, questions about the participant's work domain and role, the size of their company and cybersecurity team, and the different roles within their team provide an organisational perspective. These, combined with queries about typical tasks and skills for IT, OT, and IT-OT roles and how they collaborate, give an overview of the industry's needs and patterns.

Lastly, RQ3 aims to identify potential gaps between industry and academia by comparing findings from RQ1 and RQ2. This research question can be addressed based on the interview questions regarding the company's size, the number of cybersecurity workers, the roles within the cybersecurity team, and the tasks and skills associated with these roles. This question and the participants' perspectives regarding the ideal structure of ICS cybersecurity education and the collaboration between IT and OT personnel can help identify potential gaps in academia's preparation of cybersecurity professionals for the industry.

Thesis Outline

Chapter 2 provides background to the thesis and address the complexities of ICS cybersecurity, the software and systems engineering currilucum and related work.

Chapter 3 provides the methodology applied to answer the research questions. This covers comparison of the curriculum's for IT and OT, performing semi-structured interviews with ICS cybersecurity professionals to identify the industry perspectives, and how these relates habitus to provide insight into subsconsious patterns of behaviour and practices.

Chapter 4 presents the results from the curriculum mapping organised in cybersecurity, machine learning, soft skills, and systems engineering.

Chapter 5 present the results from the semi-structure interviews with ICT sybersecurity professionals.

Chapter 6 discuss the findings obtained from the curriculum mapping exercise and the in-depth semi-structured interviews with experienced cybersecurity professionals.

Chapter 7 summarise and conclude the research conducted in this thesis and propose future work.

Appendix A provides a manuscript submitted to *International Journal of Human Capital and Information Technology Professionals*[1] (IJHCITP) early 2023 and is currently under review. The article is based on the work presented in Chapter 4.

Appendix B provides the information and consent form applied for the interviews.

[1] https://www.igi-global.com/journal/international-journal-human-capital-information/1152

Chapter 2

Background

During the onset of the digital era, an incident occurred which forever changed the way we perceived interconnected systems - the Morris Worm of 1989. This was the first recorded cybersecurity crime, according to the FBI[1], and it serves as a wake-up call to the growing vulnerabilities associated with digital networks. An individual named Robert Morris created a self-replicating program known as the Morris Worm. The purpose of the attack was not malicious but rather to measure the magnitude of cyberspace. However, it spiralled out of control, resulting in the infecting of thousands of computers and the slowing down of networks[2].

During this period, Industrial Control System (ICS) and Operational Technology (OT) - systems crucial to the operation of factories, power plants, and other infrastructure - were largely disconnected from these early Internet versions. In this manner, they remained unaffected by the numerous security vulnerabilities and attacks that plagued the Information Technology (IT) industry. In the early 2000s, a change began to take place. Industries were enticed to connect previously isolated OT systems by the promise of system interconnectivity, coupled with the possibility of efficient data sharing and analysis. While the evolution brought with it a number of benefits, it also exposed these systems to a growing number of cyber threats (Murray et al., 2017).

Meanwhile, IT cybersecurity has developed into a sophisticated and nuanced discipline due to an escalating arms race with hackers and other malicious entities. It was developed from the ground up with an understanding of the IT world, and tailored to meet interconnected computer systems' unique requirements and vulnerabilities.

The OT cybersecurity sector has to catch up with protocols, strategies, and measures developed with IT systems in mind being retrofitted to OT systems[3]. In addition to creating a significant and persistent gap between IT and OT cybersecurity, these disparate histories and needs also resulted in cultural and conceptual differences. Understanding and bridging this gap has become increasingly important in the increasingly interconnected digital landscape of the 21st century.

2.1 The Industrial Control System

This section provides background on the complexities of ICS cybersecurity, the software and systems engineering curriculum and related work.

[1] https://www.fbi.gov/history/famous-cases/morris-worm
[2] https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/
[3] https://www.csoonline.com/article/3697730/adding-the-operation-focus-to-ot-security.html

Technological advances in mechanics, electricity, and digital technology have driven the previous three industrial revolutions (Pereira et al., 2017). The Fourth Industrial Revolution (Industry 4.0) refers to the current technological progress across industries. Industry 4.0 describes

> *"the organisation of production processes based on technology and devices autonomously communicating with each other along the value chain: a model of the 'smart' factory of the future where computer-driven systems monitor physical processes."* (Smit et al., 2016, p. 20)

The cornerstone of digital transformation in Industry 4.0 is the interconnection of IT and OT. With the emergence of the Industrial internet of things (IIoT), industries have found new ways to manage, maintain, and further develop their operations (Corporation, 2020). Examples of this include but are not limited to extensive data collection from the OT environment, remote monitoring of operations, and optimising operations through automation (Corporation, 2020; Lee, 2018).

IT and OT Interconnection

Industrial control systems are traditionally associated with technology such as Programmable logic controller (PLC), sensors, actuators, Human-Machine Interface (HMI) and Remote Terminal Unit (RTU)s. OT devices are built to operate in industrial settings and harsh environments, intended for 20+ years without regular updates and maintenance. Safety has been the critical driver in OT design principles, a prerequisite to protecting people, processes, and systems (Joint Task Force Transformation Initiative, 2011). ICS often rely on continuous uptime, and therefore dependability and reliability are the main drivers of OT devices. In contrast, IT is built for continuous hardware and software updates (Bigelow & Lutkevich, 2021).

Cybersecurity

Historically, industrial systems and networks have been considered isolated and "air-gapped" from the outside world. It has been argued that cyber security is of no concern for ICS. However, events such as the Stuxnet attack in 2010 and the Havex attack in 2013 (Hemsley & Fisher, 2018) prove that ICS environments are not as isolated as once thought. As the interconnection of IT- and OT systems allows for new opportunities, it also introduces new threats to the industrial environment. The adoption of smart sensors and the development of the IIoT has opened for increased connectivity in ICS environments, as the IIoT function as a bridge between IT and OT, enabling industrial networks to be accessed through the Internet (Corporation, 2020).

In recent years, there have been several noticeable cyber-attacks on OT environments where attackers have exploited IT vulnerabilities to access OT technology. For instance, in the Ukraine April 2022 attacks, a hacker group believed to have strong ties to the Russian Chief Intelligence Office (GRU) launched a series of malware to disrupt the Ukrainian power grid (Zorz, 2022). This attack coincided with Russia's invasion of Ukraine. The attack on the Ukrainian power grid is an example of a threat actor exploiting this by attacking OT systems through IT vulnerabilities. The attack started by hacking into the IT network, where the attacker managed to gain access to the ICS network ('Industroyer2', 2022). Most recently, the AI Chatbot ChatGPT has been found to aid in the development of malware for Supervisory Control and Data Acquisition (SCADA) systems (CYFIRMA, n.d.; Greco, 2023) lowering the threshold for skill and competence needed to deploy attacks against the ICS environment.

Machine Learning

With increased connectivity and extensive use of smart sensors, it is possible to gather vast amounts of data from ICS environments. This development supported the creation of several big data applications and Machine learning (ML) approaches for industries to use these data (Gan et al., 2021). Machine learning models, including Artificial Intelligence (AI), can quickly sort through vast data points with effective decision-making capabilities on real-time data. Machine learning methods and artificial intelligence techniques have become increasingly common within specialised ICS security tools and Intrusion Detection System (IDS)s. For instance, ML algorithms are frequently promoted as a key security feature of IDSs and other security tools (Sarker, 2021) to identify patterns that indicate abnormal processes or network data behaviour.

As the digitisation of ICS poses new challenges on how to collect, sense-make and apply these data, ML is one of the key applications to aid in the management and sensemaking of large amounts of data in Industry 4.0 (Sarker, 2021). ML models have adapted swiftly to the increasing amount of available data. Not only are ML techniques used to sense-make data for business value, but it also extensively used for cybersecurity monitoring and anomaly detection in Industrial Control System (ICS) (Teixeira et al., 2018).

2.1.1 System & Software - the fundamentals of modern industrial environments

Industrial environments have significantly evolved over the years, with Software Engineering (SwE) and Systems Engineering (SE) impacting this progression. Traditionally, system engineers were quite prominent, given their focus on devising, implementing, and maintaining complex, large-scale systems (Sheard et al., 2019). This typically required a comprehensive, multi-disciplinary understanding of various interrelated components, such as hardware, software, data, humans, and policies, mandating a systems-oriented approach (Pyster, Adcock et al., 2015). However, the rise of software's dominance in systems' functionality resulted in software engineering becoming a well-known industry term. In the mid-twentieth century, when the complexity and integrality of software within systems necessitated the establishment of software engineering as a separate discipline (Sheard, 2014).

System engineering and software engineering play an integral role in contemporary industrial environments. Modern systems are characterised by elaborate hardware and complex software, which requires synergistic collaboration between both disciplines. As a result of the understanding that software has evolved from a supporting component to an integral component of systems, often containing significant operational functions, this collaborative approach is necessary (Wade et al., 2022).

Cyberattacks have grown exponentially over the last several decades as systems and software have become increasingly connected and accessible remotely. In response, new disciplines, such as ICS cybersecurity, have developed (Karampidis et al., 2019).

2.2 The Software Engineering and Systems Engineering Curricula

The Graduate Software Engineering 2009: Curriculum Guidelines for Graduate Degree Programs in Software Engineering (GSwE2009) (Pyster, 2009) and the Graduate Reference Curriculum for Systems Engineering (GRCSE) (Pyster, Olwell et al., 2015) are designed as guidelines for their respective graduate degree programs. They were created to standardise the education for software engineers and systems engineers across educational institutions and to ensure the quality of education for graduating students.

Both curricula have developed a Core Body of Knowledge, building on the Software Engineering Body of Knowledge (SWEBOK) (Bourque & Fairley (eds), 2014) and the Systems Engineering Body of Knowledge (SEBoK) (SEBoK Editorial Board, 2021), from where they have identified *Core Concepts* or *Fundamental Knowledge* that should be a part of the curriculum for all masters degree graduates within their field. These core topics make up approximately 50% of the curriculum in both cases, while the remaining 50% are dedicated to specialised topics or training. The concepts of the CBOK (SwE) or CorBOK (SE) are grouped into Knowledge Area (KA)), which are further divided into topics and sub-topics. Detailed information about the KAs and topics are found in their own curricula or in the SWEBOK or SEBoK.

The GSwE2009 and GRCSE curricula reflect the expected learning outcomes for graduates within software- and systems engineering. Both SwE and SE curricula use Blooms cognitive levels (Bloom, 1956) to describe the expected comprehension level for graduate students within specific topics of the KAs. To ensure that these levels are comparable, it was first necessary to map how these levels were described within both curricula. The remainder of this section describes the process taken to ensure that Bloom's cognitive levels were comparable between the two curricula.

Model Analysis: Each of the curricula has identified what competence should be associated with the different cognitive levels of Bloom's Taxonomy (Knowledge, Comprehension, Application, Analysis, Synthesis and Evaluation). By identifying core skills and domain-specific focus (core responsibilities given field of study) associated with each competency level for both curricula, it was possible to analyse how the curricula defined competency on a given level. As both curricula use Bloomt's Taxonomy to describe students' expected cognitive level within a certain Knowledge Area, this analysis was relevant to ascertain whether the competence is comparable.

Mapping Design:

1. Identify core skill and educational focus described in Bloom levels of both the SwE and SE curricula.

2. Direction of comparison: identified SwE skills are mapped to identified SE skills.

3. Comparison scale definition: This scale is adapted from previous work (Baldassarre et al., 2012; Sánchez-Gordón & Colomo-Palacios, 2018) and contains the following four sections:

    - Strongly related (●): Learning outcomes (skills) has the most core concepts in common and have many of the same principles for learning outcome.
    - Partially related (◑): Learning outcomes (skills) has the most core concepts in common and have many of the same principles for learning outcome.
    - Weakly related (◔): Learning outcomes (skills) do not have any core concepts in common, but there is an underlying practice that matches an activity that can be found in the SE curriculum.
    - Not related (○): No relationship can be identified.

Mapping Execution: This mapping was performed iteratively. Data from the curricula were detailed in a spreadsheet and analysed to identify the core skill associated with each competency level of Bloom's Taxonomy before the results from the SwE were compared to SE.

Results: This subsection presents the findings from mapping the Bloom cognitive levels of SwE and SE competence levels. Table 2.1 presents how the different levels, *Knowledge* (K), *Comprehension* (C), *Application* (AP), *Analysis* (AN), *Synthesis* (S), *Evaluation* (E), are related. All SwE levels except Synthesis are strongly related to the corresponding level in SE.

Table 2.1: GSwE2009 to GRCSE mapping of competency in associated cognitive levels.

Cognitive Levels		*Software Engineering (SwE)*					
		K	C	Ap	An	S	E
Systems Engineering (SE)	K	●					
	C		●				
	Ap			●			
	An				●		
	S					◑	
	E						●

The skills described in Knowledge, Comprehension, Application, Analysis and Evaluation are practically indistinguishable. The skills associated with Synthesis, however, are only partially related. Whereas the GSwE2009 skills detail competency in design and construction (of applications or systems), the GRCSE level also emphasises prediction (of system behaviour). Neither Synthesis nor Evaluation is used to describe the cognitive levels of any identified topics in either curriculum and is therefore not considered further. The result from this mapping shows that Bloom's cognitive levels from GSwE2009 and GRCSE are comparable for the purpose of this study and are used in Chapter 3.

2.3 Related Work

Previous work has pointed to various reasons why SwE and SE struggle to work together, e.g., that SwE tends to belong to an IT department and SE to an engineering department (McBride et al., 2020; Pyster, Adcock et al., 2015). Without cross-disciplinary communication, understanding, and collaboration, they lack the tools and methods to communicate across disciplines once they enter the workforce. Gjermundrød et al. (2016) suggest that misunderstandings and difficulties working together result from the two groups using different languages and having different goals. However, according to Towhidnejad et al. (2013), GSwE2009 and GRCSE provide a foundation for mutual understanding between SE and SwE. However, current curricula in higher education and a lack of collaboration between disciplines fail to teach this.

A considerable amount of experience in the field of information security provides IT professionals with a clear advantage and responsibility when contributing to the security of ICS. Sheard. et al. (2018a) note that SE professionals are underrepresented in DevOps[4] or SE-dominant projects, resulting in new technologies being developed without sufficient input and leadership from SE professionals. Introducing IT elements into the OT environment highlights security and knowledge gaps on both sides. As IT professionals are not trained in systems engineering, they are unfamiliar with the complexities of ICS environments and OT data. Further, OT personnel do not possess the skills necessary to take preventive security measures to safeguard ICS systems

[4]https://www.bouvet.no/kurs/kategorier/smidig/devops-fundamentals-2-days

(Karampidis et al., 2019). As experts from both fields are essential to the safety and security of ICS (Muscarella et al., 2020), IT and OT professionals must work together to bridge the skill and competence gap, enabling a more effective collaboration by fostering understanding between the two disciplines.

According to research on the ICS cybersecurity skills gap, there is both a gap in the industry and a gap in efforts to standardise curriculum content (Ngambeki et al., 2022). Researchers have identified that communication and teamwork skills, closely followed by a multidisciplinary and dynamic skill set, are of the highest importance for the ICS cybersecurity industry (Azmat et al., 2020; John et al., 2020; Ngambeki et al., 2021; Slayton & Clark-Ginsberg, 2018; Sohime et al., 2020).

Chapter 3

Methodology

To answer the research questions, we will compare the competence of graduates as outlined in the academic curricula with the actual needs of the industry. The first step is performing curriculum analysis to understand what is being taught in the academic settings of software- and systems engineering. The second step is to understand the real-world requirements of the industry, which is captured through semi-structured interviews with industry leaders in ICS cybersecurity. These steps will allow us to map the gap. Figure 3.1 illustrates these steps related to habitus - which can provide insight into subsconsious patterns of behaviour and practices that can uncover dimensions of different roles in the ICS cybersecurity field.

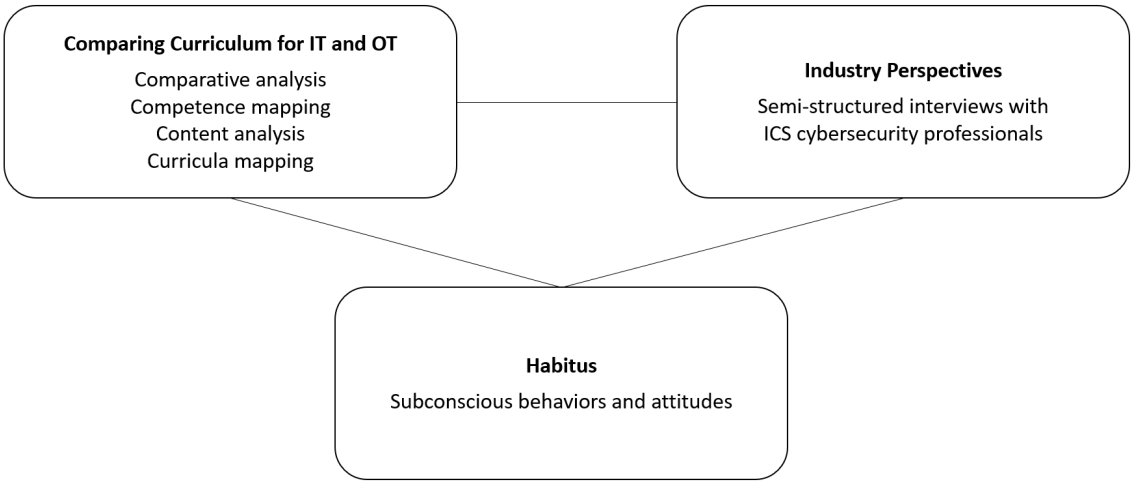


Figure 3.1: Data Triangulation

Comparing curricula (section 3.1): To ensure an accurate, comprehensive understanding of the two curricula, multiple steps will be necessary to compare the software and systems engineering curricula.

Comparative Analysis: Initially, a detailed comparative analysis will be conducted to identify similarities and differences between the two curricula. This analysis will pinpoint common areas of study and areas where curricula diverge.

Competency Mapping: A competency mapping exercise will be conducted following the comparative analysis. This will involve aligning each curriculum's topics and modules with the required skills and competencies in ICS cybersecurity.

Content Analysis: Next, a content analysis will be conducted. Content analysis involves thoroughly examining curriculum content, including learning objectives, teaching methods, and assessment strategies. This analysis will better our understanding of how each curriculum teaches and evaluates different topics.

Curricula Mapping: The final step in the comparative process involves curricula mapping, a visual representation of the curricula that provides a holistic view of the structure, content, and interrelation of different topics within each curriculum.

Interviews (section 3.2): Semi-structured interviews will be conducted with professionals working in the field of ICS cybersecurity. These interviews aim to gain insights into professionals' perspectives on the skills and competencies required in their roles and how they perceive the relevance and applicability of the curricula to their work. Interview data will be analysed using qualitative content analysis.

habitus (section 3.3): habitus, a term coined by sociologist Pierre Bourdieu, refers to ingrained habits, skills, and dispositions individuals develop over time. In the context of this thesis, habitus can provide insights into the subconscious behaviours and attitudes of professionals in the field. This is shaped by their cultural, educational, and social experiences. It can reveal how these factors influence professionals' views on ICS cybersecurity, the curricula, and their roles within the sector.

3.1 Comparing Curricula

This section details the comparative analysis, the competency mapping and the curricula mapping design.

3.1.1 Comparative Analysis

A comparative analysis (Robson, 2011; Walk, 1998) was used to assess the comparability of the software engineering (GSwE2009) and the systems engineering (GRCSE) curricula by evaluating the similarities and differences between the two curricula. As well as identifying overlaps between two curricula, a comparative analysis is used to identify curriculum gaps by comparing the objectives and outcomes of the curricula. This can be determined by examining the topics covered in each curriculum, including the amount of time allocated to each topic and the skills and knowledge required. Several aspects of the curricula were compared in this study, including the structure and sequencing of the courses, the learning outcomes, and their primary objectives.

To understand the similarities and differences between the SwE and SE curricula, the first step was to analyse the curricula. Both curricula have organised their core body of knowledge into Knowledge Area (KA), topics, and subtopics to structure the recommended competencies and skills. Both curricula utilise Bloom's cognitive levels to communicate the expected comprehension level for graduate students within each topic. According to Bloom's Taxonomy of Educational Objectives (Bloom, 1956), there are six levels of learning abilities in the Cognitive Domain. To determine the level of understanding a student should possess at a particular stage in their education, the levels range from memorising facts to evaluating at the highest level: *knowledge*, *comprehension*, *application*, *analysis*, *synthesis*, and *evaluation*.

To ensure that these levels are comparable, a mapping of how these levels were described within both curricula was done before the curricula mapping as described in section 2.2.

3.1.2 Competency Mapping

Competency mapping identifies the competencies required to perform a given job role efficiently. This can be done using a variety of tools or techniques, such as job analysis, task analysis, or through the use of competency frameworks. In this thesis, qualitative mapping describes skills and competencies the student should possess after taking a topic.

To map the desired competency for a given focus area to a topic in the SwE curriculum (GSwE2009), we first identified criteria for skills and competencies within each area. The resources needed to identify these criteria varied between areas, these are presented along with the results in chapter 4. Relevant topics within GSwE2009 were then identified by studying each KA for topics within cyber security, machine learning and soft skills.

3.1.3 Curriculum Mapping

Curriculum mapping is used in this thesis to visually represent the relationship between topics in Graduate Software Engineering 2009: Curriculum Guidelines for Graduate Degree Programs in Software Engineering (GSwE2009) and Graduate Reference Curriculum for Systems Engineering (GRCSE). Curricula mapping is not a straightforward process (Ervin et al., 2013), and a limited number of specific methods have been found in the academic literature. The process followed in this thesis is therefore adapted from previous work (Rawle et al., 2017; Robley et al., 2005a, 2005b; Uchiyama & Radin, 2009; Veltri et al., 2011; Wei et al., 2022). Identifying the relationships between the curricula was an iterative process. We used a comparison scale to determine the relation level once all relationships had been identified. A description of the steps taken follows below:

1. Identify GSwE2009 topics relating to focus areas.

   A detailed analysis of topic information in GSwE2009 and SWEBOK was conducted to identify topics relevant to the development of industry 4.0 skills and competencies. In a spreadsheet, topics whose skills and competencies matched those within either of the focus areas were detailed with information about their topic, which KA they belong to in GSwE2009 as well as the focus area(s) they relate to.

2. Identify related topics in GRCSE.

   The topics detailed in the spreadsheet in the previous step was once again studied in detail and one by one compared to the topics in GRCSE. Both GRCSE and SEBoK was used to find detailed topic information, i.e., skills and competencies related to the topic. An update to the spreadsheet included GRCSE topics with ties to GSwE2009, which resulted in a detailed list of topic relations between the two curricula.

3. Map relations according to the comparison scale. The comparison scale applied in this study is adapted from previous work (Baldassarre et al., 2012; Sánchez-Gordón & Colomo-Palacios, 2018). Four categories are described below, and the symbols for each category are used to present the results in Chapter 4.

   - Strongly related (●): the topic is specially named in the curricula and is classified to one or more of the same Bloom cognitive levels.
   - Partially related (◑): the topic is not specially named, but one or more sub-topics have activities that correlate to activities in the GRCSE curriculum.

- Weakly related (◔): the topic is not specially named, but one sub-topic has activities that can be adapted to an activity in SE curriculum.
- Not related (○): the topic or activity is mentioned, but only a high-level summary is given in SE curriculum. No relationship between competencies can be identified.

4. Create a visual representation of the relationship.

   When all relations were identified, they were organised into visual representations in tables, showing their relation from GSwE2009 to GRCSE and the degree of relationship for each topic. The relations were divided into which focus area they belonged, i.e., one table was created for each focus area. Topics in the category *not related* (○) are visible in the tables but not discussed further as they include only a brief mention or overview of the topics.

3.2 Interview Design and Process

The curricula mapping provides an academic perspective on the challenge of skills and competencies in ICS cybersecurity by understanding how Software Engineering (SwE) and Systems Engineering (SE) students learn and develop in higher education and identifying gaps related to the focus areas. Curriculum analysis allows us to understand what is being taught in software- and systems engineering academic settings. However, to address the gap between academic teaching and industry needs, we need to understand the real-world requirements of the industry. These are captured through semi-structured interviews with industry leaders in ICS cybersecurity. A total of three interviews were held for this project.

3.2.1 Interview Design

Although there is plenty of literature on the ICS cybersecurity skills gap (see section 2.3), no officially agreed-upon curricula, standards, or frameworks for determining the essential skills and competencies exist for ICS cybersecurity. The need for skills and competence in ICS cybersecurity may vary from industry to industry. Therefore a semi-structured interview approach was chosen to gain in-depth insights into the needs of the industry.

Semi-structured interviews are particularly suited to this task because they balance flexibility and consistency (Salkind, 2018). A predefined set of questions guides these interviews to ensure consistency across all interviews and enable comparability of responses. In contrast to fully structured interviews, they allow interviewees to elaborate on their answers and expand upon their perspectives and experiences. Therefore, while there is a clear focus, there is also flexibility to explore emerging themes or unexpected insights. Moreover, semi-structured interviews allow for an in-depth understanding of the complex needs of the ICS cybersecurity field. Industry leaders can provide context for their answers, explain their thinking, and share examples from their experiences, adding depth to the data collected. Using this approach, it is possible to gain a deeper, more nuanced understanding of the competencies required in the industry. The key elements of the semi-structured interviews method are summarised below:

Flexibility and depth: A semi-structured interview allows for greater flexibility than a structured interview. Despite having a predetermined set of questions, an interviewer can diverge from them if necessary. Every ICS is different, and this method allows for exploring interesting

or unexpected avenues that may arise during the interview. As a result of this approach, it is possible to gain a detailed understanding of industry leaders' perspectives on cybersecurity skills and competencies required in Industry 4.0 and how they perceive the preparedness of graduates in software and systems engineering.

Consistency: While providing room for flexibility, semi-structured interviews also maintain consistency across interviews because of the set list of questions. This can be particularly helpful when comparing and analysing responses from different interviewees.

Contextual understanding: Semi-structured interviews provide the opportunity to understand the context of the responses. Industry leaders can explain their answers, share their experiences, and provide examples, which can add depth and richness to the data collected. This could be highly valuable when discussing the complexities and specific needs of the ICS and cybersecurity field.

Addressing the gap: One of this thesis's main objectives is to compare graduates' competence as outlined in the academic curricula with the actual needs of the industry. Semi-structured interviews can provide direct insights into what industry leaders believe are the necessary skills and competencies, thereby addressing this gap.

3.2.2 Interview Process

The selection process intended to select cybersecurity professionals with experience in IT and OT environments, preferably with experience in working with multidisciplinary teams. My co-supervisor and the professional network formed through the Instiute for Energy Technology (IFE) helped identify potential interviewees.

Potential candidates were e-mailed with information about the master's thesis project and provided an online consent form (Appendix B) to complete if they wished to participate. To ensure participant consent and data handling, participants were required to log in with Bank-ID[1] to complete a form on Nettskjema.no[2]. Once the consent form was signed, participants were contacted to set up the interview.

The interviews were conducted on Microsoft (MS) Teams[3] or by telephone. The interviewer explained the study's purpose, the participants' rights to access their data, and how to withdraw from the study at any time. The interview setting was preserved as natural as possible by not using a presentation on MS Teams during the interview. Remote meetings lose many non-verbal communication aspects, and distractions (checking e-mail, a knock on the door, etc.) are more likely. The video window for all attendees would be significantly smaller if a presentation were used, limiting non-verbal communication.

Thirteen open-ended questions were prepared for the interviews, allowing interviewees to share their experiences and perspectives freely. Depending on their responses, follow-up questions were asked. Even though the conversation remained on topic, the interviews, on average, exceeded the allocated time of 35 minutes by 10-20 minutes.

For participants to feel comfortable sharing as much information as possible, no video or audio recording was conducted during any of the interviews. One interview was conducted with a

[1] https://www.bankid.no/privat/

[2] www.nettskjema.no

[3] https://www.microsoft.com/nb-no/microsoft-teams/group-chat-software/

transcriber. The transcriber participated in the introduction but limited contact with the interviewee by turning off video and audio when the interview questions began. The interviewer transcribed the remaining interviews; although transcribing while interviewing somewhat limited the number of notes taken, it also provided me with a more informal setting to conduct the interview.

Ethical considerations

The research conducted in this study complies with the ethical guidelines for human studies[4]. Participant consent, confidentiality, harm avoidance, secure data handling, and honesty in reporting are all included in these guidelines. It was ensured that participants were fully informed of the research objectives, their role, and their rights, including the right to withdraw at any time. To accomplish this, the information was provided in writing ahead of time and repeated orally at the beginning of the interview. Interviews were conducted only after obtaining written consent.

Participants' information was made anonymous and securely stored to protect their privacy. Throughout the study, caution was taken to avoid harm, and a commitment was made to presenting the truth. As cybersecurity is a complex field, all discussions are conducted with sensitivity and respect, understanding that discussions about skills gaps can sometimes be perceived as criticism. Any information shared was handled in a responsible and trust-based manner.

3.2.3 Interview Questions

The interview questions (IQ) presented in Table 3.1 address the objectives highlighted in the research questions. The interview questions were developed within three categories that were decided from the outset. The main purpose of the categories was to ensure that the questions would address various aspects. The first category (IQ1-IQ5), *domain and experience*, aimed to extract information about the participants' education, place of work and cybersecurity experience. The second category (IQ6-IQ11), *state of practice*, intended to gain information about the participants' work environment and examine data related to typical work tasks, IT-OT collaboration and team competencies. The third category (IQ12-IQ13), *skill and competence*, enquires about information related to ICS cybersecurity skills and competencies needed within the participants' current team to gain the participants' input on ICS education and how to up-skill the current workforce.

A systematic mapping of interview questions (IQ) to each research question (RQ) is discussed next (Table 3.1), providing a clear illustration of how the interview protocol was designed to meet the aims of the study.

[4]https://sikt.no/personvernhandbok-forskning

Table 3.1: Mapping of Interview Questions (IQ) to Research Questions (RQs)

IQ	Interview Questions	RQ1	RQ2	RQ3
1.	In which domain do you work?		✓	
2.	What is your current role/title?		✓	
3.	How long have you worked in this role?		✓	
4.	How many years of experience do you have within cybersecurity?	✓		
5.	What is your education?	✓		
6.	How many employees are in your company in total?		✓	✓
7.	How many work in cybersecurity in general?		✓	✓
8.	What type of roles are in your team?		✓	✓
9.	What are the typical tasks for personnel in IT, OT, and IT-OT cybersecurity roles in your team?	✓	✓	✓
10.	What are some typical skills and competencies for these roles?	✓	✓	✓
11.	How and when do IT and OT personnel collaborate?	✓	✓	✓
12.	What are the essential skills and competencies that your company needs within ICS cybersecurity?	✓	✓	✓
13.	In your opinion, how would you structure ICS cybersecurity education, teams, and upskilling of the current workforce in an ideal world?	✓	✓	✓

RQ1: *What are the skills and competencies required for ICS cybersecurity professionals, and how do they align with the graduate curriculums for IT and OT professionals?*

RQ2: *What are the industry needs for skills and competencies in ICS cybersecurity, and how do IT-OT teams collaborate in the industry today?*

RQ3: *Identify potential gaps between the industry and academia by comparing findings from RQ1 and RQ2.*

RQ1 focuses on the skills and competencies required for ICS cybersecurity professionals and how they align with graduate curriculums for IT and OT professionals. RQ2 seeks to understand the industry's needs for skills and competencies in ICS cybersecurity and how IT-OT teams collaborate in the industry today. Lastly, RQ3 aims to identify potential gaps between industry and academia by comparing findings from RQ1 and RQ2. This research question can be addressed based on the interview questions regarding the company's size, the number of cybersecurity workers, the roles within the cybersecurity team, and the tasks and skills associated with these roles.

3.2.4 Analysis Method

Qualitative Content Analysis (QCA) offers an approach for systematically analysing and interpreting the data collected from the interviews (Robson, 2011). QCA is an interpretive method that allows us to delve into the complexities and nuances of the data, providing rich and detailed insights that complement the research questions at hand. The process is illustrated in Figure 3.2 and described in detail below.

1. Preparation: Prepare for the coding process by thoroughly ready through the interview transcriptions, and become familiar with the interview responses and beginning to formulate initial ideas about how to code them.

2. Coding: Next, the text was systematically categorised into distinct codes. These codes function as labels that assign symbolic meaning to the descriptive and inferential data in the transcripts. To ensure the most accurate representation of the data, the coding process was data-driven , and several iterations were made to refine the codes. The codes were documented and arranged in Miro[5], a creative visual platform.

3. Identifying themes: A final step in the coding process is to identify broader patterns or themes in the data. This involves sorting the codes into themes and sub-themes that accurately describe the research phenomenon (Figure 3.3). As with step 2, this process was also iterative.

4. Constructing thematic networks: There have been several iterations before arriving at the final thematic network (Figure 3.4). Once finished, it is then reviewed against the coded extracts and the entire database to ensure that they accurately reflect the meanings evident throughout the data set.

5. Integration and interpretation: Further refinement and naming of themes occur in this section, as well as creating clear definitions for each theme. It is also important to identify the story each theme tells and how it fits in with the overall narrative we are telling about our data. This information is presented in Chapter 5.

[5]https://miro.com

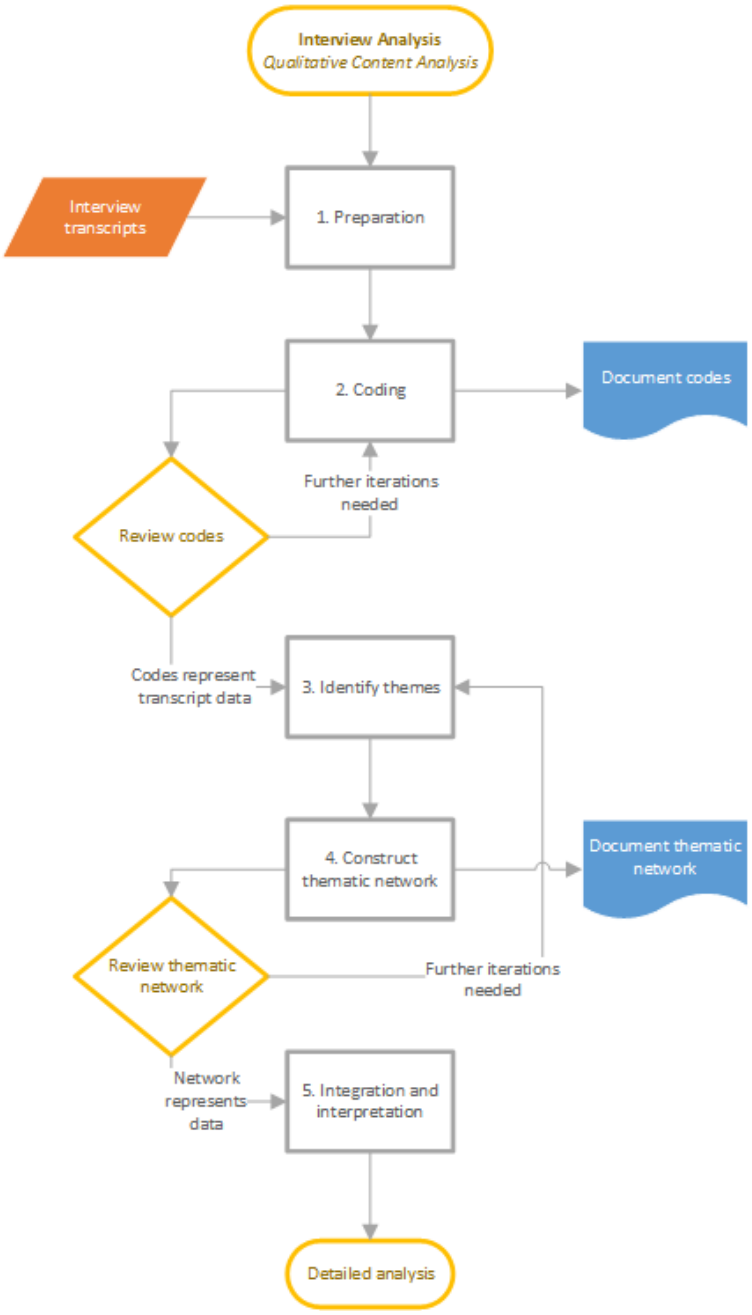


Figure 3.2: Qualitative content analysis process

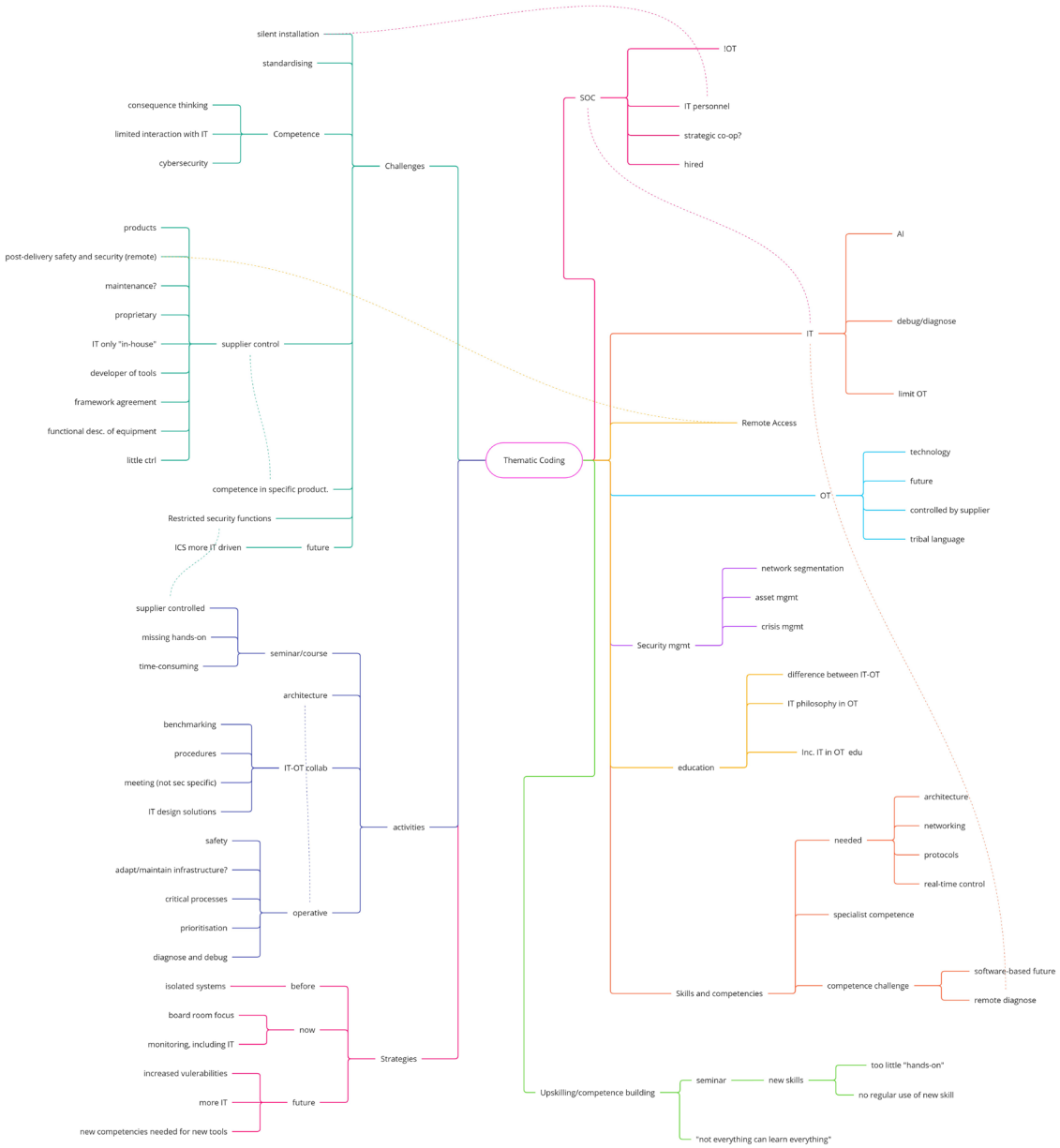


Figure 3.3: Thematic coding process

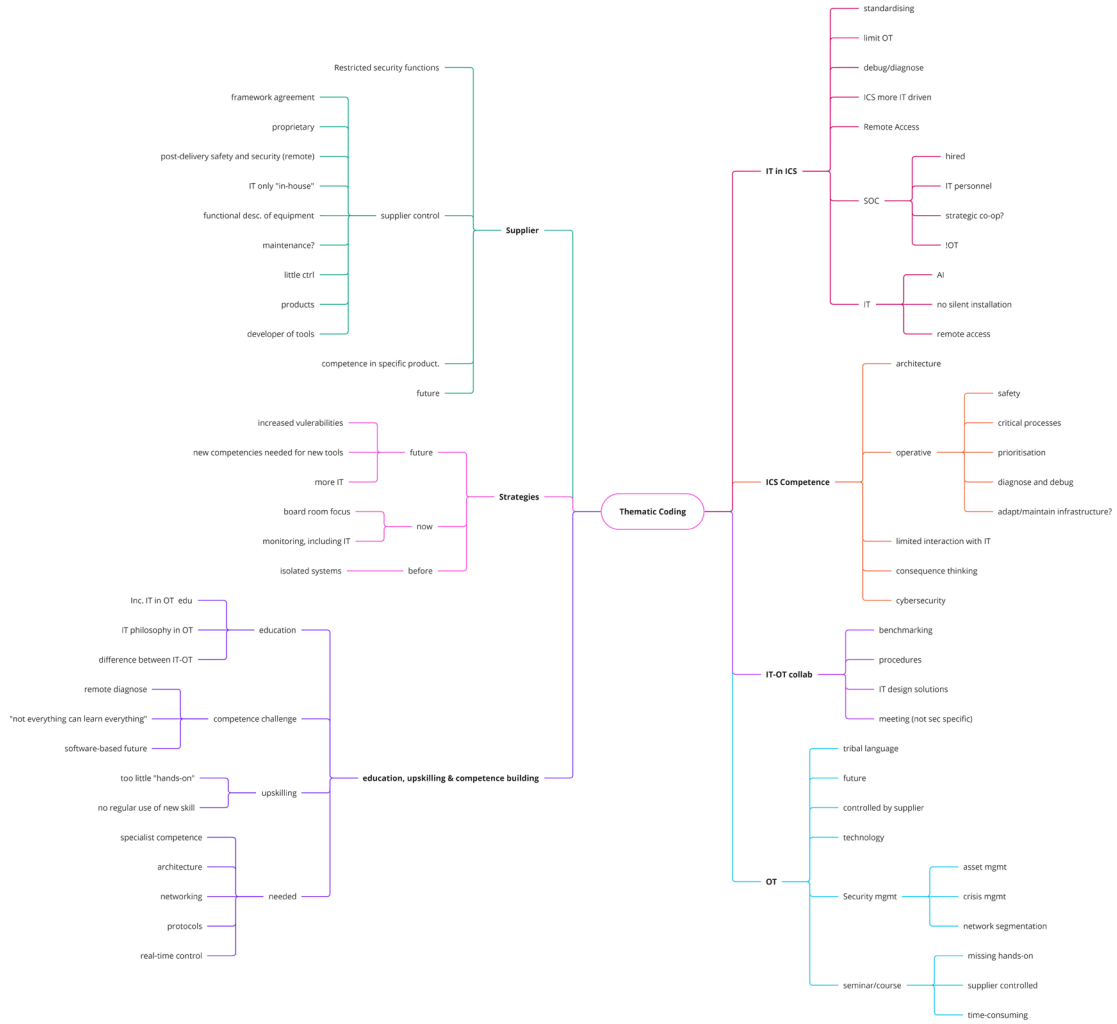


Figure 3.4: Thematic network

3.3 The Human Aspect of ICS Cybersecurity

The science of technology does not exist independently. It heavily draws on other disciplines like mathematics, chemistry, and physics. As technology is developed by and for people, it also includes sociology (Stølen, 2019). This section introduces the concept of *habitus*, used in this thesis to situate ICS cybersecurity within a broader context and explore how education, technology, and culture may contribute to opportunities and challenges.

The value of *habitus* in ICS cybersecurity

The concept of habitus, developed by French sociologist Pierre Bourdieu, encompasses the ingrained behaviours, attitudes, and dispositions individuals develop through shared experiences and environments. This perspective allows a nuanced understanding of how individuals and groups perceive, interact, and respond to their surroundings(Jeon, 2019). In the context of ICS cybersecurity, habitus can provide insight into the behaviours and practices of IT- and OT

professionals within the field. Habitus influences how individuals perceive and handle cyber threats and shapes their interaction with technology and overall approach to cybersecurity.

Including habitus in this thesis offers a perspective on the complex dynamics between two disciplines in the ICS cybersecurity landscape. It can provide a deeper understanding of the intricate interdependencies between technology and its sociocultural environment. This cross-disciplinary approach can address the underlying influences shaping cybersecurity, providing this study with a nuanced view of professionals' behaviours and attitudes (Ramsey, 2023). It explores the evolving interplay of skills, competencies, and interactions within the IT and OT domains. Focusing on these underlying, often subconscious patterns of behaviour and practices can uncover the essential yet implicit dimensions of different roles in the ICS cybersecurity field.

The concept of habitus in this study facilitates a comprehensive understanding of challenges in ICS cybersecurity, providing depth to the analysis beyond surface-level observations. It offers a practical lens to explore the real-world experiences of professionals in the field, thereby contributing to a more effective, context-sensitive approach to addressing ICS cybersecurity challenges.

Challenges, limitations and mitigations

Nevertheless, intertwining technological science with social or cultural science introduces its own set of challenges. The integration adds complexity to the project due to the need for multidisciplinary knowledge and consideration. Furthermore, social and cultural factors often introduce uncertainty and ambiguity, making the outcomes less predictable. There is also a risk of oversimplification or misunderstanding of intricate social or cultural factors, potentially leading to misguided solutions. Utilising the concept of habitus in this study brings particular challenges primarily due to its abstract nature. These challenges will be mitigated through several strategies described below.

Firstly, it is important to possess a robust understanding of the habitus concept and its application within the specific context of ICS cybersecurity. By clearly articulating the theoretical assumptions and defining how the concept is used within the study, the aim is to reduce the risk of bias and provide a more accurate analysis. Using specific examples of behaviours or dispositions that exemplify facets of habitus within ICS cybersecurity will aid in this.

To capture habitus' multi-faceted nature, utilising various types of data, such as insights from semi-structured interviews, previous work, and curriculum mapping results, can increase the depth and validity of the findings (data triangulation). By conducting semi-structured interviews, participants can freely express their experiences, attitudes, and behaviours, providing valuable insights into their habitus. A possible limitation of this study is the small sample size of participants, providing limited knowledge.

Furthermore, an iterative approach to data analysis could be beneficial (Robson, 2011). We can refine and deepen our interpretations by repeatedly revisiting the data, allowing for a more nuanced understanding of participants' habitus.

Finally, reflexivity, or the continual reflection of how our beliefs, experiences, and potential biases may influence our interpretations, is critical to ensuring our findings' validity (Mouzelis, 2008). Our analysis of habitus can be made as objective as possible if we keep these potential biases in check. By applying these strategies, we can effectively navigate the challenges associated with using habitus in our study, ensuring a comprehensive and valid analysis.

Chapter 4

Curricula Mapping

The work presented in this chapter has been submitted as a manuscript to *International Journal of Human Capital and Information Technology Professionals*[1] (IJHCITP) early 2023 and is currently under review. The manuscript is provided in Appendix A.

This chapter presents the results from the curriculum mapping, organised under the following sections: cyber security, machine learning, soft skills, and systems engineering. Figure 4.1 presents the structure of topics, Knowledge Area (KA) and the Core Body Knowledge of the SwE (GSwE2009) and SE (GRCSE) curricula side-by-side. The left presents an overview of KAs within SwE, represented by the letters A through K. The KAs of SE curriculum are on the right side of the figure and categorised in *parts*, corresponding to their location in the CRCSE CorBoK.

[1] https://www.igi-global.com/journal/international-journal-human-capital-information/1152

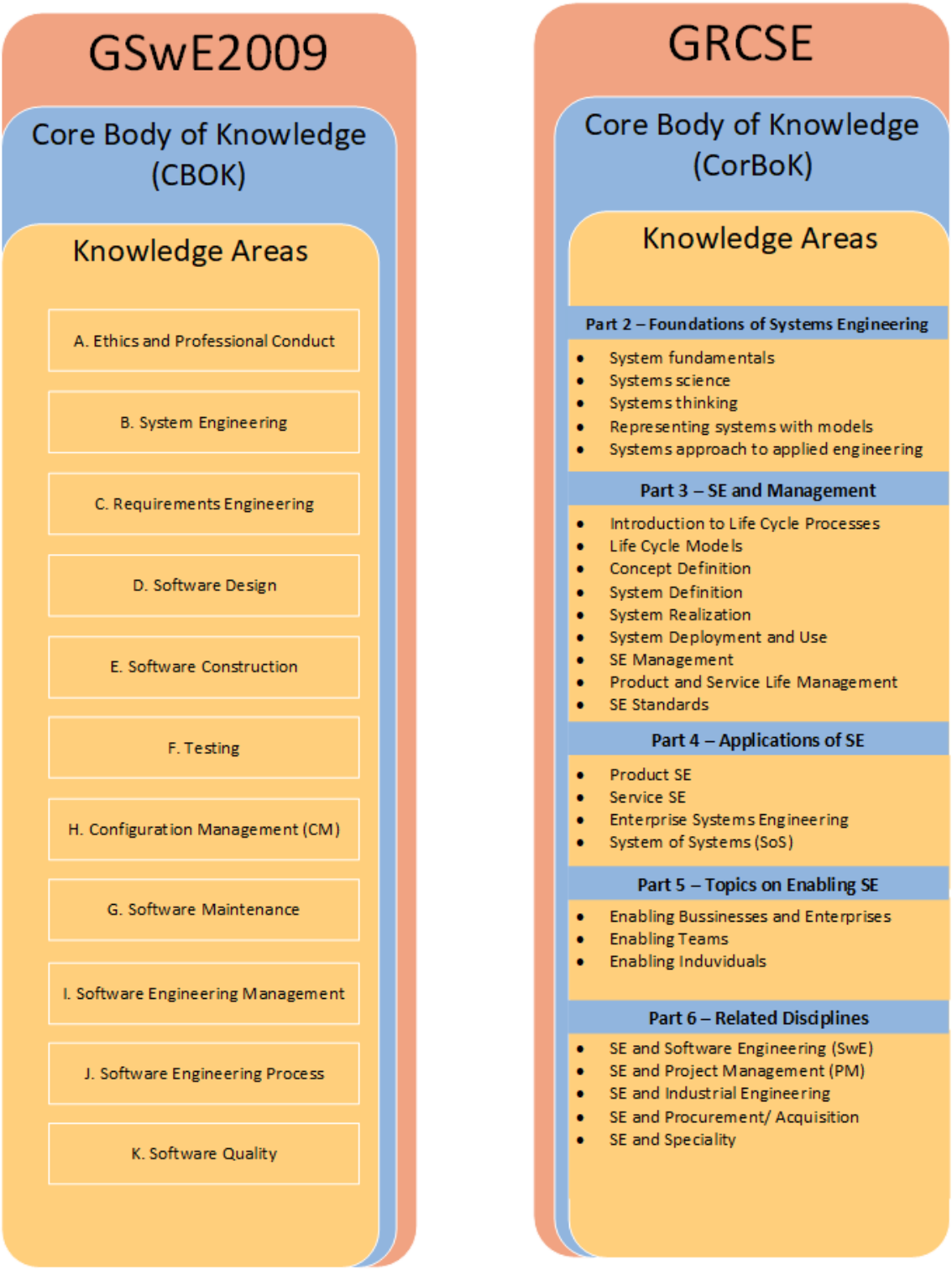


Figure 4.1: The structure of Knowledge Areas in the Core Body of Knowledge within GSwE2009 (left) and GRCSE (right)

4.1 Cybersecurity

The Cybersecurity Workforce Framework from National Initiative for Cybersecurity Education (NICE) is built on NIST 800-181 (Petersen et al., 2020). It lists knowledge and skills relevant to a cyber security work role. This framework, along with Knowledge Areas from the Cybersecurity Curricula 2017 (Joint Task Force on Cybersecurity Education, 2018), has been used as criteria when identifying topics for the cybersecurity focus area. This section presents the topics in GSwE2009 that were identified as relevant for competence within the field of cyber security. Table 4.1 lists all GSwE2009 topics relevant to cyber security and their mapping to GRCSE. The table is organised so that the rows correspond to GSwE2009 topics, and the columns represent part of the Core Body of Knowledge in GRCSE. Refer to section 3.1.3 for a description of the comparison scale (symbols).

Table 4.1: GSwE2009 Cybersecurity Topics to GRCSE Mapping

GSwE2009 topics	**GRCSE CorBOK**				
	Part 2	*Part 3*	*Part 4*	*Part 5*	*Part 6*
C.1	◔	◑			
C.2		◑			
C.3					○
C.4		●			
C.5		◑			
C.6		◑			
C.7	◔	◑			
C.8		◑			
D.					○
E.1					○
E.3					○
G.2					○
G.4					○
H.1		●			
H.2		◔			
H.3		◔			
H.4		◔			
H.5					○
I.2		◑			
J.4					○
K.1					○
K.3		●			

C: Requirements Engineering

C.1 "Fundamentals of Requirements Engineering" contains sub-topics that weakly relate to GRCSE part 2: "Representing Systems with Models", as some of the core activities for

requirements engineering could be identified in both topics. C.1 is also partially related to Part 3: "SE and Management". C.1 is defined as "The process for determining the necessary capabilities and/or functions for a specific product or service, [] specifically to the development of software requirements" in GSwE2009. In GRCSE, many of the same core processes can be identified, along with an overlap of at least one competence level. The main difference is that the topic of Requirements Engineering is covered more broadly in GRCSE, describing how requirements engineering considers not only specific system requirements: "Requirements exist at multiple levels of enterprise or system with multiple levels abstraction. This ranges from the highest level of the enterprise capability or customer need to the lowest level of the system design".

C.2 "Requirements Engineering Process" is partly related to the topics "Life Cycle Models" and "System Definition" in GRCSE part 3. Some activities can be identified in both curricula but do not match Bloom Cognitive Levels. GSwE2009 requires competence within this topic while GRCSE requires application, the latter being a higher level of competence in Bloom cognitive levels.

C.4 "Requirements Elicitation" is strongly related to the topic "Concept Definition" within Part 3 of GRCSE. Both emphasise requirements sources, stakeholder requirements and activities for requirements elicitation, and application is the required Bloom cognitive level for both.

C.5 "Requirements Analysis" relates partly to the topics "Life Cycle Processes and Enterprise Needs", "Stakeholder Needs and Requirements", and "System Requirements" in GRCSE part 3. Activities such as identifying requirements, modelling and prototyping, and validation are found in each curriculum. However, GSwE2009 requires Bloom cognitive level analysis, while GRCSE requires an application.

C.6 "Requirements Specification" partly relates to several topics within part 3: "Life Cycle Models", "Concept Definition", "System Definition", and "System Realisation". All these topics describe similar, or parts of similar, activities as described in C.6 and are mapped to the same Bloom level.

C.7 "Requirements Validation" relates weakly to GRCSE part 2 topic "Implementing and Validation a Solution". While activities such as requirements reviews, prototyping and validating are found in both curricula, the activities are specified in more detail in GSwE2009. GSwE2009 also require a competence lever of application, while GRCSE requires knowledge. C.7 is partially related to the GRCSE part 3 topic, "System Validation". Both curricula require the Bloom cognitive level application and contain a set of activities that validate previously identified requirements. GRCSE makes a strong distinction between validation and verification, while GSwE2009 uses both terms within the topic of Requirements Validation.

C.8 "Practical Considerations" describes a requirements process for a software life cycle. Overall, C.8 describes a more detailed approach, but it does relate partly to several topics within KA "Systems Definition" in GRCSE. C.8 also partly relates to the "Configuration Management" topic in KA "SE Management". C.8 requires Bloom level comprehension/application, while the topics in GRCSE require application and comprehension, respectively.

H: Configuration Management

H.1 "Management of the CM Process" strongly relates to GRCSE part 3 "SE Management", sub-topic "Configuration Management". The topics cover planning, organisation, and constraints for configuration management, and both curricula require comprehension at a competence level, though GSwE2009 specifies comprehension/application.

H.2 "Configuration Identification", H.3 "Configuration Control", and H.4 "Software Configuration Status Accounting" weekly relates topics within part 3, "Configuration Management". Activities such as identifying items of work tasks relevant to the topic, controlling configuration changes, and baselines are mentioned in both curricula. However, GRCSE describes more of an overview, whereas GSwE2009 describes this in detail. The required level of competence is comprehension and application, respectively.

I: Software Engineering Management

I.2 "Risk Management" is partly related to GRCSE part 3 topic "Risk Management" in the KA "Systems Engineering Management". GSwE2009 Risk Management relates more specifically to software-related risks, but the activities of "[] assessing potential threats to an endeavour, developing strategies to both reduce the probability of the problem occurring and counter these threats if they occur and implementing these strategies using program resources" [11, p. 111] partly relates to the GRCSE risk management process activities risk planning, risk identification, risk analysis, risk handling and risk monitoring [10, p. 456]. Also, GSwE2009 requires Bloom level application, while GRCSE requires comprehension.

K: Software Quality

K.3 "Verification and Validation (V&V)" is strongly linked to topics "System Verification" and "System Validation" in the KA "System Realization" in GRCSE part 3. Tough GSwE2009 refers specifically to methods relevant to software development, identifying V&V scope, testing techniques, and evaluating target capabilities overlap with GRCSE. Both curricula require Bloom level application.

4.2 Machine Learning

The skill and competence needed to develop Machine learning (ML) algorithms draw on SwE and Data Science (IABAC, 2019). The topics listed in Table 4.2 have been chosen by studying previous work done concerning the combination of SwE and ML, including; SwE challenges for ML (Kumeno, 2019), SwE perspectives of ML systems (Giray, 2021), and the challenges and possibilities in developing AI/ML in the context of SwE (Menzies, 2020; Nascimento et al., 2020; Rech & Althoff, 2004). Ethics and professional conduct have also been included as relevant KA, as these are relevant aspects of AI/ML development.

Table 4.2: GSwE2009 ML Topics to GRCSE Mapping

GSwE2009 topics	**GRCSE CorBOK**				
	Part 2	*Part 3*	*Part 4*	*Part 5*	*Part 6*
A.2				●	
A.3					○
C.1	◔	◑			
C.2		◑			
C.3					○
C.4		●			
C.5		◑			
C.6		◑			
C.7	◔	◑			
D.					○
E.					○
G.					○
H.1		●			
H.2		◔			
H.3		◔			
H.4		◔			
H.5					○
I.1		◑			
I.2		◑			
I.3		◔			
I.4		◔			
I.5		◔			
I.6		◑			
I.7					○
K.1		◑			
K.2					○
K.3		●			

A: Ethics and Professional Conduct

A.2 "Codes of ethics and professional conduct" relates strongly to the topic "Ethical Behaviour" in GRCSE part 5. Both curricula cover ethical behaviour and professionalism relating to law and legal issues, cultural responsibility, and responsibility to society. Both curricula require Bloom level comprehension, while GSwE2009 has specified comprehension/application.

C: Requirements Engineering

See section 4.1 for details about this mapping.

H: Configuration Management

See section 4.1 for details about this mapping.

I: Software Engineering Management

I.1 "Software Project Planning" and I.2 "Risk Management" relates partly to the topic "Planning" in GRCSE part 3. Both topics cover a high-level overview of methods, techniques, processes, economy, deliverables, and project risks that can be applied in either field. However, GSwE2009 require Bloom level application, while GRCSE require comprehension.

I.3 "Software Project Organization and Enactment" and I.4 "Review and Evaluation" is weakly related to "Assessment and Control" under the KA "Systems Engineering Management" in GRCSE part 3. In GSwE2009, the topic emphasises management activities such as monitoring, controlling, and reporting, while the GRCSE topic aims to "provide adequate visibility into the projects actual technical progress and risks concerning the technical plans". There is also a difference in Bloom level, where GRCSE require comprehension and GSwE2009 requires application.

I.4 "Review and Evaluation" and I.5 "Closure" are weakly related to "Assessment and Control" in GRCSE part 3. Both topics require Bloom level comprehension, though the topic activities are described in much more detail in GSwE2009 than in GRCSE.

I.6 "Software Engineering Measurement" is partially related to the topic "Measurement" in KA "SE Management" in GRCSE part 3. Both topics refer to the IEEE 15939 standard and have defined activities for (1) establishing and sustaining measure commitment, (2) plan measurement, (3) performing measurement, and (4) evaluating measurement. Though there are many similarities, the topics differ in Bloom levels, where GSwE2009 requires application while SE requires comprehension.

K: Software Quality

K.1 "Software Quality Fundamentals" partially relates to "Quality Management" in GRCSE part 3, KA "SE Management". Measures to assess quality in product, process quality and quality improvement are covered in both curricula, but GSwE2009 requires Bloom level application while SE requires comprehension.

K.3 "Verification and Validation" is described in section 4.1.

4.3 Soft Skills

The GSwE2009 curriculum expects graduates to "Be an effective member of a team [...] and lead in one area of project development, such as project management, requirements analysis, architecture, construction, or quality assurance." (Pyster, 2009, p. 20). The topics listed in Table 4.3 are topics that are specified as relevant for functioning in a team in GSwE2009 (Pyster, 2009, p. 96).

Table 4.3: GSwE2009 Soft Skills Topics to GRCSE Mapping

GSwE2009 topics	**GRCSE CorBOK**				
	Part 2	*Part 3*	*Part 4*	*Part 5*	*Part 6*
A.1				◑	
A.2				●	
I.3		◔			

A: Ethics and Professional Conduct

A.1 "Social, legal, and historical issues" relate partly to "Ethical behaviour" in the KA "Enabling Individuals" in GRCSE. Subjects such as cultural issues, laws, and regulations can be found in both topics. However, A.1 additionally covers subjects such as computer crime, data confidentiality, security, and privacy. GSwE2009 states that: "The use of the Internet and large databases that hold private information (medical, financial, legal, etc.) place a greater responsibility for ethical and professional conduct on the software engineers who develop products that deal with this confidential and private information".

A.2 "Codes of ethics and professional conduct" is strongly related to the topic "Ethical behaviour" in the same KA as described directly above. Both topics cover responsibility to society, models of professionalism, and codes of ethics. Bloom level comprehension is required in both instances.

I: Software Engineering Management

I.3 "Software Project Organization and Enactment" is described in section 4.1.

4.4 Systems Engineering

The topics in Table 4.4 include "content or activities that are relevant for systems engineering" (Pyster, 2009, pp. 52, 96) mapped to the GRCSE curriculum. These topics are vital to "Understand the relationship between software engineering and systems engineering and be able to apply systems engineering principles and practices in the engineering of software." (Pyster, 2009, p. 20). It is important to emphasise that the relationship found in this mapping only indicated how GSwE2009 topics relate to GRCSE. Topics in the KA "Systems Engineering" (B.1-B.7) are naturally covered to a much greater extent in GRCSE than in GSwE2009.

Table 4.4: GSwE2009 Systems Engineering Topics to GRCSE Mapping

GSwE2009 topics	**GRCSE CorBOK**				
	Part 2	*Part 3*	*Part 4*	*Part 5*	*Part 6*
A.1				◑	
A.2				●	
B.1	●				
B.2		◑			
B.3	◑	●			
B.4		●			
B.5		◑			
B.6		◑			
B.7		●			
C.1	◔	◑			
C.2		◑			
C.3					○
C.4		●			
C.5		◑			
C.6		◑			
C.7	◔	◑			
C.8		◑			
F.1		◔			
F.2		◔			
F.3					○
F.4					○
F.5					○
H.1		●			
H.2		◔			
H.3		◔			
H.4		◔			
H.5					○
I.2		◑			
I.5		◔			
I.7					○
J.4					○
K.1					○
K.3		●			

A: Ethics and Professional Conduct

See section 4.3 for mapping details.

B: Requirements Engineering

B.1 "Systems Engineering Concepts" strongly relate to all topics in the KA "System Fundamentals" in GRCSE part 2. All topics require a Bloom level of comprehension. B.1 also related to topics within KA "Systems Approach Applied to Engineering Systems". However, the required Bloom level for topics in this KA is knowledge.

B.2 "System Engineering Life Cycle Management" aims to enable "software engineers working on the development of complex systems need to be able to look at a particular project/program life cycle and be able to relate it to the spectrum of life cycle approaches [...]." It covers two main sections: 1) "Life Cycle Management" is related to the KA "Introduction to Life Cycle Processes" in GRCSE. It is partially related to the topics "Generic Life Cycle Model", "Applying Life Cycle Processes", and "Life Cycle Processes and Enterprise Need". Section 2) "Systems Engineering and Software Engineering Processes" relates partially to the topic "System Life Cycle Process Drivers and Choices" in KA "Life Cycle Models". GSwE2009 topic B.2 requires Bloom level comprehension, while all topics from GRCSE require Bloom level application.

B.3 "Requirements" consists of two sections: Stakeholder Requirements and Requirements Analysis. Stakeholder Requirements relate to several topics in GRCSE part 2 and part 3. It is partially related to the topic "Identifying and Understanding Problems and Opportunities" in KA "Systems Approach Applied to Engineering Systems" in GRCSE part 2, which "describes knowledge related to the identification and exploration of problems or opportunities in detail [...]" (SEBoK Editorial Board, 2021, p. 136). The topics differ in Bloom levels, where GSwE2009 requires comprehension/application and GRCSE requires knowledge. Requirements Analysis is strongly related to the topic "Stakeholder Needs and Requirements" in KA "Concept Definition" in GRCSE part 3, which provides a more detailed account of principles, concepts and methods related to stakeholder requirements. Bloom level application pertains to both topics.

B.4 "System Design" is divided into "Architectural Design", "Implementation", and "Trade Studies". All parts related to topics within the KA "System Definition" in GRCSE part 3. Bloom level for GSwE2009 is comprehension/application, while GRCSE topics require only an application. Architectural Design strongly relates to the topic "System Architecture", as activities related to defining a comprehensive solution encompassing all system requirements are described in both. Implementation is strongly related to "Logical Architecture Model Development", "Physical Architecture Model Development", and "System Design". All topics describe activities used to determine system details according to requirements. Trade Studies relate strongly to the topic "System Analysis", which describes approaches to technical decision-making.

B.5 "Integration and Verification" is partly related to topics "System Integration" and "System Verification" in KA "System Realization" in GRCSE. GSwE2009 require Bloom level comprehension, while GRCSE require an application. B.6 "Transition and Validation" relates partially to the topic "System Validation" in KA "System Realization" and the topic "System Deployment and Use" in KA "System Deployment and Use". Activities such as the system transfer process and system validation are described in both topics. However, GSwE2009 requires Bloom level comprehension, while GRCSE requires comprehension for the first topic and application for the second.

B.7 "Operation, Maintenance and Support" describe activities related to technical processes for a system's utilisation and disposal life cycle stages. B.7 strongly relates to topics "Operation of the System", "System Maintenance", and "Logistics" in KA "System Deployment and Use", as well as "Service Life Extension", "Capability Updates, Upgrades, and Modernization", and "Disposal and Retirement" in KA "Product and Service Life Management" in GRCSE. All topics require Bloom level comprehension.

C: Requirements Engineering

See section 4.1 for details about mapping topics C.1 - C.8.

F: Testing

F.1 "Testing Fundamentals" weakly relates to topics "System Verification", "System Validation", "System Deployment", and topic "Decision Management" in GRCSE part 3. GSwE2009 topic F.1 describes the definitions of testing in software engineering, as well as specific key issues in software testing. GRCSE topics, on the other hand, mention testing activities briefly in the topics listed here but generally describe processes of assessing rather than testing. GRCSE topic "System Deployment" requires Bloom level comprehension, whereas the remaining topics require an application.

F.2 "Test Levels" weakly relates to topics "System Validation" and "System Realization" in GRCSE part 3. Some of the activities described in F.2 can be adapted to fit activities in GRCSE. Still, most activities are explicitly related to software testing and are not transferable to a systems approach. Bloom level application is required for all topics mentioned.

H: Configuration Management

See section 4.1 for details about this mapping.

I: Software Engineering Management

I.2 "Risk Management" and I.5 "Closure" are detailed in section 4.1 and 4.2.

K: Software Quality

K. 3 "Verification and Validation (V&V)" is detailed in section 4.1.

Chapter 5

Industry Perspective

ICS cybersecurity skills and competence are examined in this chapter in light of the interviews conducted with industry leaders. The interviews aim to explore what skills and competencies the industry needs for cyber security within the ICS environment, and there were a total of three participants. As described in Chapter 3, the findings are presented according to the themes found in through the Qualitative Content Analysis (QCA).

The first section presents the participants, their working environment and their education. Next, we present the findings of the content analysis, with a total of four global themes: IT in ICS, ICS competence, vendors in ICS and education, upskilling and background.

5.1 Participants

The interviews aimed to gain insight into the participants themselves, specifically their experience, education, and domain of expertise. Tables 5.1-5.3 provide a summary of the participant information and any additional information provided in the interviews.

As part of the energy industry, participant A (Table 5.1) is responsible for the communication, maintenance, and safeguarding of installations. Participant A's teams are responsible for both these installations' hardware and software components. Other tasks include framework agreements, technical specifications, system requirements specifications, and version control of components. Participant A has been in this position for 14 years and has been part of a security-focused expert group for the last 10-12 years. He has a background as an electrical engineer, with a Master's degree in electrical engineering.

Table 5.1: Participant A

IQ	*Question*	*Participant A*
1	Domain of work	Energy
2	Title/role	Subject-matter specialist
3	Years in current role	14 years
4	Cybersecurity experience	10-12 years
5	Education	Electrical engineer (MSc)

Participant B (Table 5.2) is the head of industrial digitalisation and OT in the process industry and has had this responsibility for 29 years. Among the responsibilities of this position are system responsibility, applications and operational aspects of systems, and maintenance and development of those systems. Participant B has a background as an automation/electronics engineer with a Master's in cybernetics. Cybersecurity challenges have been a part of their work since 2004.

Table 5.2: Participant B

IQ. ID	*Question*	*Participant B*
1	Domain of work	Process industry
2	Title/role	Head of industrial digitisation / OT
3	Years in current role	29 years
4	Cybersecurity experience	10 years
5	Education	Cybernetics (MSc)

Participant C (Table 5.3) works in research and development as a Chief Information Officer (CIO), a role he's had for 4,5 years. In addition to a background in IT and development, he holds a Master's degree in communication systems. Their industry experience, which spans 20-25 years, has always included security, even though he has not held a position in the field of cybersecurity.

Table 5.3: Participant C

IQ. ID	*Question*	*Participant C*
1	Domain of work	Research and Development
2	Title/role	Chief Information Officer
3	Years in current role	4,5 years
4	Cybersecurity experience	-
5	Education	Communication systems (MSc)

5.2 Findings

This section discusses the findings from the interview and discusses them according to the thematic network (Figure 3.4).

5.2.1 IT in ICS

One of the key narratives throughout the interview analysis is the emerging role of IT in the ICS environment.

The interconnection between IT and OT: Participants discussed the interconnection of IT and OT. Participant B stated that *"We have been experiencing a more intertwined working relationship with the IT department over the years"*, emphasising the challenges related to the complexities of incorporating IT into the ICS, particularly monitoring physical processes. They acknowledged the

struggle with IT-OT interconnection, noting that though similar, the technologies are *"are worlds apart"*.

According to Participant B, they submit a specification to the IT department when they require IT components for their installations. The IT department then creates a template based on their requirements. Participant C explained a similar situation, where the IT department is responsible for network design for OT systems. This implies that interconnections between IT and OT are increasing.

As the CIO of their organisation, Participant C is aware that IT and OT collaboration, while still in its early stages, is undergoing significant changes. He states that

> *"OT is an area we have not been heavily involved in yet. OT is more building and process, etc. It is its own expertise area that IT has not had much to do with before. This is now changing. For instance, it [Building Management] is now called Building and Technology to account for this development."* (Participant C)

Participant C further highlighted this challenge, revealing a shift within their company to include OT within IT security governance. The interconnection of IT and OT has further illustrated in the participant's quote: *"The most significant change is that OT must be included as part of the security governance that is being done within IT."*

Remote access: The interviews also revealed the complexity and inherent risks associated with remote access. Participant A expressed concern about remote access as a significant vulnerability, remarking that *"if the wrong people get access to these systems, they can cause a lot of damage."* In their organisation, remote access is already in use to facilitate greater efficiency when working on some installations, and they expressed some concern relating to increased use of the solution in the future. Aside from security concerns, remote data collection also poses challenges. There are few readily available solutions for collecting these data, and these are limited by vendor type. Additional challenges related to remote access, such as competence needs, are discussed below.

Participant B mentioned the risk of remote access when it comes to vendors' need for access to their systems:

> *"When a vendor needs remote access to an installation/solution, they don't see the whole environment. One thing is [secure] access via two-factor solutions, but another concern is where they end up within the system, or where they can navigate to."* (Participant B)

In addition, they state that their company follows a strict standardisation policy, limiting the number of vendors and vendor-specific expertise within their organisation.

IT-OT Collaboration: According to the interview results, IT and OT collaboration are critical to the company's cybersecurity practices. The interaction between these two domains has been noted in various areas, from daily operations to handling potential threats. Participant A is the primary contact person for communication between their team (OT) and the SOC (IT).

> *"I have had a lot of contact with both [IT and OT]. We collaborate, for example, on troubleshooting." "SOC personnel are purely IT. They enquire about vulnerabilities, CVEs [common vulnerabilities and exposures], etc. They request information when they get an alert about a newly discovered vulnerability: 'Does this concern us?"* (Participant A)

Throughout the interview, participant B highlights the critical importance of robust collaboration between IT and OT while emphasising that IT and OT are distinct domains requiring different competencies and operational understandings. An example of IT-OT collaboration in Participant B's organisation was provided concerning their emergency response system, which includes personnel both with IT and OT expertise:

> *"It is crucial that we can assess what is transpiring. From the OT side of things, our strategy is to isolate the threat from the IT side. In a cyber event, it is crucial to know the consequences. The example from Hydro*[1] *is a good example of a situation where responsibilities and consequences were unclear. These are important aspects of an emergency preparedness plan: what is taking place, what are the consequences, and how can we manage the situation in the long run?"* (Participant B)

There are no set meetings between IT and OT specifically concerning security, but they do have systems in place on department levels. He continues:

> *"We collaborate with IT regarding technology, procedures, and benchmarking. These are common areas for IT and OT today. We are operational on OT security, while IT purchases security solutions from a third party."* (Participant B)

Security Operations Centre: Findings from the interviews revealed that the Security Operations Centre (SOC) has a significant role in ICS security. Three dominant themes emerged in the analysis relating to the SOC: its organisational structure, role in cybersecurity management, and collaborative relationship with OT.

Participants A and B informed that the SOC monitors some of their ICS systems, and in both cases, the SOC is only staffed with IT personnel. When asked if anyone in the SOC had OT competence, participant A responded:

> *"No, that's often the problem. They have little or no competence in our equipment. Working together is a challenge. We usually don't hire anyone with IT competence in our domain, and the same goes for hiring OT competence in the IT domain."* (Participant A)

In response to a similar question, participant B responded that they do not have their own SOC. However, there is a service that provides a SOC for the IT side of the organisation. Through collaboration between the SOC, IT and OT personnel, this is now monitoring parts of the OT environment. There are no OT professionals on the SOC staff. *"We have a practical SOC via [company name], but in terms of strategic alignment, it is IT and OT that are working together to gain a common understanding of each other."*

Participant B highlighted the division of the SOC, IT, and OT divisions in their organisation. However, despite the distinct separation, they noted the SOC's crucial role in their emergency response system. The emergency response plan includes the SOC, IT, and OT personnel, highlighting the need for solid collaboration.

Participant C has a SOC in their organisation but does not monitor OT systems. *"We currently regulate OT by limiting OT equipment, segmenting the network, etc. We set up the [communication] network, but security and maintenance are the vendor's responsibility."*

[1] https://www.hydro.com/en/media/on-the-agenda/cyber-attack/

5.2.2 ICS competence

Upon analysing the interviews with participants A, B, and C, it becomes apparent that the complexity of the ICS environment requires a wide array of specialised competencies and skills in the industrial control system. These range from foundational architectural understanding to complex cybersecurity expertise.

ICS architecture: A principal theme common to all the interviews is the significance of understanding ICS architecture. Participant B explicitly emphasises this point, advocating the importance of understanding both the design and layout of the OT and IT systems at a fundamental level. This is especially relevant to remote access:

> *"It is crucial to understand the architecture that provides this service. This is a job for a system engineer [on their team]. Managing external access involves understanding the user's needs, the architecture being used, and your system requirements. Who has access to what, and when?"* (Participant B)

Participant C shares this perspective, stating, *"We need to establish better cyber process models and ensure that OT is involved in these processes, including the selection and purchasing of OT equipment."*

OT competence: The analysis of the interviews revealed an overarching theme regarding the importance of specialist knowledge and skill sets in OT. These include how technology is utilised, the value of hands-on competence, and participation in continuous learning initiatives such as seminars.

A solid understanding of OT technical elements appears to be a recurring theme in the interviews. Participant B underlines the importance of understanding OT systems' design and layout, positioning this knowledge as a fundamental competency. They state that

> *"In the world of OT, you need to know the exact consequences of your actions- there can be no guesswork. This factor probably distinguishes an IT engineer from an OT engineer. For example, you do not simply patch a server and hope it will work."* (Participant B)

Additionally, participant B stresses the importance of hands-on competence and the ability to follow up with vendors. *"It is essential that those who work with OT systems possess the necessary competencies. For example, understanding system criticality. This is probably a matter of competence gap between IT and OT."* In addition, emphasis was added on that that practical, specific expertise in a particular product is extremely valuable in the OT environment: *"we look for people who already have system knowledge because this knowledge is easily transferable"*.

Participants also focus on potential impacts and consequences. In light of this, participant C commented that IT development is progressing accelerated. They suggested that IT might be better off reverting to a more controlled form. They also indicated that IT personnel, especially those working within ICS, should aim to understand questions such as "What is acceptable downtime for this system?" and "What is acceptable operational risk?"

Continuous learning and development, such as vendor seminars, emerge from these discussions. Participant B reflected on the value of seminars and other learning platforms, advocating their importance in staying up-to-date with the rapidly evolving field of OT. However, participant A

expressed increasing concern regarding the lack of ability to apply the skills they learn at such seminars.

> *"We can travel to [vendor] for an introductory seminar, but it's hard to learn without hands-on experience. We can attend a seminar to gain new competence. However, it may take four months before the need for that competence arises."* (Participant B)

The language of the tribe is also a significant aspect of OT, according to Participant B:

> *"The OT language is probably like a tribal language, where you have to be a member of the tribe [to understand]. It may not be something that can be acquired through education."* (participant B)

Cybersecurity: Participant A's team consists of two cybersecurity personnel out of sixteen total. They explicitly mention the importance of handling cyber threats and how this is a shared responsibility with the SOC.

Further, they discuss the possibility of developing new software methods for securing the ICS, such as patch management or asset management systems. However, they caution that such a system may also introduce additional vulnerabilities. Additionally, participant A's team is responsible for maintaining the software that allows remote access to installations and ensuring that it is operational.

Participant A also pointed to the development of Intrusion Detection System (IDS) for ICS environments, commenting on the difficulty in implementing security functions on hardware not designed with security in mind. *"[OT] Hardware is not built for that, and you get issues with memory, CPU capacity, etc. This is one of the most significant challenges with current systems. They are not developed with security [features] and lack the memory capacity to implement them later."*

Participant B emphasised the secure architecture policy tied to their IT and OT technology. They state that

> *"The driving force behind this is the adoption of digitisation and cybersecurity in the board room, and upper management has shifted their focus. As a result, we need to adapt, but we are also given more funding. We now spend more exclusively on security. Isolating [systems] is not a sufficient strategy by itself anymore."* (Participant B)

Moreover, they concluded that it is vital to consider the different aspects of priority and order of things for security measures within IT and OT. *"If you understand why IT and OT are different, we've come a long way. [...] The biggest threat to an OT system is not e-mail. There are other priorities."*

Concurrently, participant C discusses the need to incorporate OT into broader cybersecurity processes, emphasising the integration of different system domains for effective cybersecurity governance. Further concluding that *"OT will be as vulnerable as IT is today"* and that *"existing IT tools must be adapted to fit OT requirements"*. They also draw attention to the difficulties associated with incorporating OT components into current IT processes, stating that

> *"We have struggled with these challenges [implementing security processes] in IT for a long time without really figuring it all out, and now a whole new domain is supposed to draw on the same competence that IT has."* (Participant C)

Participant C further noted that AI models could help bring OT components into IT processes; *"AI operative solutions are maybe 2-5 years away"*. Participant A provided a more critical perspective, explaining their experiences with IDSs with machine learning functionality.

> *"I have spoken with the vendors who sell these solutions, and they state that their solution needs about one month of data to create a baseline for normal operations. Only about 1/3 of all possible events occur within a month in our installations."* (Participant A)

They continued that if a baseline were useful, it would have to include every possible scenario within the given system, presumably taking more than one month. *"We have done research projects with this [IDSs in OT environment] before. There are many false alarms. Most of the flagged data is ok; however, some actual attacks went unnoticed [in the ICS]."* (Participant A)

Future ICS competencies: Both participants A and B are in the OT domain, and neither have any employees with IT education in their teams. Participant C, who has a background in IT and works in research and development, provides a different perspective.

Participant A's team consists of two cybersecurity personnel out of sixteen total. They explicitly mention the importance of handling cyber threats and how this is a shared responsibility with the SOC. Participant A considers an understanding of communication networks, different protocols and installation networks, and control of real-time systems. Below are three quotes relevant to the future skills and competencies in the ICS:

> *"Future control facilities will include more IT, for instance, network switches that can affect how ting operates in the facility."*

> *"Diagnosing installations will shift from instrument measures to Wireshark, and we will need more competence on this when OT moves closer to IT, and the competence needed for diagnosing and debugging changes. It will be a whole new way of working."*

> *"The future will be more software-driven, Which poses extreme challenges for operations. We'll be able to access and diagnose with updated tools remotely, but we'll need the competence to use them. Not everyone will be able to keep up with these changes [in terms of new competencies and skills]."*

5.2.3 Vendors in the ICS

A recurring theme in the interviews is the relationship between vendors and vendors and their role in ICS. The participants shared their insights and experiences regarding vendor management, system standardisation, and proprietary technology challenges.

Competency: Participant A stated that, in terms of IT-OT collaboration and competence, vendors have the same separation of disciplines as most ICS, where you can get support from either one or the other: *"The vendors we have framework agreements with are in the same situation. You get either electrical or automation, while IT is <in-house>"*. They further stated that vendors have the same challenges related to the increasing need for IT competencies in their OT teams.

Participant B reported a lack of competence in cybersecurity from vendors within the OT space, noting that *"they have matured somewhat over the last three years, but there is [still] a tendency to push IT end-node tools to OT."*

Standardising: Participant C further underscores the role of vendors from a challenging perspective, expressing frustrations over vendors who propose outdated technology solutions to customers. For instance, participant C states, *"the supplier has suggested OT units where what they suggest is completely outdated technology"*. This highlights a significant challenge where vendors are not fully aligned with customer needs or industry technological advancements.

Continuing with vendor challenges, participant C mentions proprietary technology. They argue that *"it is difficult to become data-driven when a supplier like [company name] does not offer [Application Programming Interface] APIs, and everything is proprietary"*. Vendors' use of proprietary systems complicates the integration and analysis of data, limiting opportunities for leveraging data-driven insights in the industry. Additionally, participant C pointed out that the restrictions set by the lack of APIs and access to insight into the OT components are forcing IT to *"compensate by limiting/restricting these components to the point where they are almost unable to communicate with anyone"*.

Participant A likewise expressed frustration with the inability to have control over the components provided by vendors. Participant A stated that while some framework agreements are set, there is still a lot of freedom for the vendor to choose components as long as they fit with the functional requirements sent from the customer.

> *"Three different vendors will have three different solutions, such as a gateway, HMI and other components. We send functional requirements, but the three suppliers can deliver three different solutions."* (Participant A)

They further explained that some installations require two different vendors for redundancy. However, the wide range of other solutions they have to support creates challenges relating to competence building, optimising asset management and patching, and so on.

Maintenance and control: Participant A commented on the challenge they face with vendors having access to systems after installation.

> *"an issue we would spend two days on, they resolved remotely in 2 hours. However, if we do this, we will never learn to do it ourselves. We will not get the competence we need as long as we keep calling them to debug our systems. This is an IT-OT problem."* (Participant A)

5.2.4 Education, Upskilling and Competence Building

The three interviews revealed insightful perspectives on upskilling, competence building, and education within the ICS cybersecurity context. There was an emphasis on continuous learning and development throughout all three discussions and the importance of a wide range of competencies.

Participant A suggested an introductory course on OT for IT students and stressed the need for IT to be incorporated into the education of OT disciplines. *"The reality I see is that many [newly educated] have some practical knowledge, but when they enter the OT environment, they reach a dead end. This may be alleviated by incorporating a little more variety in disciplines/subjects in their education"*.

Participant B noted that fundamentally, there are very few differences between IT and OT, as their technology, at its core, is very similar. It might be helpful to bring OT into engineering education as a distinct subject and the nuances of different OT technology. Furthermore, participant B emphasised the importance of understanding the operational aspect and students understanding

the crucial difference between IT and OT. They further commented on the state of cybersecurity competence in ICS outside of IT and OT, noting:

> *"Outside the IT-OT tribe, it is completely blank. I spend much of my time explaining to people why we do this- simple things like why you can't charge your phone with a USB connection to a PC."* (Participant B)

Participant C argues for philosophies and methods to educate students in thorough planning and process orientation within ICS cybersecurity. Within ICS operations, continuity and criticality must also be considered. They argue for IT to consider the speed of current development and reapply previously used frameworks and methodologies. Furthermore, they suggest that sharing philosophies, methods, and frameworks can effectively educate and upskill new and existing employees.

Chapter 6

Discussion

This chapter discusses the findings obtained from the curriculum mapping exercise and the in-depth semi-structured interviews with experienced cybersecurity professionals. The discussion also offers insight into the roles of 'habitus' - a term derived from sociology - encapsulating the inherent behaviours, attitudes, and tendencies cultivated through shared experiences and environments and their influence on ICS cybersecurity.

In order to address these new challenges arising from the interconnectedness of IT and OT within ICS cybersecurity, it is essential that we consider the varied nature of these systems. However, the complexity is not limited to the industrial ecosystem. It also involves the mindset of the individuals who design, operate, and secure these systems. This shared mentality, also known as 'habitus', impacts and is influenced by practices within the field, creating differences between traditional IT-focused cybersecurity and the evolving requirements of ICS cybersecurity. It is therefore important not only to focus on technological advances but also to address these mental, social and cultural gaps in order to create a comprehensive understanding of ICS cybersecurity, which encompasses both the IT and OT sectors.

6.1 Curriculum mapping - Results analysis

This section discusses curriculum mapping results and considers the relations and topics mapped. As one topic in Graduate Software Engineering 2009: Curriculum Guidelines for Graduate Degree Programs in Software Engineering (GSwE2009) can relate to several topics in Graduate Reference Curriculum for Systems Engineering (GRCSE), the number of relations is not equal to the total number of topics in Table 4.1 to Table 4.4.

The curriculum mapping identified 67 relations, of which 22 were weakly related, 28 were partially related, and 17 were strongly related. Figure 6.1 illustrates the distribution of the 67 relations in the four focus areas cybersecurity, machine learning, soft skills and systems engineering. Identifying these relationships required comparing topic activities from the curriculum and Bloom's cognitive levels associated with each topic.

Out of the 67 relations mapped in chapter 4, only 8 belong to part 2 of the GRCSE (Figure 6.2. According to GRCSE,

> *"Part 2 topics are primarily conceptual, with the concepts supporting the topics in part 3. Part 3 concentrates on the processes, methods, and practices used to manage, develop, operate and maintain systems."* (Pyster, Olwell et al., 2015, p. 35).

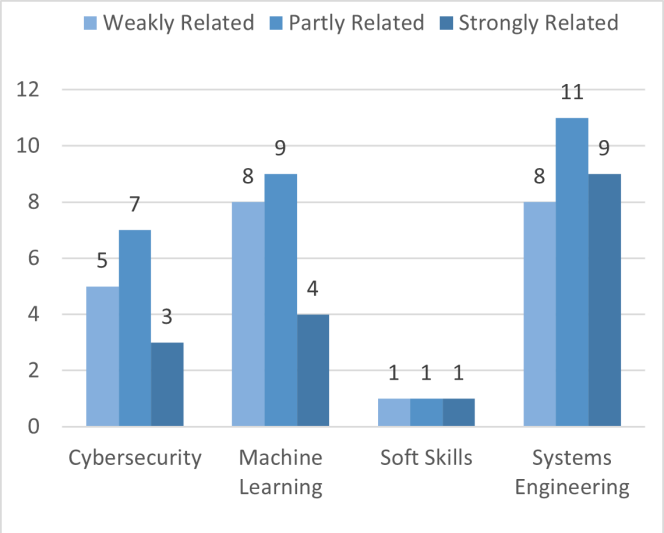


Figure 6.1: Distribution of relations in the four focus areas

6 of the topics related to part 2 are weakly related, 1 topic is partly related, and the last topic is strongly related. Considering that this part of the CorBOK contains the foundational SE concept, it is worth noting that only 8 relations are mapped to this part of "fundamental SE knowledge". For instance, mapped topics within the KA Systems Engineering to GRCSE (Table 4.4) only have four relations to GRCSE part 2, i.e., "fundamental aspects of SE". However, 22 relations are mapped to part 3, *"a more in-depth coverage of requirements, architecture, and management topics"* (Pyster, Olwell et al., 2015, p. 33). Considering that GRCSE part 3 builds on knowledge from part 2, this could indicate that many of the GSwE2009 topics relating to Part 3 would lack fundamental knowledge about that specific topic, which could contribute to hindering students' full understanding of SE for SwE students.

6.1.1 Focus Areas

This mapping shows that SwE's graduate curriculum, GSwE2009, shares many similarities with SE's GRCSE. This section discusses these results in the broader context of SwE, SE and IT professionals in ICS cybersecurity.

A total of 15 topics have been identified relevant to GRCSE in the GSwE2009 cybersecurity focus area. The topics supported an understanding of aspects relevant to cybersecurity; requirements engineering (in software development), configuration management, risk management, and verification and validation (V&V). However, none of the topics mentioned cybersecurity specifically.

Within the ML focus area, 19 topics were found to relate to GRCSE. However, they only cover the software development process, not software design or ML specifically. ML algorithms are more than just software development; the topics mapped (Table 4.2) would not provide SE graduates with sufficient insights into ML's fundamentals or technical aspects. AI and machine learning are becoming increasingly relevant to the ICS, and the future workforce should be familiar with these technologies regardless of their role in the industrial environment (Karampidis et al., 2019; Kipper et al., 2021; Ngambeki et al., 2022).

An increasing amount of ICS cybersecurity tools for ICS utilise ML, and they are often developed by IT personnel. However, the tools they develop are intended to communicate possible

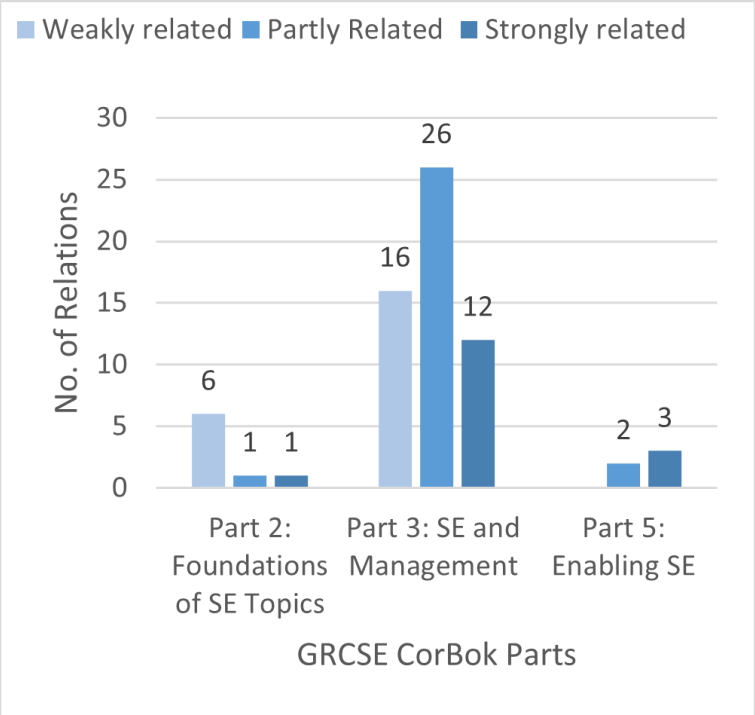


Figure 6.2: Distribution of the identified relations in GRCSE

threats in an understandable and relatable way to OT personnel (M.R. et al., 2021). OT experts with an understanding of ML can collaborate with IT developers to develop more effective AI/ML tools for securing the ICS.

In the focus area of soft skills, three GSwE2009 topics were mapped to GRCSE (table 4.3). The expected outcome of the first two topics from the KA "Ethical and Professional Conduct" is that graduates should have a fundamental understanding of ethical and professional conduct and laws and regulations. These high-level topics do not detail communication, teamwork, or leadership methods. In contrast, GRCSE has devoted part 5 to enabling businesses, teams, and individuals in SE. Both curricula cover process monitoring, but GRCSE emphasises risk management.

A total of 25 GSwE2009 topics relate to GRCSE within the focus area of systems engineering. Activities within these SwE topics can be found across several topics and KAs within GRCSE. It may be because GSwE2009 reads mainly like a *reference manual* containing detailed information about specific topics. GRCSE, on the other hand, provides KAs and topics within parts (parts 2-6) that connect to processes within the lifecycle of SE projects and systems. GRCSE is organised more like a "project handbook." As such, it provides a more comprehensive view of the entire systems lifecycle, while GSwE2009 focuses more on specific topics.

The mapping found that some topics' activities in GSwE2009 could be mapped to activities located in several different topics (and KAs) in GRCSE. Although the activities overlap, their terminology differs significantly. It is consistent with previous findings (McBride et al., 2020; Sheard. et al., 2018a; Turner et al., 2009), that the difference in vocabulary hinders mutual understanding and collaboration. In addition, other studies have mentioned difficulty in collaborating on projects due to miscommunication, an inability to understand each other's discipline, and a lack of respect for each other's contributions (Kasser & Shoshany, 2000; Sheard et al., 2018b; Towhidnejad et al., 2013).

6.2 Industry Perspective

Interviews with industry leaders revealed several interesting aspects of ICS cybersecurity. The following section presents and discusses the key findings based on the three interviews.

While participants A and B are OT educated and experienced in the ICS environment, participant C has an IT and development background. Despite the small sample size, the differences in backgrounds provide a broader perspective since they cover both IT and OT.

The increasing interconnection between IT and OT was reported by all participants, as well as the need for collaboration between the two. The use of the Security Operations Centre (SOC) for the ICS environments was noted by participants A and B. As neither SOC had personnel with OT competence, both participants reported that OT personnel actively collaborated with the SOC to protect the ICS. Participant A reported being the primary point of contact between the SOC and the OT personnel. However, the environment described by participant B was more collaborative, with several members from the OT department participating.

Cybersecurity competence in the ICS environment revealed several interesting responses, most notably the range of skills and competencies required to understand the various aspects of the ICS environment effectively. All participants acknowledged that IT and OT have significant differences, which must be considered. The skills and competencies emphasised the most in the interviews are listed below:

- Understanding fundamental ICS architecture is critical in IT-OT systems. This relates to cybersecurity, remote access, networking and monitoring.
- Operational knowledge is tied to a solid technical and hands-on understanding of OT technical elements. Participants tie this to a specific "mindset", including consequence thinking, system knowledge, system design, and criticality in ICS systems.
- IT-OT collaboration will be vital for protecting future ICS. All participants point to the increasing interconnection between IT and OT technology and the digitisation of the industry. Key skills for the future include remote access architecture monitoring and diagnosing, complex system architecture with interconnected IT and OT components, and networking competence related to data collection from complex systems.

The statement made by participant B regarding the "OT tribal language" is interesting since a difference in terminology is documented in academic literature as one of the main barriers to collaboration (see Chapter 2) going back over 20 years: *"A major barrier is the semantic barrier due to the different perceptions of the use of words"* (Kasser & Shoshany, 2000).

Participant C displayed a much more optimistic attitude towards machine learning and AI's potential in OT cybersecurity than participant B, corresponding to previous studies on IT and OT personnel having a very different outlook on how to bring new technology into an existing system (Sheard et al., 2019).

Concerning educating future ICS cybersecurity professionals, all participants highlighted the need for collaboration and interdisciplinary projects between IT and OT students. Suggestions included introductory courses in OT for IT students, incorporating more IT into OT education, and sharing methods and philosophies to foster collaboration and mutual understanding.

Lastly, the interviews revealed extensive challenges connected to the role of vendors in the ICS. Difficulties related to standardising, components control, cybersecurity and competence building trace back to how vendors operate in the OT space. Though not a focus of this thesis, it should be

considered that the current lack of control over vendors and the components they provide could be a contributing factor to IT-OT challenges:

- Vendors supply components based on functional requirements from the customer but are free to deliver any components that fit this description.
- Vendors require remote access to components. For instance, to perform maintenance or diagnose errors in functionality. Vendors often keep executive control over some of the functionality of components they supply.
- Challenges collecting data from components due to proprietary issues.

These could be aspect to address in future work (Chapter 7).

6.3 Connecting Academic and Industry Perspectives

Several discussion points can be identified based on the insights from the interviews and the systematic exploration of the curriculum mapping. This section discusses these themes in depth, combining the interpretations from the interview with those from the curriculum mapping and existing literature sources.

An emerging theme from the analysis is the interdependence of competency areas. This is reflected in the overlapping relationships between topics in the focus areas, such as cybersecurity, systems engineering, and machine learning, an overlap that signifies the depth of skills necessary for effective IT-OT collaboration. This interdependence is personified in participant A's view that an interchange of knowledge involving IT's cybersecurity expertise and OT's control system proficiency is crucial.

The curriculum mapping analysis revealed potential barriers to collaboration between IT and OT. As reflected in the interview data, there are apparent differences between software engineering and systems engineering perspectives, which may contribute to misunderstandings between IT and OT personnel. This nuance is most apparent in participant B's comment on the "OT tribal language". Competence and skill from both disciplines are needed to secure the ICS, making the language barrier particularly challenging. The analysis suggested that IT and OT personnel must be better educated in each other's fields to bridge the communication gap. Additionally, more collaboration between the two 'fields' could give students a better understanding of the opportunities and challenges in IT-OT systems.

An analysis of the curriculum mapping process indicates that foundational knowledge plays an important role. The predominance of relations allocated to GRCSE CorBOK part 3, which focuses on the application of SE, in contrast to part 2, which lays the theoretical foundation, illustrates potential deficiencies in basic knowledge. This reality echoes the concerns the interviewees, especially participant A, raised about the IT department's limited understanding of the OT environment. Thus, the curriculum mapping process can help identify areas of foundational knowledge that need bolstering to enhance mutual understanding and collaboration.

Equally significant is the role of soft skills in fostering effective communication and mutual understanding. A comparative analysis of GSwE2009 and GRCSE reveals a shortfall in soft skills coverage, particularly in risk management. This shortfall is reminiscent of the apprehensions expressed by the interviewees regarding interdepartmental communication, emphasising the role of soft skills in facilitating IT-OT collaboration.

Lastly, the challenge of disparate vocabulary is evident in the mapping and echoed in the interviews. The significant variation in terminologies between SwE and SE could be a potential barrier to effective communication between IT and OT departments.

In the findings from the curriculum mapping and the academic literature, the communication barriers, the rapidly changing landscape of OT environments, and the need for mutual understanding and knowledge exchange between IT and OT departments resonate with those expressed in the interviews. These observations highlight the complexity of IT-OT collaboration in ICS environments.

6.3.1 Including Habitus

Incorporating Pierre Bourdieu's habitus concept can further deepen IT-OT collaboration analysis within ICS environments. Habitus refers to the socially ingrained habits, skills, and dispositions individuals develop over time due to their experiences within specific social and institutional contexts.

By applying habitus to the IT and OT fields, we can view them as unique social realms with their own distinct habitus. For instance, the IT department, focusing on data management, security, and programming, develops certain dispositions, behaviours, and ways of thinking. On the other hand, the OT department, with its emphasis on physical equipment, processes and system up-time, cultivates a different habitus. These different 'habitus fields' influence how individuals in each field perceive and interpret their work and collaborative efforts.

The challenges noted in the interviews, such as communication barriers, differences in perspective, and the need for knowledge exchange, can be interpreted as clashes of habitus. The challenges arise when different habitus fields - IT and OT - interact within an ICS environment. Participant A's highlighting of the need for IT personnel to understand the criticality of processes within an OT environment can be seen as a call for a deeper appreciation of the OT's habitus. Similarly, Participant C's discussion about the gradual progression in integrating OT into security management reflects a gradual merging of habitus.

From a curriculum mapping perspective, the notable differences between the GSwE2009 and GRCSE can also be interpreted as reflections of distinct habitus. The divergence in emphasis, terminology, and coverage of topics may be viewed as a consequence of the separate social and institutional contexts from which software and systems engineering have developed. This divergence might also explain the lack of consistency in foundational knowledge in the curriculum mapping process, resulting from different habitus within the software and systems engineering disciplines.

Understanding and acknowledging these differences in habitus can facilitate the development of a shared understanding or a hybrid habitus. This considers IT and OT personnel's distinct dispositions, skills, and perspectives. A shared habitus could promote effective IT-OT collaboration and foster a more holistic approach to ICS cybersecurity. Therefore, a habitus-focused perspective contributes with a valuable dimension to understanding IT-OT collaboration dynamics, underscoring the importance of recognising and reconciling this diverse habitus to enhance collaboration in ICS environments.

6.4 Research Questions

This section presents how the work done in this thesis answers the research questions posed in Chapter 1.

RQ1: What are the skills and competencies required for ICS cybersecurity professionals, and how do they align with the graduate curriculum for IT and OT professionals?

The thesis addressed the research question by performing a curriculum mapping exercise on graduate programs intended for OT and OT professionals, specifically the GSwE2009 (software engineering) and GRCSE (systems engineering) curricula. In parallel, semi-structured interviews with experienced cybersecurity experts provided practical insights from the field.

Main findings:

- Curriculum mapping identified 67 relationships between cybersecurity, machine learning, soft skills, and system engineering. The study found overlaps and mismatches between the curriculum and the necessary skills identified by professionals. Cybersecurity focused on 15 relevant topics, but none specifically addressed cybersecurity. Instead, they supported risk management and configuration management.
- In the Machine Learning (ML) area, the curricula primarily focused on the software development process but lacked sufficient emphasis on ML's specific technical and design aspects. As AI and ML are increasingly relevant in ICS, there seems to be a mismatch between curriculum and industry needs.
- There were significant gaps in the curricula regarding soft skills such as communication, teamwork, and risk management.
- The focus on specialised topics rather than understanding the fundamental aspects of the systems lifecycle may cause SwE students to lack a basic understanding of systems engineering.

RQ2: What is the industry's need for skills and competencies in ICS cybersecurity, and how do IT-OT teams collaborate in the industry today?

This thesis examined the industry's need for ICS cybersecurity skills and competencies through semi-structured interviews with industry professionals. The IT and OT roles overlap and are becoming increasingly interdependent, making it necessary for professionals to possess a variety of skillsets.

Main findings:

- The industry's demand for foundational and soft skills and technical competencies. Both participants B and C stressed the importance of these skills in developing mutual understanding and effective collaboration.
- Participant A noted the existing terminological and understanding barriers between the two teams and stressed the importance of communicating between them. The 'OT tribal language' concept, as introduced by participant B, further demonstrated these barriers, illustrating a unique language OT teams use that can contribute to misunderstandings and miscommunications.
- Based on the interviews, measures could be taken to enhance the existing IT-OT collaboration, including developing a shared understanding and facilitating continuous knowledge exchange.

RQ3: Identify potential gaps between the industry and academia by comparing findings from RQ1 and RQ2.

We acquired both academic and industrial perspectives in order to identify gaps between academic and industry perspectives concerning ICS cybersecurity skills and competencies. The academic perspective was obtained by answering RQ1, whereas the industrial perspective was obtained by interviewing industry leaders, answering RQ2.

Main findings:

- The thesis identified several gaps between industry and academia in ICS cybersecurity. Despite the demand for a hybrid skillset in ICS cybersecurity, as established through RQ1, the thesis found that academic courses are often siloed, failing to provide this comprehensive perspective.
- ThThe academic curricula did not adequately address the issue of collaboration between IT and OT teams identified in RQ1, thereby contributing to the gap between theory and practice. It was found that academia lacked practical insights into the challenges faced by IT-OT teams, limiting its capacity to train future professionals to fill that gap. RQ2 analysis showed no industry-academia collaboration initiatives that could have enabled academia to remain current with industry requirements and trends.
- An understanding of habitus can help identify potential gaps between industry and academia. These gaps represent a disparity between the 'academic habitus' cultivated through education and the 'professional habitus' required by industry. ICS cybersecurity requires practical, technical skills in both IT and OT disciplines. The comparison indicates that academic curricula need to be updated to better align with industry's needs, thereby preparing graduates for careers in ICS cybersecurity.

6.5 Limitations of the study

6.5.1 Threats to validity

Curriculum mapping and GSwE2009 topics limit this study's results. Additionally, only SWEBOK was used to find information about GSwE2009 topics, whereas other sources might have given different results. Most topic descriptions in GSwE2009 are high-level, requiring subjective judgement in selecting topics for each focus area. The two curricula were systematically analysed and supported by a template guide. However, the curricula used in this study do not represent all universities' programs, limiting its scope. The mapping was based on publicly available data and might not have fully captured current practices or emerging trends in cybersecurity education.

Several factors could affect the outcome of the mapping process, including the selection of specific topics. Considering that there are no official frameworks or guidelines for Industry 4.0 skills and competencies, assessing the skills and competencies related to the four focus areas was challenging. Certain aspects must be considered for cybersecurity and machine learning skills and competencies. Several frameworks and curriculum guidelines identify cybersecurity skills and competencies, making discretion necessary. Without official curriculum guidelines or standards for ML, the definition of skills and competencies is subject to interpretation. While we aimed to follow best practices, some decisions were made based on practical considerations, potentially impacting the validity of the findings.

The semi-structured interview method employed in this study possesses strengths and weaknesses. While this approach enabled a comprehensive exploration of experiences and views, its open-ended nature can induce interviewer and interviewee bias and may lead to less standardisation and comparability between different interviewees.

In addition to the author's interview performance, personal biases and the ability to establish rapport can influence how questions are answered. While adherence to the prepared questions was followed, the varying depth and detail of responses received could affect the analysis and conclusions drawn. As the author works with ICS cybersecurity in her work at IFE, previous work can have influenced the choice of questions or which areas to follow up on during the interview. Not showing the participants the questions beforehand might have limited their ability to prepare and reflect on their responses. This could have affected their answers' depth and accuracy. However, this approach captured spontaneous responses and avoided rehearsed answers.

To accurately document interviews, transcription was needed. However, human error, misunderstandings, or failure to capture nonverbal cues could have affected the accuracy of the notes. It is possible that the accuracy of the information transcribed was affected by the fact that the first interview had a designated transcriber, while the interviewer transcribed the second and third interviews. Errors in the transcripts was mitigated by sending the transcripts to the participants after the interview, allowing them to correct any mistakes.

During data analysis, organising and interpreting responses carries the risk of misinterpretation or subjective bias, which could influence the conclusions drawn. The thematic content analysis employed in this study also carries validity threats. This approach relies heavily on the analyst's judgement and interpretations, introducing a potential source of bias. The identification, categorisation, and interpretation of themes are inherently subjective and could have been influenced by the author's other work within ICS cybersecurity.

The decision on what constitutes a theme can be another validity threat. The relevance of a theme is not determined by quantifiable measures. Instead, it is determined by whether it captures something meaningful about the data in relation to the research question. This leaves room for interpretation and subjectivity. Therefore, the risk of overemphasising or underemphasising certain themes could lead to a partial or distorted representation of the data. While thematic content analysis has inherent validity threats due to its interpretive nature, systematic analysis has mitigated these risks as much as possible.

The order of the activities, namely, curriculum mapping and interviews, might have influenced the results. Different insights might have been gained if the activities were performed in a different sequence, potentially changing the study's approach or focus. For instance, interview insights could inform a more targeted curriculum mapping or result in the decision to map other frameworks for educating ICS cybersecurity professionals.

Chapter 7

Conclusion

The objective of this thesis was to contribute to the understanding of the competence provided by graduate level curricula compared to industry needs and challenges in Industrial Control Systems (ICS) cybersecurity.

ICS presents unique and complex challenges in the evolving cybersecurity landscape. The interconnection of Information Technology (IT) and Operational Technology (OT) domains highlights the need for a comprehensive understanding of how these disciplines intersect within ICS.

To begin the study, a comprehensive curriculum map of the Graduate Reference Curriculum for Software Engineering (GSwE2009) and the Graduate Reference Curriculum for Systems Engineering (GRCSE) was performed to uncover potential gaps and overlaps in the educational frameworks of these domains. It revealed the differences between knowledge acquisition and application within the IT and OT fields.

The mapping results suggest an insufficient overlap between the topics and activities of GSwE2009 and GRCSE to impart the needed knowledge within these focus areas. The topic descriptions fail to provide sufficient details about the focus areas to allow a conclusion about their significance specifically to ICS cybersecurity to be drawn. Consequently, the result is a mapping of a broader set of skills and competencies, highlighting the differences and similarities between SwE and SE disciplines. Additionally, as highlighted above, cultural and traditional aspects of the teaching of SwE and SE may contribute to a gap between the disciplines. Soft skills have been identified as vital for ICS security, making it worthwhile to explore how SwE and SE can communicate and collaborate more comprehensively. To this end, focusing on bridging gaps between SwE and SE through collaboration and communication of soft skills can be a viable area of further exploration.

Next, interviews were conducted with experienced professionals from IT and OT backgrounds using a qualitative approach to gather in-depth, experiential insights about their collaboration in real-world ICS environments. The discussions revealed interesting aspects of their respective habitus, the ingrained behaviours, attitudes, and dispositions formed through shared experiences and environments. The findings have been analysed in light of Bourdieu's concept of habitus, illuminating how these professionals navigate the intricacies of ICS cybersecurity and how their collaborative dynamics shape the outcomes.

Main findings from connecting academic and industrial perspectives together:

- An interchange of knowledge involving ITs cybersecurity expertise and OTs control system proficiency is crucial.
- IT and OT personnel must be better educated in each others fields to bridge the communication gap.
- More collaboration between the two fields could provide students with a better understanding of the opportunities and challenges in IT-OT systems.
- The curriculum mapping process can help identify areas of foundational knowledge that need bolstering to enhance mutual understanding and collaboration.
- The significant variation in terminologies between software- and system engineering represents a barrier to effective communication between IT and OT departments.

The challenges noted in the interviews, such as communication barriers, differences in perspective, and the need for knowledge exchange, can be interpreted as clashes of habitus.

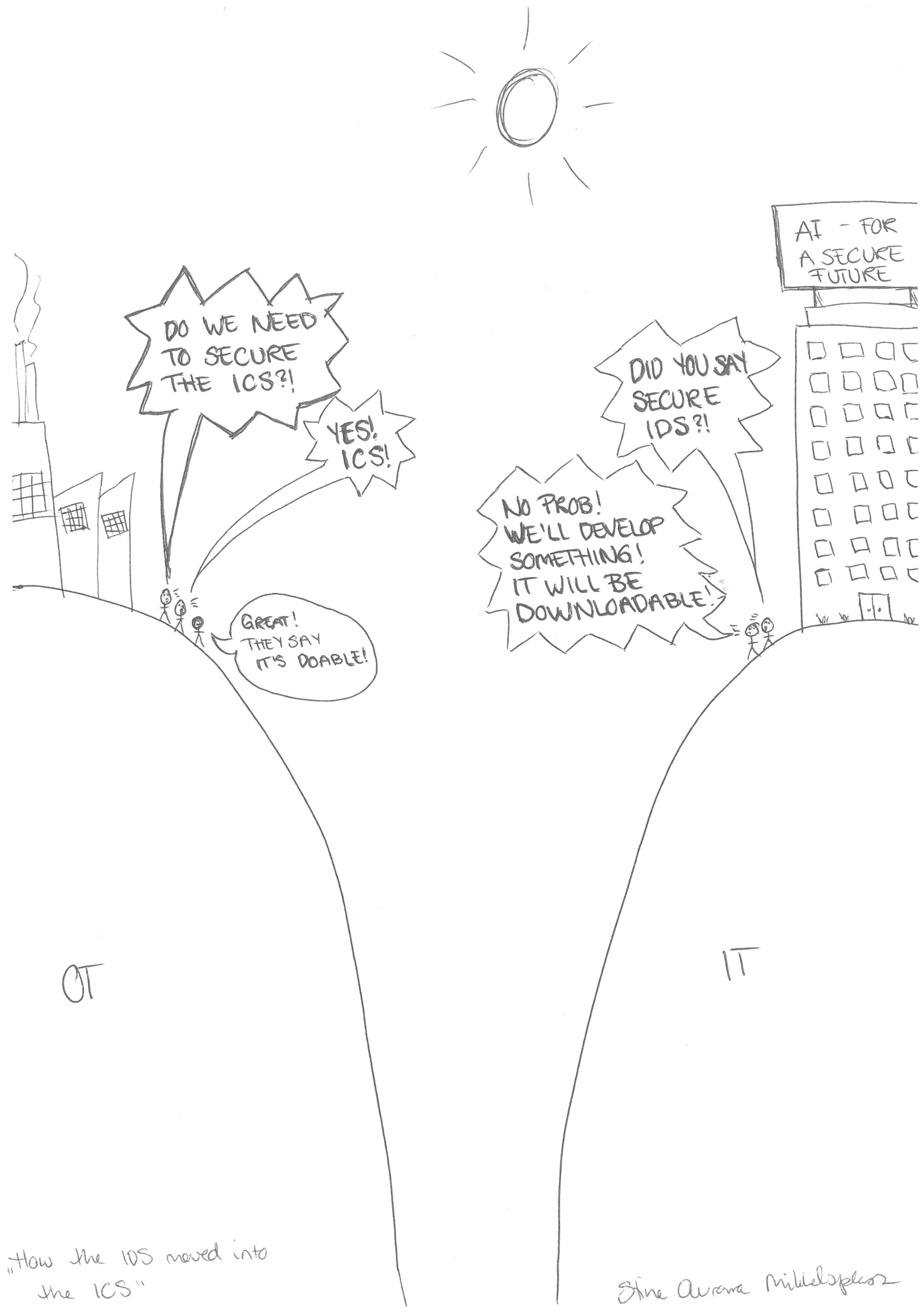
This thesis unveiled that while the IT and OT domains each bring distinct competencies, fostering effective collaboration between them is crucial for enhancing ICS cybersecurity. It underscores the need for a paradigm shift, moving from a silo approach to a collaborative framework where knowledge and skills from both disciplines can be applied collaboratively. In addition, this study demonstrates the importance of cross-disciplinary competencies and mutual understanding between IT and OT professionals.

7.1 Future Work

Future work can include exploring a collaborative framework where knowledge and skills from both software and system engineering disciplines can be applied collaboratively. To fully capture current practices and emerging trends in cybersecurity education, one could verify the mapping together with educational institutions.

Another aspect can be exploring the current lack of control over vendors and the components they provide, as they could contribute to IT-OT challenges. Key findings connected to ICS cybersecurity challenges related to competence building, asset management and cybersecurity that could to be addressed include:

- Vendors supply components based on functional requirements from the customer but are free to deliver any components that fit this description.
- Vendors require remote access to components and often keep executive control over some of the functionality of components they supply.
- Challenges collecting data from components due to proprietary issues.



„How the IDS moved into the ICS"

Stine Aurora Mikkelsplass

Bibliography

Armstrong, J. R., & Pyster, A. (1997). Resolved: Software Should Lead in Systems Engineering. *INCOSE International Symposium*, *7*(1), 317–324. https://doi.org/10.1002/j.2334-5837.1997.tb02188.x

Azmat, F., Ahmed, B., Colombo, W., & Harrison, R. (2020). Closing the Skills Gap in the Era of Industrial Digitalisation. *2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS)*, *1*, 365–370. https://doi.org/10.1109/ICPS48405.2020.9274788

Baldassarre, M. T., Caivano, D., Pino, F. J., Piattini, M., & Visaggio, G. (2012). Harmonization of ISO/IEC 9001:2000 and CMMI-DEV: From a theoretical comparison to a real case application. *Software Quality Journal*, *20*(2), 309–335. https://doi.org/10.1007/s11219-011-9154-7

Bigelow, S. J., & Lutkevich, B. (2021, August). *What is IT/OT Convergence? Everything You Need to Know*. IT Operations. Retrieved February 14, 2023, from https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence

Bloom, B. S. (1956). *Taxonomy of educational objectives: The classification of educational goals*. D. McKay Co.
OCLC: 1018252076.

Bourque, P., & Fairley (eds), R. E. (2014). *Guide to the software engineering body of knowledge*. IEEE Computer Society. www.swebok.org
OCLC: 880350861

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*(103614), 1–16. https://doi.org/10.1016/j.compind.2022.103614

Corporation, B. (2020, July 7). *Achieving successful IT/OT network convergence*. Industrial Ethernet Book. Retrieved March 27, 2022, from https://iebmedia.com/technology/iiot-industry-4-0/achieving-successful-it-ot-network-convergence/

CYFIRMA. (n.d.). *ChatGPT AI Cybersecurity Potential*. CYFIRMA. Retrieved January 6, 2023, from https://www.cyfirma.com/outofband/chatgpt-ai-cybersecurity-potential/

Ervin, L., Carter, B., & Robinson, P. (2013). Curriculum mapping: Not as straightforward as it sounds. *Journal of Vocational Education & Training*, *65*(3), 309–318. https://doi.org/10.1080/13636820.2013.819559

Fortinet. (2022, June 21). *2022 State of Operational Technology and Cybersecurity Report* (1578659-0-0-EN). Retrieved April 17, 2023, from https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf

Gan, T. H., Kanfoud, J., Nedunuri, H., Amini, A., & Feng, G. (2021). Industry 4.0: Why Machine Learning Matters? In L. Gelman, N. Martin, A. A. Malcolm & C. K. (Liew (Eds.), *Advances in Condition Monitoring and Structural Health Monitoring* (pp. 397–404). Springer Singapore. https://doi.org/10.1007/978-981-15-9199-0_37

Giray, G. (2021). A software engineering perspective on engineering machine learning systems: State of the art and challenges. *Journal of Systems and Software*, *180*(111031), 1–35. https://doi.org/10.1016/j.jss.2021.111031

Gjermundrød, H., Dionysiou, I., Baumberger, M., & Pattinson, M. (2016). An assessment of the ICT Security Skills in the Industrial Sector as Provided Through Education and Training. *MCIS 2016 Proceedings*, 1–12.

Greco, J. (2023, January 4). *The Rise of ChatGPT: How AI Plays a Vital Role In Cybersecurity*. Data Connectors. Retrieved January 6, 2023, from https://dataconnectors.com/the-rise-of-chatgpt-how-ai-plays-a-vital-role-in-cybersecurity/

Hemsley, K. E., & Fisher, R. E. (2018, December). *History of Industrial Control System Cyber Incidents* (Study INL/CON-18-44411-Revision-2). Idaho National Labs. Idaho, United States. https://doi.org/10.2172/1505628

Industroyer2: Industroyer reloaded [magazine]. (2022). *WeLiveSecurity*. Retrieved February 13, 2023, from https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Jeon, J. (2019). Rethinking Scientific Habitus: Toward a Theory of Embodiment, Institutions, and Stratification of Science. *Engaging Science, Technology, and Society*, *5*, 160–172. https://doi.org/10.17351/ests2019.303

John, S. N., Noma-Osaghae, E., Oajide, F., & Okokpujie, K. (2020). Cybersecurity Education: The Skills Gap, Hurdle! In K. Daimi & G. Francia III (Eds.), *Innovations in Cybersecurity Education* (pp. 361–376). Springer International Publishing. https://doi.org/10.1007/978-3-030-50244-7_18

Joint Task Force on Cybersecurity Education. (2018). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Association for Computing Machinery. https://doi.org/10.1145/3184594

Joint Task Force Transformation Initiative. (2011). *Managing information security risk :: Organization, mission, and information system view* (0th ed., NIST SP 800-39). National Institute of Standards and Technology. Gaithersburg, MD, USA. https://doi.org/10.6028/NIST.SP.800-39

Karampidis, K., Panagiotakis, S., Vasilakis, M., Markakis, E. K., & Papadourakis, G. (2019). Industrial CyberSecurity 4.0: Preparing the Operational Technicians for Industry 4.0, 1–6. https://doi.org/10.1109/CAMAD.2019.8858454

Kasser, J., & Shoshany, S. (2000). Systems engineers are from Mars, software engineers are from Venus. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cb890d41bf72b252ce573c31c0c92a4490cc1a93

Kipper, L. M., Iepsen, S., Dal Forno, A. J., Frozza, R., Furstenau, L., Agnes, J., & Cossul, D. (2021). Scientific mapping to identify competencies required by industry 4.0. *Technology in Society*, *64*, 101454. https://doi.org/10.1016/j.techsoc.2020.101454

Kumeno, F. (2019). Software engineering challenges for machine learning applications: A literature review. *Intelligent Decision Technologies*, *13*(4), 463–476. https://doi.org/10.3233/IDT-190160

Kuttolamadom, M., Wang, J., Griffith, D., & Greer, C. (2020). Educating the Workforce in Cyber and Smart Manufacturing for Industry 4.0. *ASEE Annual Conference Exposition Proceedings*. Retrieved March 27, 2022, from https://par.nsf.gov/biblio/10178926-educating-workforce-cyber-smart-manufacturing-industry

Lee, K. (2018). Deploying operational data to an OT/IT cloud [magazine]. *Industrial Ethernet Book*. Retrieved March 28, 2022, from https://iebmedia.com/technology/edge-cloud/deploying-operational-data-to-an-ot-it-cloud/

Malatras, A., Skouloudi, C., & Koukounas, A. (2019, May). *Industry 4.0 - Cybersecurity Challenges and Recommendations*. European Union Agency for Network and Information Security (ENISA), Attiki, Greece. Retrieved March 27, 2022, from https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

Maleh, Y. (2021). IT/OT convergence and cyber security. *Computer Fraud & Security*, *2021*(12), 13–16. https://doi.org/10.1016/S1361-3723(21)00129-9

McBride, S., Schou, C., & Slay, J. (2020). *A Security Workforce to Bridge the IT-OT Gap*. https://industrialcyberforce.org/wp-content/uploads/2020/08/A-Security-Workforce-to-Bridge-the-IT-OT-Gap.pdf
Industrial Cybersecurity Workforce Development.

Menzies, T. (2020). The Five Laws of SE for AI [magazine]. *IEEE Software*, *37*(1), 81–85.

Michalec, O., Milyaeva, S., & Rashid, A. (2022). Reconfiguring governance: How cyber security regulations are reconfiguring water governance. *Regulation & Governance*, *16*(4), 1325–1342. https://doi.org/10.1111/rego.12423

Mouzelis, N. (2008). Habitus and Reflexivity: Restructuring Bourdieu's Theory of Practice. *Sociological Research Online*, *12*(6), 123–128. https://doi.org/10.5153/sro.1449

M.R., G. R., Ahmed, C. M., & Mathur, A. (2021). Machine learning for intrusion detection in industrial control systems: Challenges and lessons from experimental evaluation. *Cybersecurity*, *4*(1), 1–12. https://doi.org/10.1186/s42400-021-00095-5

Murray, G., Johnstone, M., & Valli, C. (2017). The convergence of IT and OT in critical infrastructure. *Australian Information Security Management Conference*. https://doi.org/10.4225/75/5a84f7b595b4e

Muscarella, S., Osaisai, M., & Sheard, S. (2020). Systems and Software Interface Survey. *INCOSE International Symposium*, *30*(1), 1305–1323. https://doi.org/10.1002/j.2334-5837.2020.00787.x

Nascimento, E., Nguyen-Duc, A., Sundbø, I., & Conte, T. (2020). Software engineering for artificial intelligence and machine learning software: A systematic literature review. *arXiv e-prints*, 1–68. https://doi.org/10.48550/arXiv.2011.03751

Ngambeki, I., McBride, S., & Slay, J. (2022). Knowledge Gaps in Curricular Guidance for ICS Security. *Journal of The Colloquium for Information Systems Security Education*, *9*(1), 1–6. Retrieved March 27, 2022, from http://cisse.info/journal/index.php/cisse/article/view/149

Ngambeki, I., Spafford, E., Ansari, S., Alhasan, I., Basil-Camino, M., & Rapp, D. (2021). Creating a Concept Map for ICS Security A Delphi Study. *2021 IEEE Frontiers in Education Conference (FIE)*, 1–7. https://doi.org/10.1109/FIE49875.2021.9637386

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, *13*, 1253–1260. https://doi.org/10.1016/j.promfg.2017.09.047

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020, November 16). *Workforce Framework for Cybersecurity (NICE Framework)* (NIST Special Publication 800-181 REV. 1). National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.SP.800-181r1

Pyster, A. (2009, September 30). *Graduate Software Engineering 2009 (GSwE2009): Curriculum Guidelines for Graduate Degree Programs in Software Engineering.* Stevens Institute of

Technology. Retrieved March 28, 2022, from https://www.acm.org/binaries/content/assets/education/gsew2009.pdf

Pyster, A., Adcock, R., Ardis, M., Cloutier, R., Henry, D., Laird, L., Lawson, H. B., Pennotti, M., Sullivan, K., & Wade, J. (2015). Exploring the Relationship between Systems Engineering and Software Engineering. *Procedia Computer Science*, *44*, 708–717. https://doi.org/10.1016/j.procs.2015.03.016

Pyster, A., Olwell, D., Ferris, T., Hutchison, N., Enck, S., Anthony, J., Henry, D., & Squires, A. ((2015). *Graduate Reference Curriculum for Systems Engineering (GRCSE) V1.1*. Trustees of the Stevens Institute of Technology. Hoboken, NJ, USA. www.bkcase.org/grcse/

Ramsey, G. (2023, March 16). *Pierre Bourdieu & Habitus (Sociology): Definition & Examples*. Retrieved May 19, 2023, from https://simplysociology.com/pierre-bourdieu-habitus.html

Rawle, F., Bowen, T., Murck, B., & Hong, R. (2017). Curriculum Mapping Across the Disciplines: Differences, Approaches, and Strategies. *Collected Essays on Learning and Teaching*, *10*, 75–88. https://doi.org/10.22329/celt.v10i0.4765

Rech, J., & Althoff, K. D. (2004). Artificial Intelligence and Software Engineering: Status and Future Trends. *KI*, *18*(3), 5–11.

Robley, W., Whittle, S., & MurdochEaton, D. (2005a). Mapping generic skills curricula: A recommended methodology. *Journal of Further and Higher Education*, *29*(3), 221–231. https://doi.org/10.1080/03098770500166801

Robley, W., Whittle, S., & MurdochEaton, D. (2005b). Mapping generic skills curricula: Outcomes and discussion. *Journal of Further and Higher Education*, *29*(4), 321–330. https://doi.org/10.1080/03098770500353342

Robson, C. (2011). *Real world research: A resource for users of social research methods in applied settings* (3. ed). Wiley.

Salkind, N. J. (2018). *Exploring research* (Ninth, global edition., Vol. Ninth, global edition). Pearson.

Sánchez-Gordón, M.-L., & Colomo-Palacios, R. (2018). From Certifications to International Standards in Software Testing: Mapping from ISQTB to ISO/IEC/IEEE 29119-2. In X. Larrucea, I. Santamaria, R. V. O'Connor & R. (Messnarz (Eds.), *Systems, Software and Services Process Improvement* (pp. 43–55). Springer International Publishing. https://doi.org/10.1007/978-3-319-97925-0_4

Sarker, I. H. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, *2*(3), 160. https://doi.org/10.1007/s42979-021-00592-x

SEBoK Editorial Board. (2021, October 15). *Guide to the Systems Engineering Body of Knowledge (SEBoK), Version 2.5*. The Trustees of the Stevens Institute of Technology. Retrieved February 10, 2022, from http://www.sebokwiki.org/

Sheard, S. (2014, April 19). *Needed: Improved Collaboration Between Software and Systems Engineering*. Carnegie Mellon University's Software Engineering Institute Blog. Retrieved January 11, 2023, from https://insights.sei.cmu.edu/blog/needed-improved-collaboration-between-software-and-systems-engineering/

Sheard., S., Cadigan, J., Chim, L., Creel, R., Marvin, J., & Pafford, M. E. (2018a). INCOSE Working Group Addresses System and Software Interfaces. *INCOSE International Symposium*, *28*(1), 456–474. https://doi.org/10.1002/j.2334-5837.2018.00493.x

Sheard, S., Creel, R., Cadigan, J., Marvin, J., Chim, L., & Pafford, M. E. (2018b). INCOSE Working Group Addresses System and Software Interfaces. *INSIGHT*, *21*(3), 62–71. https://doi.org/10.1002/inst.12213

Sheard, S., Pafford, M. E., & Phillips, M. (2019). Systems EngineeringSoftware Engineering Interface for Cyber-Physical Systems. *INCOSE International Symposium*, *29*(1), 249–268. https://doi.org/10.1002/j.2334-5837.2019.00602.x

Siemers, B., Attarha, S., Kamsamrong, J., Brand, M., Valliou, M., Pirta-Dreimane, R., Grabis, J., Kunicina, N., Mekkanen, M., Vartiainen, T., & Lehnhoff, S. (2021). Modern Trends and Skill Gaps of Cyber Security in Smart Grid : Invited Paper. *IEEE EUROCON 2021 - 19th International Conference on Smart Technologies*, 565–570. https://doi.org/10.1109/EUROCON52738.2021.9535632

Slayton, R., & Clark-Ginsberg, A. (2018). Beyond regulatory capture: Coproducing expertise for critical infrastructure protection. *Regulation & Governance*, *12*(1), 115–130. https://doi.org/10.1111/rego.12168

Smit, J., Kreutzer, S., Moeller, C., & Carlberg, M. (2016). *Industry 4.0 Analytical Study* (Study PE 570.007). Policy Department A: Economic and Scientific Policy. European Union. Retrieved January 23, 2023, from https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf

Sohime, F. H., Ramli, R., Rahim, F. A., & Bakar, A. A. (2020). Exploration Study of Skillsets Needed in Cyber Security Field. *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, 68–72. https://doi.org/10.1109/ICIMU49871.2020.9243448

Stølen, K. (2019). *Teknologivitenskap: Forskningsmetode for teknologer*. Universitetsforlaget OCLC: 1350631410.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015, June). *Guide to Industrial Control Systems (ICS) Security* (NIST SP 800-82r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., & Samaka, M. (2018). SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet*, *10*(8), 76. Retrieved May 5, 2022, from https://www.mdpi.com/1999-5903/10/8/76

Towhidnejad, M., Hilburn, T., & Fairley, R. (2013). Software and System Engineering Education: Commonalities and Differences. *2013 ASEE Annual Conference & Exposition Proceedings*, 23.1074.1–23.1074.10. https://doi.org/10.18260/1-2--22459

Turner, R., Pyster, A., & Pennotti, M. (2009). Developing and validating a framework for integrating systems and software engineering. *2009 3rd Annual IEEE Systems Conference*, 407–412. https://doi.org/10.1109/SYSTEMS.2009.4815836

Uchiyama, K. P., & Radin, J. L. (2009). Curriculum Mapping in Higher Education: A Vehicle for Collaboration. *Innovative Higher Education*, *33*(4), 271–280. https://doi.org/10.1007/s10755-008-9078-8

Veltri, N. F., Webb, H. W., Matveev, A. G., & Zapatero, E. G. (2011). Curriculum Mapping as a Tool for Continuous Improvement of IS Curriculum. *Journal of Information Systems Education*, *22*, 13.

Wade, J., Gerardo, H., & Sorenson, H. (2022). Systems Engineering Competency Expectations, Gaps, and Program Analysis. *INCOSE International Symposium*, *32*(1), 1359–1372. https://doi.org/10.1002/iis2.13000

Walk, K. (1998). How to Write a Comparative Analysis [magazine]. *The Writing Center at Harvard University*. Retrieved June 6, 2023, from https://writingcenter.fas.harvard.edu/pages/how-write-comparative-analysis

Wei, Y.-Y., Chen, W.-F., Xie, T., & Peng, J.-J. (2022). Cross-disciplinary curriculum integration spaces for emergency management engineering talent cultivation in higher education. *Computer Applications in Engineering Education*, *30*(4), 1175–1189. https://doi.org/10.1002/cae.22513

Wray, R. B. (1993). Systems Engineering and Software Engineering: Cooperative or Competitive? *INCOSE International Symposium*, *3*(1), 833–843. https://doi.org/10.1002/j.2334-5837.1993.tb01667.x

Zorz, Z. (2022, April 12). *Sandworm hackers tried (and failed) to disrupt Ukraine's power grid*. Help Net Security. Retrieved February 6, 2023, from https://www.helpnetsecurity.com/2022/04/12/sandworm-ukraine/

Appendix A

Submitted Manuscript for Journal Article

The article was submitted to *International Journal of Human Capital and Information Technology Professionals*[1] (IJHCITP) early 2023 and is currently under review.

[1] https://www.igi-global.com/journal/international-journal-human-capital-information/1152

Software and Systems Engineers in ICS security: a study on their competences

Stine Aurora Mikkelsplass[1], Ricardo Colomo-Palacios[1], John Eidar Simensen[2]

[1] Østfold University College, Halden, Norway

[2] Institute for energy technology, Halden, Norway

Abstract: The introduction of IIoT has enabled the interconnection of IT-OT systems and exposed the industrial control system to cyber threats. Industrial cybersecurity requires knowledge and skill within both IT and OT technology, which relies on the collaboration between IT – and OT personnel. This study examines two disciplines who fits these roles: software engineering and systems engineering. The graduate curriculum of software engineering (GSwE2009) and systems engineering (GRCSE) are then mapped to identify overlapping competence within ICS cybersecurity. The result of this mapping is then discussed in the context of software- and systems engineering in the context of ICS cybersecurity.

Keywords: systems engineering, software engineering, cybersecurity, skills gap, machine learning, curriculum mapping, industrial control systems.

Introduction

The fourth industrial revolution (Industry 4.0) refers to the technological progress across industries. Industry 4.0 describes "the organisation of production processes based on technology and devices autonomously communicating with each other along the value chain: a model of the 'smart' factory of the future where computer-driven systems monitor physical processes." (Smit et al., 2016, p. 20). The cornerstone of digital transformation in Industry 4.0 is the interconnection of information technology (IT) and operation technology (OT)[i]. With the emergence of the Industrial Internet of Things (IIoT), industries have found new ways to manage, maintain, and further develop their operations (Belden Corporation, 2020). Examples of this include, but are not limited to: extensive data collection from the OT environment, remote monitoring of operations, and optimising operations through automation (Belden Corporation, 2020; Lee, 2018). Software is a fundamental part of modern engineering systems, also called cyber-physical systems (CPS), and as such software engineering (SwE) and systems engineering (SE) are both fundamental to the maintenance and development of complex systems (Pyster, Adcock, et al., 2015; Sheard et al., 2019). However, despite their significant roles in the fast-developing industry, the relationship between SwE and SE is

not well defined (Pyster, Adcock, et al., 2015). This issue has been debated since the 1990s (Armstrong & Pyster, 1997; Wray, 1993), and as recently as 2018, the International Council on Systems Engineering (INCOSE) started a working group exclusively to meet these challenges, the *Systems and Software Interface Working Group* (SaSIWG) (Sheard. et al., 2018).

As the digitisation of industrial control systems (ICS) poses new challenges on how to collect, sense-make and apply these data, machine learning (ML) is one of the key applications to aid in the management and sensemaking of large amounts of data in Industry 4.0 (Sarker, 2021). ML models have adapted swiftly to the increasing amount of available data. Not only are ML techniques used to sense-make data for business value, but it also extensively used for cybersecurity monitoring and anomaly detection in ICS (Teixeira et al., 2018). As the interconnection of IT- and OT systems allows for new opportunities, it also introduces new threats to the industrial environment. In recent years, there have been several noticeable cyber-attacks on OT environments where attackers have exploited IT vulnerabilities to access OT technology. For instance, in the Ukraine April 2022 attacks, a hacker group believed to have strong ties to the Russian Chief Intelligence Office[ii] (GRU) launched a series of malware to disrupt the Ukrainian power grid[iii,iv]. This attack coincided with Russia's invasion of Ukraine. Most recently, the AI Chatbot ChatGPT[v] has been found to aid in the development of malware for SCADA systems ('ChatGPT AI Cybersecurity Potential', n.d.; Greco, 2023), lowering the threshold for skill and competence needed to deploy attacks against the ICS environment.

Fundamental support functions and services in modern society, such as water treatment, transportation, and energy systems, rely upon ICS. As these systems become more complex and interdependent, there is a need for cybersecurity professionals who understand both the IT and the OT environment. Recent literature states that there currently is a lack of skill and competence in this area, as well as significant challenges related to educating and developing the workforce needed to secure critical industrial systems[vi] (Corallo et al., 2022; Kuttolamadom et al., 2020; Malatras et al., 2019; Maleh, 2021; Ngambeki et al., 2022; Simmers et al., 2021). Unlike ICS security, IT security has a

long history of frameworks, guidelines, and standards for managing their systems. As a result, the recruitment and organisation of professionals for ICS cybersecurity teams is often the responsibility of IT professionals, such as information security managers or Chief Information Security Officers (CISOs) (Michalec et al., 2022; Stouffer et al., 2015). Fortinet (2022) reports that 52% of OT security professionals state that all monitoring and tracking of OT activities is done by the same Security Operations Centre (SOC) that safeguards a company's information technology, i.e., IT professionals. The same report indicates that 79% of OT security professionals anticipate that OT security will fall under CISO responsibilities in the near future, further underlining the importance of IT professionals in ICS security. Consequently, IT professionals are crucial for the successful implementation and management of ICS security, and their involvement in this process will likely increase as ICS environments become increasingly digitised.

The reported study, as part of ongoing master thesis project, compares the competence of graduates within software engineering (SwE) and systems engineering (SE) by mapping their respective curricula GSwE2009 (Pyster, 2009) and GRCSE (Pyster, Olwell, et al., 2015). The disciplines of SwE and SE are chosen for this study because of their required competence in maintaining and developing complex systems (Sheard et al., 2019). This mapping considers skills and competence related to four focus areas: cybersecurity, machine learning, soft skills, and systems engineering. The importance of skill and competence within these focus areas into key competence for ICS and Industry 4.0 cybersecurity is supported by previous studies (Chowdhury & Gkioulos, 2021; Karampidis et al., 2019; Kipper et al., 2021; Von Solms & Futcher, 2018). This paper is structured as follows: Section 2 describes the background. Section 3 presents the method and mapping used in this study. Section 4 presents the curriculum mapping results, while section 5 analyses the relations mapped in the previous section. In section 6, the results are discussed within the context of the security of ICS, while in section 7, concluding remarks are provided.

Background

The background is divided into four subsections where the first three provide an overview of cybersecurity's key challenges and concepts in Industry 4.0. Of these, the first subsection describes the challenges of interconnected IT-OT systems. In the second, the evolution of cybersecurity in ICS is presented, with an introduction to challenges related to IT-OT systems. A presentation on the role of machine learning (ML) in Industry 4.0 follows in the third. The fourth subsection describes the graduate curricula for systems and software engineering.

Challenges of an IT-OT environment

Industrial control systems are traditionally associated with technology such as programmable logic controllers (PLCs), sensors, actuators, human-machine interfaces (HMIs) and remote terminal units (RTUs). OT devices are built to operate in industrial settings and harsh environments, intended for 20+ years of use without the need for regular updates and maintenance. Safety has been the critical driver in OT design principles, a prerequisite to protecting people, processes, and systems (Joint Task Force Transformation Initiative, 2011). ICS often rely on continuous uptime, and therefore dependability and reliability are the main drivers of OT devices. In contrast, information technology is built for continuous hardware and software updates (Bigelow & Lutkevich, 2021).

Cybersecurity in ICS

Industrial systems and networks have historically been considered isolated and "air-gapped" from the outside world. It has been argued that cyber security is of no concern for ICS. However, events such as the *Stuxnet* attack in 2010 and the *Havex* attack in 2013 (Hemsley & Fisher, 2018) prove that ICS environments are not as isolated as once thought. The adoption of smart sensors and the development of the IIoT has opened for increased connectivity in ICS environments, as the IIoT function as a bridge between IT and OT[vii], enabling industrial networks to be accessed through the Internet (Belden Corporation, 2020). The attack on the Ukrainian power grid is an example of a threat actor exploiting exactly this by attacking OT systems through IT vulnerabilities. The attack

started by hacking into the IT network, from where the attacker managed to gain access to the ICS network (*Industroyer2*, 2022).

Machine Learning in Industry 4.0

With increased connectivity and extensive use of smart sensors, it is possible to gather vast amounts of data from ICS environments. This development supported the creation of several big data applications and machine learning approaches for industries to use these data (Gan et al., 2021). Machine learning models, including artificial intelligence (AI), can quickly sort through vast data points with effective decision-making capabilities on real-time data. Within specialised ICS security tools and IDSs, machine learning methods and artificial intelligence techniques have become increasingly common. ML algorithms are frequently promoted as a key security feature of IDSs and other security tools (Sarker, 2021), for instance to identify patterns that indicate abnormal processes or network data behaviour.

The Software Engineering Curriculum and the Systems Engineering Curriculum

The *Graduate Software Engineering Curriculum 2009 (*GSwE2009*)* (Pyster, 2009) and the *Graduate Reference Curriculum for Systems Engineering (*GRCSE*)* (Pyster, Olwell, et al., 2015) are guidelines for their respective graduate degree programs. They aim to standardise the education for software engineers and systems engineers across educational institutions and to ensure the quality of education for graduating students.

Both curricula have developed a *Core Body of Knowledge,* building on the *Software Engineering Body of Knowledge* (SWEBOK) (Bourque & Fairley (eds), 2014) and the *Systems Engineering Body of Knowledge* (SEBoK) (SEBoK Editorial Board, 2021). Both have identified *Core Concepts* or *Fundamental Knowledge* that should be a part of the curriculum for all master's degree graduates within their field, covering approximately 50% of the curriculum in both cases. The remaining 50% is dedicated to specialised topics or training. The concepts of the CBOK (SwE) or CorBOK (SE) are grouped into *Knowledge Areas* (KA), which are further divided into *topics* and s*ub-topics*.

The Method of Curriculum Mapping

The GSwE2009 and GRCSE curricula reflect the expected learning outcomes for graduates within software and systems engineering. This study uses curriculum mapping to compare topics and activities from GSwE2009 to GRCSE to create a visual representation of the relationship between these curricula in the focus areas of cybersecurity, machine learning, soft skills, and systems engineering.

Models' analysis

This mapping began with an analysis of the SwE and SE curricula to identify their similarities and differences. Both curricula structure their Core Body of Knowledge into Knowledge Areas, Topics, and Subtopics. Bloom's Taxonomy Cognitive Levels (Bloom, 1956) provide information on the suggested cognitive level for each topic or subtopic. The SwE and SE curricula were studied to identify topics within cyber security, machine learning and soft skills.

Mapping design

This mapping was designed to compare these two graduate curricula and analyse the results of this activity. The following steps were taken:

1. Identify KAs and topics within GSwE2009 that relate to cybersecurity, machine learning, soft skills, or systems engineering. Topics identified were then analysed in terms of description in SWEBOK, learning outcomes and Bloom cognitive level.
2. The direction of comparison is from GSwE2009 to GRCSE.
3. The comparison scale applied in this study is adapted from previous work (Baldassarre et al., 2012; Sánchez-Gordón & Colomo-Palacios, 2018). There are four categories:
    - *Strongly related* (●): the topic is specially named in the curricula and is classified to one or more of the same Bloom cognitive levels.
    - *Partially related* (◑): the topic is not specially named, but one or more sub-topics have activities that correlate to activities in the GRCSE curriculum.

- *Weakly related* (◔): the topic is not specially named, but one sub-topic has activities that can be adapted to an activity in the SE curriculum.
- *Not related* (○): the topic or activity is mentioned, but only a high-level summary is given in the SE curriculum. No relationship between competencies can be identified.

4. Comparison template definition: This comparison was an iterative process, analysing and considering topics from both curricula in the context of their respective disciples and the focus areas.

Mapping execution

The first author performed an iterative mapping process, studying both curricula to understand their structures, scopes, and objectives. For each of the areas, cybersecurity, machine learning, systems engineering, and soft skills, identifying skills and competencies was performed as detailed in section *Outcomes*. The identified skills and competencies were used to analyse topics in GSwE2009 for similar activities. The identified topics were detailed in a spreadsheet with associated focus area, *Knowledge Area*, *topic name* and *Bloom Cognitive Level.* Topic name and activities were used to examine GRCSE and SEBOK for related activities, with identified GRCSE topics added to the spreadsheet with respective *Knowledge Area, topic name* and *Bloom Cognitive Level.* This provided a high-level overview of relations between the curricula. To gain a more comprehensive understanding of these relationships both curricula were re-examined with attention to activity details, updating the spreadsheet in accordance with new findings. The remaining relations were analysed one final time and mapped according to the comparison scale, described in subsection Mapping *Execution* The re-examination step also served as a verification of the described mapping execution. The overall validation of the steps was provided by the second and third authors as part of the MSc work evaluation process.

Bloom Cognitive Levels Mapping

Both SwE and SE curricula use Bloom's Cognitive Levels to describe the expected comprehension level for graduate students within specific topics of the KAs. A mapping of these levels was performed to ensure their comparability. Both curricula have identified what competence should be associated with the different cognitive levels of Bloom's Taxonomy: *Knowledge, Comprehension, Application, Analysis, Synthesis* and *Evaluation*. By identifying *core skills* and *domain-specific focus* (core responsibilities given field of study) associated with each competency level for both curricula, it was possible to analyse how the curricula defined competency on a given level. The mapping process and comparison scale follow the same methods as the curriculum mapping detailed above and range from strongly related to un*related.* The skills described in *Knowledge, Comprehension, Application, Analysis* and *Evaluation* are practically indistinguishable and, therefore, strongly related. The skills associated with *Synthesis*, however, are only partially related. Neither *Synthesis* nor *Evaluation* is used to describe the cognitive levels of any identified topics in either curriculum and is therefore not considered further. This mapping showed that the Bloom cognitive levels from GSwE2009 and GRCSE are comparable for this study.

Outcomes

Presented in this section are the mapping results. Table 3-Table 6 presents results for the four focus areas (see section *Introduction*). Each section will discuss topics identified as having strong relationships; topics previously discussed are not repeated.

SE curriculum Knowledge Areas (KA) are divided into Parts (Table 1) based on their location in the CRCSE CorBOK. Table 2 shows the KAs within GSwE2009, represented by the letters A-K. Only relevant SwE topics are listed in full to keep the tables legible. The GRCSE, GSwE2009, SWEBOK, and SEBOK were used to find details about topic activities.

Table 1: GRCSE Knowledge Areas

GRCSE Knowledge Areas	
Part 2:	Foundations of SE Topics
Part 3:	SE and Management
Part 4:	Applications of SE
Part 5:	Enabling SE
Part 6:	Related Disciplines

Table 2: GSwE2009 Knowledge Areas

GSwE2009 Knowledge Areas	
A:	Ethical and Professional Conduct
B:	Systems Engineering
C:	Requirements Engineering
D:	Software Design
E:	Software Construction
F:	Testing
G:	Software Maintenance
H:	Configuration Management
I:	Software Engineering Management
J:	Software Engineering Process
K:	Software Quality

Cyber security

Topics in GSwE2009 relevant to cyber security competence are presented in Table 3. Based on NIST 800-181 (Petersen et al., 2020), the National Initiative for Cybersecurity Education's Cybersecurity Workforce Framework details the knowledge and skills required for cybersecurity work. As part of identifying topics for cybersecurity, this framework was used in conjunction with Knowledge Areas in the Cybersecurity Curricula 2017 (Joint Task Force on Cybersecurity Education, 2018).

Table 3: Cyber security topics (GSwE2009) to GRCSE mapping

GSwE2009 topics		*GRCSIE CorBOK*				
		Part 2	*Part 3*	*Part 4*	*Part 5*	*Part 6*
C.1	Fundamentals of Requirements Engineering	◔	◑			
C.2	Requirements Engineering Process		◑			
C.3	Initiation and Scope Definition					○
C.4	Requirements Elicitation		●			
C.5	Requirements Analysis		◑			
C.6	Requirements Specification		◑			
C.7	Requirements Validation	◔	◑			
C.8	Practical Considerations		◑			
D.	Software Design					○
E.1	Software Construction Fundamentals					○
E.3	Practical Considerations					○
G.2	Key Issues in Software Maintenance					○
G.4	Techniques for Maintenance					○
H.1	Management of the CM Process		●			
H.2	Configuration Identification		◔			
H.3	Configuration Control		◔			
H.4	Software Configuration Status Accounting		◔			
H.5	Software Release Management					○
I.2	Risk Management		◑			
J.4	Product and Process Management					○
K.1	Software Quality Fundamentals					○
K.3	Verification and Validation (V&V)		●			

C.4 “Requirements Elicitation” is strongly related to “Concept Definition” in Part 3 of GRCSE. Both emphasise requirements sources, stakeholder requirements and activities for requirements elicitation, and *application* is the required Bloom cognitive level for both.

H.1 “Management of the CM Process” strongly relates to GRCSE Part 3 “SE Management”, sub-topic “Configuration Management”. The topics cover planning, organisation, and constraints for

configuration management, and both curricula require competence level *comprehension*, though GSwE2009 specifies *comprehension/application*.

K.3 “Verification and Validation (V&V)” is strongly linked to the topic “System Verification” and “System Validation” in the KA “System Realization” in GRCSE Part 3. Tough GSwE2009 refers specifically to software development methods, identifying V&V scope, testing techniques, and evaluating target capabilities overlap with GRECE. Both curricula require Bloom level *application.*

Machine Learning

The skills and competence needed to develop machine learning algorithms relate to the disciplines of SwE and Data Science (IABAC, 2019). These curricula and previous work done concerning the ML in SwE (Giray, 2021; Kumeno, 2019; Menzies, 2020; Nascimento et al., 2020; Rech & Althoff, 2004) informed the selection of topics in Table 4.

Table 4: Machine Learning topics (GSwE2009) to GRCSE mapping

GSwE2009 topics		*GRCSIE CorBOK*				
		Part 2	Part 3	Part 4	Part 5	Part 6
A.2	Codes of ethics and professional conduct				●	
A.3	The nature and role of software engineering standards					○
C.1	Fundamentals of Requirements Engineering	◔	◑			
C.2	Requirements Engineering Process		◑			
C.3	Initiation and Scope Definition					○
C.4	Requirements Elicitation		●			
C.5	Requirements Analysis		◑			
C.6	Requirements Specification		◑			
C.7	Requirements Validation	◔	◑			
D.	Software Design					○
E.	Software Construction					○
G.	Software Maintenance					○
H.1	Management of the CM Process		●			
H.2	Configuration Identification		◔			
H.3	Configuration Control		◔			
H.4	Software Configuration Status Accounting		◔			
H.5	Software Release Management					○
I.1	Software Project Planning		◑			
I.2	Risk Management		◑			
I.3	Software Project Organization and Enactment		◔			
I.4	Review and Evaluation		◔			
I.5	Closure		◔			
I.6	Software Engineering Measurement		◑			
I.7	Engineering Economics					○
K.1	Software Quality Fundamentals		◑			
K.2	Software Quality Management Processes					○
K.3	Verification and Validation (V&V)		●			

A.2 "Codes of ethics and professional conduct" relates strongly to "Ethical Behaviour" in GRCSE Part 5. Both curricula cover ethical behaviour and professionalism relating to law and legal issues, cultural responsibility, and responsibility to society.

Soft skills

Graduates of SwE should: *"Be an effective member of a team […] and lead in one area of project development, such as project management, requirements analysis, architecture, construction, or quality assurance."* (Pyster, 2009, p. 20). Table 5 lists topics relevant to functioning in a team are (Pyster, 2009, p. 96).

Table 5: Soft skills topics (GSwE2009) to GRCSE mapping

GSwE2009 topics		*GRCSIE CorBOK*				
		Part 2	Part 3	Part 4	Part 5	Part 6
A.1	Social, legal, and historical issues				◑	
A.2	Codes of ethics and professional conduct				●	
I.3	Software Project Organization and Enactment		◔			

Systems engineering

Table 6 includes systems engineering-related content or activities (Pyster, 2009, pp. 56, 96) mapped to the GRCSE curriculum. These topics are considered vital to "Understand the relationship between software engineering and systems engineering and be able to apply systems engineering principles and practices in the engineering of software." (Pyster, 2009, p. 20).

Table 6: Systems Engineering topics (GSwE2009) to GRCSE mapping

GSwE2009 topics		*GRCSIE CorBOK*				
		Part 2	*Part 3*	*Part 4*	*Part 5*	*Part 6*
A.1	Social, legal, and historical issues				◑	
A.2	Codes of ethics and professional conduct				●	
B.1	Systems Engineering Concepts	●				
B.2	System Engineering Life Cycle Management		◑			
B.3	Requirements	◑	●			
B.4	System Design		●			
B.5	Integration and Verification		◑			
B.6	Transition and Validation		◑			
B.7	Operation, Maintenance and Support		●			
C.1	Fundamentals of Requirements Engineering	◔	◑			
C.2	Requirements Engineering Process		◑			
C.3	Initiation and Scope Definition					○
C.4	Requirements Elicitation		●			
C.5	Requirements Analysis		◑			
C.6	Requirements Specification		◑			
C.7	Requirements Validation	◔	◑			
C.8	Practical Considerations		◑			
F.1	Testing Fundamentals		◔			
F.2	Test Levels		◔			
F.3	Testing Techniques					○
F.4	Test-Related Measures					○
F.5	Test process					○
H.1	Management of the CM Process		●			
H.2	Configuration Identification		◔			
H.3	Configuration Control		◔			
H.4	Configuration Status Accounting		◔			
H.5	Software Release Management and Delivery					○
I.2	Risk Management		◑			
I.5	Closure		◔			
I.7	Engineering Economics					○
J.4	Product and Process Measurement					○
K.1	Software Quality					○
K.3	Verification and Validation (V&V)		●			

B.1 "Systems Engineering Concepts" strongly related to all topics in the KA "System Fundamentals" in GRCSE pt. 2, as well as topics within KA “Systems Approach Applied to Engineering Systems". All topics require a Bloom level of comprehension.

B.3 “Requirements” consists of two sections: *Stakeholder Requirements* and *Requirements Analysis*. *Stakeholder Requirements* relate to several topics in GRCSE pt. 2 and pt. 3. B.3 is partially related to the “Identifying and Understanding Problems and Opportunities” topic in KA “Systems Approach

Applied to Engineering Systems" in GRCSE pt. 2. The topics differ in Bloom levels, where GSwE2009 requires *comprehension/application* and GRCSE requires *knowledge. Requirements Analysis* is strongly related to the topic "Stakeholder Needs and Requirements" in KA "Concept Definition" in GRCSE pt. 3, which provides a more detailed account of principles, concepts and methods related to stakeholder requirements. Bloom level application pertains to both topics.

B.4 "System Design" is divided into three parts: Architectural Design, Implementation and Trade Studies. All parts relate to topics within the KA "System Definition" in GRCSE pt. 3. Bloom level for GSwE2009 is comprehension/application, while GRCSE topics require application. Architectural Design strongly relates to the topic "System Architecture", as activities related to defining a comprehensive solution that encompasses all system requirements are described in both topics. *Implementation* is strongly related to "Logical Architecture Model Development", "Physical Architecture Model Development", and "System Design". All topics describe activities used to determine system details according to requirements. Trade Studies relate strongly to the topic "System Analysis", which describes approaches to technical decision-making.

B.7 "Operation, Maintenance and Support" describe activities related to technical processes for a system's utilisation and disposal life cycle stages. B.7 strongly relates to topics "Operation of the System", "System Maintenance", and "Logistics" in KA "System Deployment and Use", as well as "Service Life Extension", "Capability Updates, Upgrades, and Modernization", and "Disposal and Retirement" in KA "Product and Service Life Management" in GRCSE. All topics require Bloom level *comprehension.*

Results analysis

This section discusses the outcome of the curriculum mapping and considers the relations and topics mapped. As one topic in GSwE2009 can relate to several topics in GRCSE, the number of relations is not equal to the total number of topics in Table 3 – Table 6.

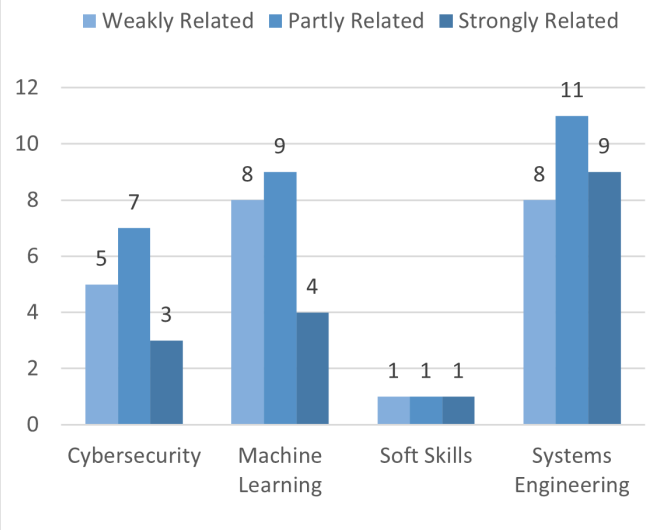


Figure 1: Distribution of relations in the four focus areas.

This mapping identified 67 relations, of which 22 were weakly related, 28 were partially related, and 17 were strongly related (figure 1). Identifying these relationships required comparing topic activities and Bloom cognitive levels associated with each topic. If considering only topics, i.e., not the number of relations, there are 39 individual topics identified in this mapping. Of these, 17 related to two or three focus areas (figure 2): 1) Cybersecurity, SE, and ML, 2) Soft skills, SE, and ML, 3) Soft skills and SE, 4) SE and cybersecurity, and 5) SE and ML. The remaining topics that belong only to one focus area, ML and SE, with 4 and 9 topics, are not included in the figure. There are large overlaps between topics in the focus areas, evident within 1) cybersecurity, SE, and ML. This finding could be seen in relation to the general description of curricula topics and may also indicate the variety of competence and skill necessary for each focus area.

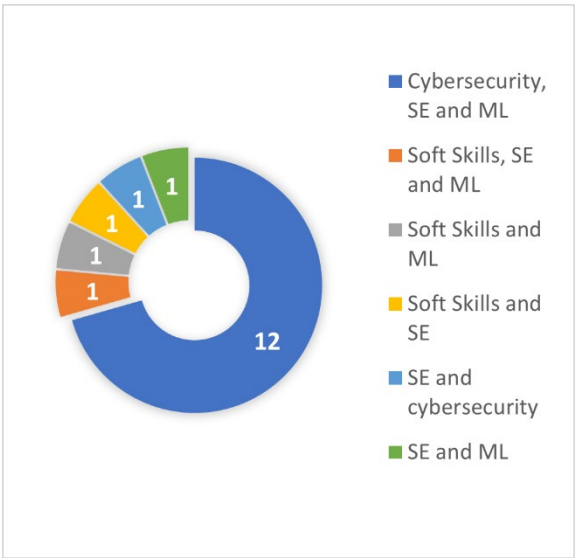


Figure 2: Topics relating to two or more focus areas.

Figure 3 shows the identified relations mapped to the distinct parts of GRCSE CorBOK. Part 2, "Foundations of SE Topics", contains an overview of SE discipline, principles, and context. Most of the relations identified are within GRCSE CorBOK part 3: "SE and Management", which addresses in-depth information about how SE is conducted, management processes, and standards.

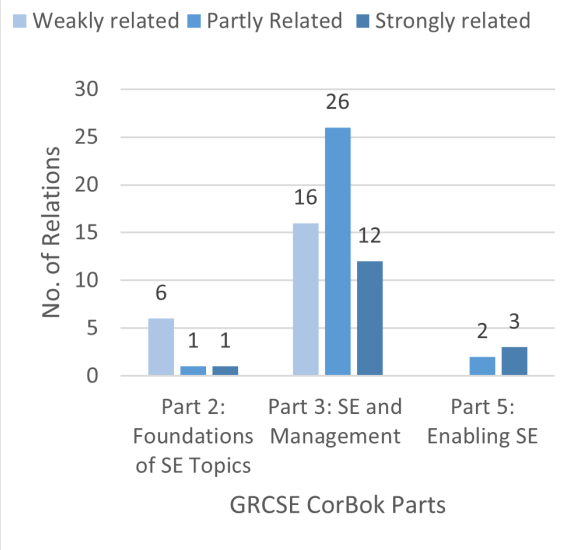


Figure 3: Distribution of the identified relations in GRCSE

Out of the 68 relations mapped in section *Outcomes*, only 8 of the identified relations belong to part 2. According to GRCSE, "Part 2 topics are primarily conceptual, with the concepts supporting the topics in Part 3. Part 3 concentrates on the processes, methods, and practices used to manage, develop, operate and maintain systems." (Pyster, Olwell, et al., 2015, p. 35). Moreover, 6 of the topics related to part 2 are weakly related, one is partly related, and the last is strongly related. Considering that this part of the CorBOK contains the foundational SE concept, it is interesting that only 8 of the GSwE2009 relations are mapped to this part of "fundamental SE knowledge". For instance, mapped topics within the KA Systems Engineering to GRCSE (table 7) only have four relations to GRCSE part 2, i.e., fundamental aspects of SE. However, 22 relations are mapped to part 3, which is "a more in-depth coverage of requirements, architecture, and management topics" (Pyster, Olwell, et al., 2015, p. 33).

Discussion: SwE and SE in the context of ICS cybersecurity

This mapping shows that SwE's graduate curriculum, GSwE2009, shares many similarities with SE's GRCSE. This section discusses these results in the broader context of SwE, SE and IT professionals in ICS security.

A total of 15 topics have been identified as relevant to GRCSE in the GSwE2009 cybersecurity focus area. None of the topics covered cybersecurity specifically, but they supported an understanding of requirements engineering (in software development), configuration management, risk management, and verification and validation (V&V).

Within the ML focus area, a total of 19 topics were found to have a relation to GRCSE. However, they only cover the process of software development, not software design or ML specifically. ML

algorithms are more than just software development, and the topics mapped (Table 4) would not provide SE graduates with sufficient insights into ML's fundamentals or technical aspects. AI and machine learning are becoming increasingly relevant to the ICS, and the future workforce should be familiar with these technologies regardless of their role in the industrial environment (Karampidis et al., 2019; Kipper et al., 2021; Ngambeki et al., 2022). ML tools within ICS security are often developed by IT personnel, yet they must communicate possible threats in a way that is understandable to OT personnel (M.R. et al., 2021). Accordingly, an understanding of ML could enable an OT expert to participate and communicate effectively with ML developers and enable them to contribute their expertise to developing AI/ML tools for ICS cybersecurity.

In the focus area of soft skills, 3 GSwE2009 topics were mapped to GRCSE (Table 5). The expected outcome of the first two topics from the KA "Ethical and Professional Conduct" is that graduates should have a fundamental understanding of ethical and professional conduct and laws and regulations. These high-level topics do not detail communication, teamwork, or leadership methods. In contrast, GRCSE has devoted part 5 to enabling businesses, teams, and individuals in SE. Both topics cover process monitoring, but GRCSE emphasises risk management more.

A total of 25 GSwE2009 topics relate to GRCSE within the focus area of systems engineering. Activities within these SwE topics can be found across several topics and KAs within GRCSE. It may be because GSwE2009 reads mainly like a "reference manual" containing detailed information about specific topics. GRCSE, on the other hand, provides KAs and topics within parts (parts 2-6) that connect to processes within the lifecycle of SE projects and systems. GRCSE is organised more like a "project handbook." As such, it provides a more comprehensive view of the entire process of systems lifecycle, while GSwE2009 focuses more on specific topics.

The mapping found that some topics' activities in GSwE2009 could be mapped to activities located in several different topics (and KAs) in GRCSE. Although the activities overlap, their terminology differs significantly. It is consistent with previous findings (McBride et al., 2020; Sheard. et al., 2018; Turner

et al., 2009), that the difference in vocabulary hinders mutual understanding and collaboration. In addition, other studies have mentioned difficulty collaborating on projects due to miscommunication, an inability to understand each other's discipline, and a lack of respect for each other's contributions (Kasser & Shoshany, 2000; Sheard. et al., 2018; Towhidnejad et al., 2013).

Previous work has pointed to various reasons why SwE and SE struggle to work together, e.g., that SwE tends to belong to an IT department and SE to an engineering department (McBride et al., 2020; Pyster, Adcock, et al., 2015). Without cross-disciplinary communication, understanding, and collaboration, they lack the tools and methods for communicating across disciplines once they enter the workforce. Gjermundrød et al. (2016) suggest that misunderstandings and difficulties working together result from the two groups using different languages and having different goals. However, according to Towhidnejad et al. (2013), GSwE2009 and GRCSE provide a foundation for mutual understanding between SE and SwE. However, current curricula in higher education, as well as a lack of collaboration between disciplines, fail to teach this.

A considerable amount of experience in the field of information security provides IT professionals with a clear advantage and responsibility when contributing to the security of ICS. Sheard et al. (2021) note that SE professionals are underrepresented in DevSecOps- or SE-dominant projects, resulting in new technologies being developed without sufficient input and leadership from SE professionals. The introduction of IT elements into the OT environment highlights security and knowledge gaps on both sides. As IT professionals are not trained in systems engineering, they are not familiar with the complexities of ICS environments and OT data. Further, OT personnel do not possess the skills necessary to take preventive security measures to safeguard ICS systems (Karampidis et al., 2019). As experts from both fields are essential to the safety and security of ICS (Muscarella et al., 2020), IT and OT professionals must work together to bridge the skill and competence gap, enabling a more effective collaboration by fostering understanding between the two disciplines. According to research on the ICS security skills gap, there is both a skills gap in the industry and a gap in efforts to standardise curriculum content (Ngambeki et al., 2022). Researchers have identified that communication and teamwork skills, closely followed by a multidisciplinary and dynamic skillset, are of the highest importance for the ICS cybersecurity industry (Azmat et al., 2020; John et al., 2020; Ngambeki et al., 2021; Slayton & Clark-Ginsberg, 2018; Sohime et al., 2020).

Threats to validity

Curriculum mapping and the choice of GSwE2009 topics limit the results of this study. Additionally, only SWEBOK was used to find information about GSwE2009 topics, whereas other sources might have given different results.

The two curricula were systematically analysed supported by a template guide. However, certain aspects must be considered for the skills and competencies identified for cybersecurity and machine learning. Cybersecurity skills and competencies are identified by several frameworks and curriculum guidelines, making discretion necessary. In the absence of official curriculum guidelines or standards for ML, the definition of skills and competencies is subject to interpretation. Also, most topics in GSwE2009 are high-level, requiring subjective judgement in selecting topics for each focus area.

Conclusion

The mapping results suggest an insufficient overlap between the topics and activities of GSwE2009 and GRCSE to impart the needed knowledge within these focus areas. The topic descriptions fail to provide sufficient details about the focus areas to allow a conclusion about their significance specifically to ICS cybersecurity to be drawn. Consequently, the result is a mapping of a broader set of skills and competencies, highlighting the differences and similarities between SwE and SE disciplines. Additionally, as highlighted above, cultural, and traditional aspects of the teaching of SwE and SE may contribute to a gap between the disciplines. Soft skills have been identified as vital for ICS security, making it worthwhile to explore how SwE and SE can communicate and collaborate more comprehensively. To this end, focusing on bridging gaps between SwE and SE through collaboration and communication of soft skills can be a viable area of further exploration.

Future work will include interviews with industry leaders in ICS cybersecurity to determine what skills and competencies are needed for IT-OT security professionals. This study will be compared to the results of interviews to assess the relative needs of academia and industry.

Acknowledgements

Thank you to Dr Bjørn Axel Gran for the review and valuable input to this paper.

References

Armstrong, J. R., & Pyster, A. (1997). Resolved: Software Should Lead in Systems Engineering. *INCOSE International Symposium*, *7*(1), 317–324. https://doi.org/10.1002/j.2334-5837.1997.tb02188.x

Baldassarre, M. T., Caivano, D., Pino, F. J., Piattini, M., & Visaggio, G. (2012). Harmonization of ISO/IEC 9001:2000 and CMMI-DEV: from a theoretical comparison to a real case application. *Software Quality Journal*, *20*(2), 309–335. https://doi.org/10.1007/s11219-011-9154-7

Belden Corporation. (2020, July 7). Achieving successful IT/OT network convergence [Technology report]. *Industrial Ethernet Book*. https://iebmedia.com/technology/iiot-industry-4-0/achieving-successful-it-ot-network-convergence/

Bigelow, S. J., & Lutkevich, B. (2021, August). What is IT/OT Convergence? Everything You Need to Know. *IT Operations*. https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence

Bloom, B. S. (1956). *Taxonomy of educational objectives: The classification of educational goals*. D. McKay Co.

Bourque, P., & Fairley (eds), R. E. (2014). *Guide to the software engineering body of knowledge*. IEEE Computer Society. www.swebok.org

ChatGPT AI Cybersecurity Potential. (n.d.). *CYFIRMA*. Retrieved 6 January 2023, from https://www.cyfirma.com/outofband/chatgpt-ai-cybersecurity-potential/

Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: A systematic literature review. *Information and Computer Security*, *29*(5), 697–723. https://doi.org/10.1108/ICS-07-2020-0121

Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*(103614), 1–16. https://doi.org/10.1016/j.compind.2022.103614

Fortinet. (2022). *2022 State of Operational Technology and Cybersecurity Report* (No. 1578659-0-0-EN; p. 25). https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf

Gan, T. H., Kanfoud, J., Nedunuri, H., Amini, A., & Feng, G. (2021). Industry 4.0: Why Machine Learning Matters? In L. Gelman, N. Martin, A. A. Malcolm, & C. K. (Edmund) Liew (Eds.), *Advances in Condition Monitoring and Structural Health Monitoring* (pp. 397–404). Springer Singapore. https://doi.org/10.1007/978-981-15-9199-0_37

Giray, G. (2021). A software engineering perspective on engineering machine learning systems: State of the art and challenges. *Journal of Systems and Software*, *180*(111031), 1–35. https://doi.org/10.1016/j.jss.2021.111031

Greco, J. (2023, January 4). The Rise of ChatGPT: How AI Plays a Vital Role In Cybersecurity. *Data Connectors*. https://dataconnectors.com/the-rise-of-chatgpt-how-ai-plays-a-vital-role-in-cybersecurity/

Hemsley, K. E., & Fisher, R. E. (2018). *History of Industrial Control System Cyber Incidents* (Study INL/CON-18-44411-Revision-2; pp. 1–33). Idaho National Labs. https://doi.org/10.2172/1505628

IABAC. (2019). *A Guide to the Data Science Body of Knowledge—Version 2* (pp. 1–47). International Association of Business Analytics Certification. https://iabac.org/g-standards/IABAC-EDSF-DSBOK-R2.pdf

Industroyer2: Industroyer reloaded. (2022, April 12). WeLiveSecurity. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

Joint Task Force on Cybersecurity E. (2018). *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. ACM. https://doi.org/10.1145/3422808

Joint Task Force Transformation Initiative. (2011). *Managing information security risk: Organization, mission, and information system view* (NIST SP 800-39; 0 ed., Reports on Computer Systems

Technology, p. 88). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-39

Karampidis, K., Panagiotakis, S., Vasilakis, M., Markakis, E. K., & Papadourakis, G. (2019). *Industrial CyberSecurity 4.0: Preparing the Operational Technicians for Industry 4.0*. 1–6. https://doi.org/10.1109/CAMAD.2019.8858454

Kasser, J., & Shoshany, S. (2000). *Systems engineers are from Mars, software engineers are from Venus*. Proceedings of the Thirteen Annual International Conference on Software & Systems Engineering and their Applications, Paris, France. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=cb890d41bf72b252ce573c31c0c92a4490cc1a93

Kipper, L. M., Iepsen, S., Dal Forno, A. J., Frozza, R., Furstenau, L., Agnes, J., & Cossul, D. (2021). Scientific mapping to identify competencies required by industry 4.0. *Technology in Society*, *64*, 101454. https://doi.org/10.1016/j.techsoc.2020.101454

Kumeno, F. (2019). Software engineering challenges for machine learning applications: A literature review. *Intelligent Decision Technologies*, *13*(4), 463–476. https://doi.org/10.3233/IDT-190160

Kuttolamadom, M., Wang, J., Griffith, D., & Greer, C. (2020, January). Educating the Workforce in Cyber and Smart Manufacturing for Industry 4.0. *ASEE Annual Conference Exposition Proceedings*. American Society for Engineering Education Virtual Conference. https://par.nsf.gov/biblio/10178926-educating-workforce-cyber-smart-manufacturing-industry

Lee, K. (2018, October 5). Deploying operational data to an OT/IT cloud. *Industrial Ethernet Book*. https://iebmedia.com/technology/edge-cloud/deploying-operational-data-to-an-ot-it-cloud/

Malatras, A., Skouloudi, C., & Koukounas, A. (2019). *Industry 4.0—Cybersecurity Challenges and Recommendations* (pp. 1–12). European Union Agency for Network and Information Security

(ENISA),. https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations

Maleh, Y. (2021). IT/OT convergence and cyber security. *Computer Fraud & Security*, *2021*(12), 13–16. https://doi.org/10.1016/S1361-3723(21)00129-9

McBride, S., Schou, C., & Slay, J. (2020). *A Security Workforce to Bridge the IT-OT Gap*. https://industrialcyberforce.org/wp-content/uploads/2020/08/A-Security-Workforce-to-Bridge-the-IT-OT-Gap.pdf

Menzies, T. (2020, January). The Five Laws of SE for AI. *IEEE Software*, *37*(1), 81–85.

Michalec, O., Milyaeva, S., & Rashid, A. (2022). Reconfiguring governance: How cyber security regulations are reconfiguring water governance. *Regulation & Governance*, *16*(4), 1325–1342. https://doi.org/10.1111/rego.12423

Muscarella, S., Osaisai, M., & Sheard, S. (2020). Systems and Software Interface Survey. *INCOSE International Symposium*, *30*(1), 1305–1323. https://doi.org/10.1002/j.2334-5837.2020.00787.x

Nascimento, E., Nguyen-Duc, A., Sundbø, I., & Conte, T. (2020). Software engineering for artificial intelligence and machine learning software: A systematic literature review. *ArXiv E-Prints*, 1–68. arXiv:2011.03751. https://doi.org/10.48550/arXiv.2011.03751

Ngambeki, I., McBride, S., & Slay, J. (2022). Knowledge Gaps in Curricular Guidance for ICS Security. *Journal of The Colloquium for Information Systems Security Education*, *9*, Article 1.

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *Workforce Framework for Cybersecurity (NICE Framework)* (NIST Special Publication 800-181 REV. 1; pp. 1–18). National Institute of Standards and Technology (NIST). https://doi.org/10.6028/NIST.SP.800-181r1

Pyster, A. (2009). *Graduate Software Engineering 2009 (GSwE2009): Curriculum Guidelines for Graduate Degree Programs in Software Engineering.* Stevens Institute of Technology. https://www.acm.org/binaries/content/assets/education/gsew2009.pdf

Pyster, A., Adcock, R., Ardis, M., Cloutier, R., Henry, D., Laird, L., Lawson, H. 'Bud', Pennotti, M., Sullivan, K., & Wade, J. (2015). Exploring the Relationship between Systems Engineering and Software Engineering. *Procedia Computer Science*, *44*, 708–717. https://doi.org/10.1016/j.procs.2015.03.016

Pyster, A., Olwell, D., Ferris, T. L. J., Hutchison, N., Enck, S., Anthony, J., Henry, D., & Squires, A. (eds). (2015). *Graduate Reference Curriculum for Systems Engineering (GRCSE™) V1.1.* Trustees of the Stevens Institute of Technology. www.bkcase.org/grcse/

Rech, J., & Althoff, K. D. (2004). Artificial Intelligence and Software Engineering: Status and Future Trends. *KI*, *18*(3), 5–11.

Sánchez-Gordón, M.-L., & Colomo-Palacios, R. (2018). From Certifications to International Standards in Software Testing: Mapping from ISQTB to ISO/IEC/IEEE 29119-2. In X. Larrucea, I. Santamaria, R. V. O'Connor, & R. Messnarz (Eds.), *Systems, Software and Services Process Improvement* (Vol. 896, pp. 43–55). Springer International Publishing. https://doi.org/10.1007/978-3-319-97925-0_4

Sarker, I. H. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, *2*(3), 160. https://doi.org/10.1007/s42979-021-00592-x

SEBoK Editorial Board. (2021). *Guide to the Systems Engineering Body of Knowledge (SEBoK), Version 2.5*. The Trustees of the Stevens Institute of Technology. http://www.sebokwiki.org/

Sheard, S., Bouyaud, M., Osaisai, M., Siviy, J., & Nidiffer, K. E. (2021). A Guide for Systems Engineers to Finding Your Role in 21st-Century Software-Dominant Organizations. *INCOSE International Symposium*, *31*(1), 926–941. https://doi.org/10.1002/j.2334-5837.2021.00878.x

Sheard., S., Cadigan, J., Chim, L., Creel, R., Marvin, J., & Pafford, M. E. (2018). INCOSE Working Group Addresses System and Software Interfaces. *INCOSE International Symposium*, *28*(1), 456–474. https://doi.org/10.1002/j.2334-5837.2018.00493.x

Sheard, S., Pafford, M. E., & Phillips, M. (2019). Systems Engineering–Software Engineering Interface for Cyber-Physical Systems. *INCOSE International Symposium*, *29*(1), 249–268. https://doi.org/10.1002/j.2334-5837.2019.00602.x

Siemers, B., Attarha, S., Kamsamrong, J., Brand, M., Valliou, M., Pirta-Dreimane, R., Grabis, J., Kunicina, N., Mekkanen, M., Vartiainen, T., & Lehnhoff, S. (2021). Modern Trends and Skill Gaps of Cyber Security in Smart Grid: Invited Paper. *IEEE EUROCON 2021 - 19th International Conference on Smart Technologies*, 565–570. https://doi.org/10.1109/EUROCON52738.2021.9535632

Smit, J., Kreutzer, S., Moeller, C., & Carlberg, M. (2016). *Industry 4.0 Analytical Study* (Study PE 570.007; pp. 1–81). Policy Department A: Economic and Scientific Policy. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). *Guide to Industrial Control Systems (ICS) Security* (NIST SP 800-82r2; NIST Special Publication, p. NIST SP 800-82r2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r2

Teixeira, M. A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., & Samaka, M. (2018). SCADA system testbed for cybersecurity research using machine learning approach. *Future Internet*, *10*(8), 76.

Towhidnejad, M., Hilburn, T., & Fairley, R. (2013). Software and System Engineering Education: Commonalities and Differences. *2013 ASEE Annual Conference & Exposition Proceedings*, 23.1074.1-23.1074.10. https://doi.org/10.18260/1-2--22459

Turner, R., Pyster, A., & Pennotti, M. (2009). Developing and validating a framework for integrating systems and software engineering. *2009 3rd Annual IEEE Systems Conference*, 407–412. https://doi.org/10.1109/SYSTEMS.2009.4815836

Von Solms, S., & Futcher, L. (2018). Identifying the Cybersecurity Body of Knowledge for a Postgraduate Module in Systems Engineering. In L. Drevin & M. Theocharidou (Eds.),

Information Security Education – Towards a Cybersecure Society (Vol. 531, pp. 121–132). Springer International Publishing. https://doi.org/10.1007/978-3-319-99734-6_10

Wray, R. B. (1993). Systems Engineering and Software Engineering: Cooperative or Competitive? *INCOSE International Symposium*, *3*(1), 833–843. https://doi.org/10.1002/j.2334-5837.1993.tb01667.x

[i] https://iebmedia.com/technology/iiot-industry-4-0/achieving-successful-it-ot-network-convergence/

[ii] https://www.britannica.com/topic/GRU

[iii] https://www.bbc.com/news/technology-61085480

[iv] https://www.helpnetsecurity.com/2022/04/12/sandworm-ukraine/

[v] https://chat.openai.com/

[vi] https://www.iso.org/news/ref2655.html

[vii] https://www.techtarget.com/iotagenda/blog/IoT-Agenda/Bridge-the-OT-and-IT-gap-with-IIoT

Appendix B

Information and Consent Form

Nettskjema

ICS cybersecurity skills and competencies - Assessing the industry's needs

Are you interested in taking part in the research project "ICS cybersecurity skills and competencies - Assessing the industry's needs"

Purpose of the project
You are invited to participate in a research project where the main purpose is to study the skills and competencies required for securing industrial control systems (ICS). This project is conducted as a part of an ongoing master thesis project. The first part of the project focused on academic requirements, briefly described below:

As industrial cybersecurity requires knowledge and skills in IT and OT technology, this study focuses on two disciplines that fit these roles: software engineering and systems engineering. The Graduate Curriculum for Software Engineering (GSwE2009) and the Graduate Reference Curriculum for Systems Engineering (GRCSE) were analysed to identify topics providing skills and competence in cybersecurity, machine learning, software engineering and soft skills. While some topic activities overlap between GSwE2009 and GRCSE, neither curriculum is sufficiently detailed in its topic description to support the knowledge needed to secure the ICS. Additional findings indicate that collaboration challenges exist because the disciplines are taught in different academic fields.

The presented work focused on the academic requirements. In the second part, the aim is to provide better insights into actual industry knowledge needs based on interviews with industry leaders in ICS cybersecurity. By providing a comprehensive understanding of cybersecurity professionals' skills, qualifications, and professional development requirements, this study will assist in bridging the gap between educational – and industry requirements.

Which institution is responsible for the research project?
Østfold University College is responsible for the project (data controller).

Why are you being asked to participate?
You are asked to participate in this study because of your work in ICS cybersecurity. Professionals asked to contribute to this study has been chosen by reaching out to people in the project groups network. The final sample size will consist of between 3-6 interviewees.

What does participation involve for you?
If you choose to take part in this project, this will involve an interview conducted either in-person or online. The interview will take approximately 35 minutes. The interview will consist of questions relating to your specific work situation, more specifically about; skills and competencies required for ICS cybersecurity professionals, roles and tasks in ICS cybersecurity and collaboration between IT and OT personnel. The interviewer will not be recorded, but the interviewer or a transcriber will take notes. After the interview, the notes will be sent to the interviewee for approval. The notes will be anonymised and stored securely.

Participation is voluntary
Participation in the project is voluntary. If you chose to participate, you can withdraw your consent at any time without giving a reason. All information about you will then be made anonymous. There will be no negative consequences for you if you chose not to participate or later decide to withdraw.

Nettskjema

Your personal privacy – how we will store and use your personal data
We will only use your personal data for the purpose(s) specified here and we will process your personal data in accordance with data protection legislation (the GDPR).

The project group, in connection with the institution responsible for the project, will have access to the personal data.

Name and contact details will be replaced by a code and stored separate from interview notes.

Notes the interview will be stored anonymously on a secure research server at Østfold University College.

The co-supervisor of the master's project, John Eidar Simensen at the Institute for Energy Technology, will transcribe the interviews, but will not have access to the data thereafter.

There will be no identifiable information included in any publication regarding the participant or their workplace.

What will happen to your personal data at the end of the research project?
The planned end date of the project is July 2023. All data will be deleted at the end of the project.

Your rights
So long as you can be identified in the collected data, you have the right to:

access the personal data that is being processed about you.

request that your personal data is deleted.

request that incorrect personal data about you is corrected/rectified.

receive a copy of your personal data (data portability), and

send a complaint to the Norwegian Data Protection Authority regarding the processing of your personal data

What gives us the right to process your personal data?
We will process your personal data based on your consent.

Based on an agreement with Østfold University College, The Data Protection Services of Sikt – Norwegian Agency for Shared Services in Education and Research has assessed that the processing of personal data in this project meets requirements in data protection legislation.

Where can I find out more?
If you have questions about the project, or want to exercise your rights, contact:

Østfold University College via

- Project leader: Ricardo Colomo-Palacios. Email: ricardo.colomo-palacios@hiof.no
- Project member: Stine Aurora Mikkelsplass. Email: stineami@hiof.no

Our Data Protection Officer: Hanne Pernille Gulbrandsen. Email: personvernombud@hiof.no

If you have questions about how data protection has been assessed in this project by Sikt, contact:

email: (personverntjenester@sikt.no) or by telephone: +47 73 98 40 40.

Your sincerely,

Stine Aurora Mikkelsplass (master student) and Ricardo Colomo-Palacios (supervisor)