International Journal of Human Capital and Information Technology Professionals
Volume 14 • Issue 1

Software and Systems Engineers in ICS Security:
Graduate-Level Curricula and Industry Needs

Stine Aurora Mikkelsplass, Østfold University College, Norway & Institute for Energy Technology, Norway*
John Eidar Simensen, Institute for Energy Technology, Norway
Ricardo Colomo-Palacios, Østfold University College, Norway

ABSTRACT

The introduction of Industry 4.0 and IIoT has enabled the interconnection of information technology (IT) and operational technology (OT) and exposed industrial control systems to cyber threats. Industrial cybersecurity requires knowledge, skill, and collaboration between IT and OT. A comparison of graduate curricula of software engineering and systems engineering identifies competencies related to industrial control systems cybersecurity. Industry experts are interviewed to identify needs for cybersecurity skills and competencies. Results from the mapping are discussed in the context of software and systems engineering challenges in ICS cybersecurity and leveraged against industry experiences and needs expressed through interviews with three OT and IT industry professionals. The curricula mapping reveals variations in both how they are organised and expressed to the extent that subjective interpretation is required for evaluation and comparison. The interviews with the industry experts indicate a gap between graduate competence from the curricula and industry needs.

KEYWORDS

Cybersecurity, Industry Needs, Information Technology, Operation Technology, Skills Gap, Software Engineering, Software Engineering Curriculum, Systems Engineering, Systems Engineering Curriculum

INTRODUCTION

The fourth industrial revolution (Industry 4.0) refers to the technological progress across industries, described as "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). Digital transformation in Industry 4.0 is the interconnection of information technology (IT) and operation technology (OT)[1]. Through the Industrial Internet of Things (IIoT), industries have found new ways to develop, manage, and maintain their operations, e.g., by extensive data collection from the OT environment, remote monitoring of processes, and optimising operations through automation (Belden Corporation, 2020; Lee, 2018). Software is a fundamental part of modern engineering systems, or cyber-physical systems (CPS), and software engineering (SwE) and systems engineering (SE) are

DOI: 10.4018/IJHCITP.333857 *Corresponding Author

both fundamental to the development and maintenance of complex systems (Pyster, Adcock, et al., 2015; Sheard, et al., 2019). Despite their significant roles, exploration of the relationship between SwE and SE is poorly defined (Pyster, Adcock, et al., 2015) and only partially explored in Fairley (2019). This issue has been debated since the 1990s (Wray, 1993), and in 2018, the International Council on Systems Engineering (INCOSE) started a working group exclusively to address these challenges, the *Systems and Software Interface Working Group* (SaSIWG) (Sheard, et al., 2018).

The study reported on aims to answer the following research questions (RQs): 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's 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 (CS) professionals and how they align with graduate curricula for IT and OT professionals. RQ2 seeks to understand the industry's needs for skills and competencies in ICS CS 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.

As part of the data collection process, two main activities were performed: 1) to identify the competencies required by GSwE2009 (Pyster, 2009) and GRCSE (Pyster, Olwell, et al., 2015) a mapping of graduate curricula within software engineering (SwE) and systems engineering (SE) curricula was performed to uncover potential gaps and overlaps in the educational frameworks of these domains. The disciplines of SwE and SE were chosen due to their requirements in maintaining and developing complex systems (Sheard, et al., 2019). The mapping considers four areas of focus: CS, machine learning (ML), soft skills, and systems engineering. According to previous studies (Chowdhury & Gkioulos, 2021; Karampidis, et al., 2019; Kipper, et al., 2021; Von Solms & Futcher, 2018), skills and competencies within these focus areas contribute to the development of key competences for ICS and Industry 4.0 CS. This was followed by activity 2) interviewing IT and OT professionals to identify industry needs and determine how well curricula support industry needs.

Section 2 presents background literature. Section 3 describes the methodology. Section 4 details the curriculum mapping results, while section 5 presents the interview results and analysis. The discussion follows in section 6, while section 7 presents the concluding remarks.

BACKGROUND

Safety is a critical driver in OT design principles, a prerequisite to protecting people, processes, and systems (Joint Task Force Transformation Initiative, 2011). Industrial control systems are traditionally associated with technology, such as programmable logic controllers, sensors, actuators, human-machine interfaces, and remote terminal units, built to operate in industrial settings and harsh environments for 20+ years without regular updates and maintenance. In contrast, information technology routinely handles hardware and software updates (Bigelow & Lutkevich, 2021). Historically, industrial systems and networks have been considered isolated and "air-gapped" from the outside world. However, events such as the *Stuxnet* attack in 2010 and the *Havex* attack in 2013 (Hemsley & Fisher, 2018) prove that ICS environments are not entirely isolated. The adoption of smart sensors, as well as IIoT, have opened up the possibility for increased connectivity in ICS environments, as the IIoT functions as a bridge between IT and OT[2], 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 hacking into the IT network, from where the attacker managed to gain access to the ICS network (*Industroyer2*, 2022).

In Industry 4.0, ML has emerged as a key application for managing and analysing large amounts of data. As a result of ICS digitization, challenges have arisen regarding data collection, analysis, and use (Sarker, 2021). In addition to ML models, artificial intelligence (AI) can make real-time

decisions based on vast amounts of data. Intrusion Detection Systems (IDSs) and other security tools use ML algorithms, for example, to identify abnormal patterns in network data. It is widely used in CS monitoring and anomaly detection in information systems (Teixeira, et al., 2018) and to give business value to data. As the interconnection of IT and OT systems allows for new opportunities, it also introduces new threats to the industrial environment. The April 2022 attacks in Ukraine, coincident with the Russian invasion, showed how malware can disrupt power grids[3,4] . As recently noted, ChatGPT[5] has been found to aid in the creation of malware targeted at SCADA systems ('ChatGPT AI Cybersecurity Potential', n.d.; Greco, 2023), reducing the threshold for skill and competence to attack ICS systems.

As fundamental support functions and services, such as water treatment, transportation, and energy systems become more complex and interdependent, there is a need for CS professionals to understand both IT and OT environments. Literature indicates a general lack of skill and competence in ICS CS, and identifies significant challenges in educating and developing the workforce to secure critical industrial systems[6] (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 systems management standards. The recruitment and organisation of professionals for ICS CS 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 shortly. 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.

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, aiming to standardise the education for software engineers and systems engineers across institutions and ensure quality of education. Both curricula have developed a *Core Body of Knowledge (CBOK and CoRBOK* respectively), 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 or CoRBOK are grouped into *Knowledge Areas* (KA), which are further divided into *topics* and s*ub-topics*.

METHODOLOGY

Performing a curriculum analysis of software and systems engineering educational settings is the first step towards answering the RQs. To understand the real-world requirements of the industry, semi-structured interviews with industry leaders in ICS CS were conducted.

Software and systems engineering graduates are expected to achieve certain learning outcomes through the GSwE2009 and GRCSE curricula. Curriculum mapping illustrates the relationship between GSwE2009 and GRCSE curricula in the focus areas of CS, ML, soft skills, and systems engineering. The 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 was analysed using qualitative content analysis.

Comparing Curricula

Using a comparative analysis (Robson, 2011; Walk, 1998), overlap and gaps were identified between the software engineering (GSwE2009) and the systems engineering (GRCSE) curricula. This can be determined by examining the topics covered in each curriculum. This includes the amount of time allocated to each topic, as well as the expected outcomes in skills and knowledge. The following aspects of the curricula were assessed in this study: the structure and sequencing of the courses, the learning outcomes, and the primary objectives of the courses. The recommended competencies and skills are structured based on the Knowledge Areas (KAs), topics, and subtopics of both curricula. In both curricula, Bloom's cognitive levels are utilized to communicate the expected level of comprehension for graduate students within each topic. In the Cognitive Domain (Bloom, 1956), there are six levels of learning ability: knowledge, comprehension, application, analysis, synthesis, and evaluation. Before the curricula mapping, a mapping of these levels was performed for both curricula to ensure they are comparable.

Competency mapping identifies the skills and competencies required to perform a specific job role efficiently. We identified criteria for skills and competencies within each focus area to map the desired competency to a topic in the SwE curriculum (GSwE2009). We then identified relevant topics within GSwE2009 by examining each KA for topics pertaining to CS, ML, and soft skills.

Curriculum Mapping

Curriculum mapping visually represents the relationship between Graduate Software Engineering 2009 topics: GSwE2009 and GRCSE. Curricula mapping can be challenging (Ervin, et al., 2013) due to its subjective nature, and the approach has been 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 relationships between curricula was done iteratively to determine the level of relationship. The process was as follows:

1. Identify GSwE2009 topics relating to focus areas.
   A detailed analysis of topic information in GSwE2009 and SWEBOK was done to identify topics relevant to developing 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 were again compared to the topics in GRCSE. GRCSE and SEBoK were used to find detailed topic information, i.e., skills and competencies related to the topic. An update to the spreadsheet added GRCSE topics with ties to GSwE2009, giving a detailed breakdown of topic relations.
3. Map relations according to the comparison scale, adapted from previous work (Baldassarre, et al., 2012; Sánchez-Gordón & Colomo-Palacios, 2018). The four categories of the scale are:
   - 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 were identified and the topics are omitted from the results. Details can be found in Mikkelsplass (2023).
4. Create a visual representation of the relationship.

To visualize the relationship between GSwE2009 and GRCSE, and the degree of relationship between each topic, all relations were organised into visual representations.

Interview Design and Questions

Although there is available literature on the ICS CS skills gap, no officially agreed upon curricula, standards, or frameworks exist for determining the essential skills and competencies for ICS CS. To gain a detailed understanding of the needs of the industry, semi-structured interviews were conducted with three industry experts.

Semi-structured interviews (Salkind, 2018) balance flexibility and consistency. To ensure consistency across all interviews and enable comparability of responses, predefined questions guide these interviews. They allow interviewees to elaborate on their responses and share their experiences and perspectives. Although there is a clear focus, there is also flexibility to explore emerging themes or unexpected insights. Additionally, semi-structured interviews provide a deeper understanding of the ICS CS field's complex needs. The data collected can be enhanced by industry leaders providing context, explaining their thinking, and sharing examples from their experiences. The key elements of the semi-structured interview method are summarised below.

1) Every ICS is unique, so an interviewer may deviate from predetermined questions if necessary, allowing the interviewer to explore interesting or unexpected avenues. It is therefore possible to gain insight into industry leaders' views on Industry 4.0 skills and competencies, as well as their perceptions of graduates' readiness. 2) The set of questions maintains consistency across interviews, which is helpful when comparing and analysing answers from different interviewees. 3) In discussing ICS and CS, a rich and deep dataset can be enhanced by industry leaders describing their answers, sharing their experiences, and providing examples. 4) By interviewing industry leaders, we identify gaps between graduates' competences and actual industry requirements.

A systematic mapping of interview questions (IQ) to RQ is presented in Table 1, providing an illustration of how the interview protocol was designed to meet the aims of the study.

CURRICULUM MAPPING RESULTS

This section presents the results from the curriculum mapping, organised under the following sections: CS, ML, soft skills, and systems engineering. Note that for the tables in the following we present result excerpts only. The full results can be found in Mikkelsplass (2023).

Cybersecurity

Topics in GSwE2009 relevant to cybersecurity competence are presented in Table 2. 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 CS work. As part of identifying topics for CS, this framework was used in conjunction with Knowledge Areas in the Cybersecurity Curricula 2017 (Joint Task Force on Cybersecurity Education, 2018) as criteria when identifying topics.

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*.

Table 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 works 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 on 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?	✓	✓	✓

Table 2. Cybersecurity topics (GSwE2009) to GRCSE mapping

GswE2009 Topics		*GRCSE CorBOK*				
		Part 2	*Part 3*	*Part 4*	*Part 5*	*Part 6*
C.1	Fundamentals of Requirements Engineering	◔	◑			
C.2	Requirements Engineering Process		◑			
C.4	Requirements Elicitation		●			
C.5	Requirements Analysis		◑			
C.6	Requirements Specification		◑			
C.7	Requirements Validation	◔	◑			
C.8	Practical Considerations		◑			
H.1	Management of the CM Process		●			
H.2	Configuration Identification		◔			
H.3	Configuration Control		◔			
H.4	Software Configuration Status Accounting		◔			
I.2	Risk Management		◑			
K.3	Verification and Validation (V&V)		●			

Machine Learning

The skills and competence needed to develop ML algorithms relate to the disciplines of SwE and Data Science (IABAC, 2019). These curricula and previous works concerning the ML in SwE (Giray, 2021; Kumeno, 2019; Menzies, 2020; Nascimento, et al., 2020) informed the selection of topics in Table 3.

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.

Table 3 Machine learning topics (GSwE2009) to GRCSE mapping

GSwE2009 Topics		*GRCSE CorBOK*				
		Part 2	Part 3	Part 4	Part 5	Part 6
A.2	Codes of ethics and professional conduct				●	
C.1	Fundamentals of Requirements Engineering	◔	◑			
C.2	Requirements Engineering Process		◑			
C.4	Requirements Elicitation		●			
C.5	Requirements Analysis		◑			
C.6	Requirements Specification		◑			
C.7	Requirements Validation	◔	◑			
H.1	Management of the CM Process		●			
H.2	Configuration Identification		◔			
H.3	Configuration Control		◔			
H.4	Software Configuration Status Accounting		◔			
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		◑			
K.1	Software Quality Fundamentals		◑			
K.3	Verification and Validation (V&V)		●			

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 4 lists topics relevant to functioning on a team (Pyster, 2009, p. 96).

Systems Engineering

Table 5 includes systems engineering-related content or activities (Pyster, 2009, pp. 56, 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).

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

Table 4. Soft skills topics (GSwE2009) to GRCSE mapping

GSwe2009 Topics		*GRCSE 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		◔			

Table 5. Systems engineering topics (GSwE2009) to GRCSE mapping

GSwe2009 Topics		GRCSE 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.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		◔			
H.1	Management of the CM Process		●			
H.2	Configuration Identification		◔			
H.3	Configuration Control		◔			
H.4	Configuration Status Accounting		◔			
I.2	Risk Management		◑			
I.5	Closure		◔			
K.3	Verification and Validation (V&V)		●			

B.3 "Requirements" consists of *Stakeholder Requirements* and *Requirements Analysis*. *Stakeholder Requirements* relate to several topics in GRCSE Part 2 and Part 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 Part 2. The topics differ in Bloom levels, where GSwE2009 requires *comprehension/application,* and GRCSE requires *knowledge.*

INTERVIEW RESULTS AND ANALYSIS

The interviews aimed to identify skills and competencies the industry needs for ICS environment cybersecurity. Findings are presented according to themes found in the Qualitative Content Analysis (QCA).

Participants

Participant A oversees both hardware and software components in the energy industry and leads a team that manages installation communication, maintenance, and safeguarding. Participant A has been involved with security-focused expert groups for 12 years and has an MSc in electrical engineering. Participant B has an MSc in cybernetics and has overseen industrial digitalisation and OT for 29 years in the process industry. Maintaining and developing systems, applications, and the operational aspects of those systems are part of their responsibilities. Participant C is a Chief Information Officer (CIO)

in research and development, with a background that includes IT and development and 20+ years' experience, with an MSc in communication systems. Despite the limited sample size, the differences in backgrounds and experience provide a broad perspective.

Interview Result Summary

The following provide examples and overview of the information gained from the ICS IT and OT experts, summarized as findings. A complete overview of all questions and answers can be found in (Mikkelsplass, 2023).

The increasing interconnection, and the need for collaboration between IT and OT, was reported by all participants. Participants A and B noted the use of the SOC for the ICS environments and that OT personnel actively collaborated with the SOC to protect the ICS. While one participant was the primary point of contact between the SOC and the OT personnel, the environment described by the participant was more collaborative, with several members from the OT department participating.

CS competence in the ICS environment revealed most notably the range of skills and competencies required to understand the various aspects of the ICS environment effectively. All acknowledged that IT and OT have significant differences that must be considered. The following skills and competencies were emphasised in the interviews:

- Understanding fundamental ICS architecture is critical in IT-OT systems. This relates to CS, 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 highlighted the increasing interconnection between IT and OT technology and the digitisation of the industry, pointing out skills such as 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.

Participant B stated that *"The OT language is probably like a tribal language, where you must be a member of the tribe [to understand]. It may not be something that can be acquired through education."* Academic literature support this as one of the main barriers for collaboration, 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, being the only one with a background in IT and development, showed a more optimistic attitude towards ML and AI's potential in OT CS than participants A and B, corresponding to previous studies on IT and OT personnel having a very different outlook on bringing new technology into an existing system (Sheard, et al., 2019).

For educating future ICS CS 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.

DISCUSSION

The IT-OT gap can be attributed both to the actual technical variability of the industrial ecosystem, and to the mindset of the individuals who design, operate, and secure these systems. Mindsets are influenced by practices within the field, creating differences between traditional IT-focused CS and the evolving requirements of ICS CS. In addition to focusing on technological advances, one must

also have to address the mental, social, and cultural gaps to create a comprehensive understanding of ICS CS, which encompasses both the IT and OT sectors.

Curricula Mapping: Results Analysis

The curriculum mapping identified 67 relations, of which 22 were weakly related, 28 were partially related, and 17 were strongly related. Figure 1 depicts the distribution of the 67 relations in the four focus areas CS, ML, soft skills, and systems engineering. These relationships were identified by comparing topic activities from the curriculum and Bloom's cognitive levels associated with each topic.

Out of the 67 relations mapped in section 4, only 8 belong to part 2 of the GRCSE (Figure 2). According to GRCSE, "Part 2 topics are primarily conceptual, with the concepts supporting the topics

Figure 1. Distribution of relations in the four focus areas

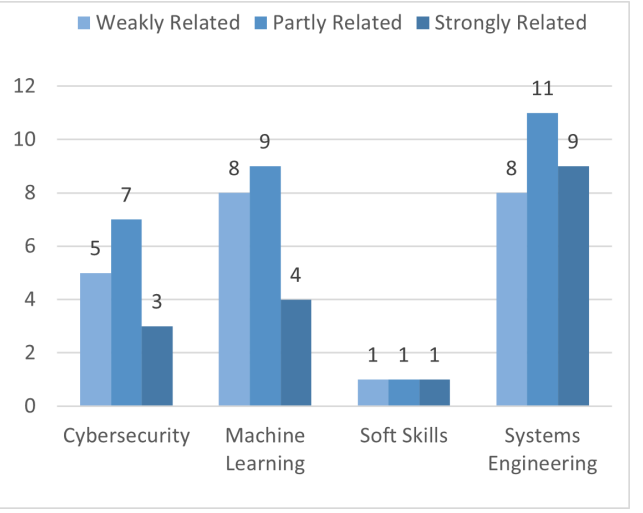
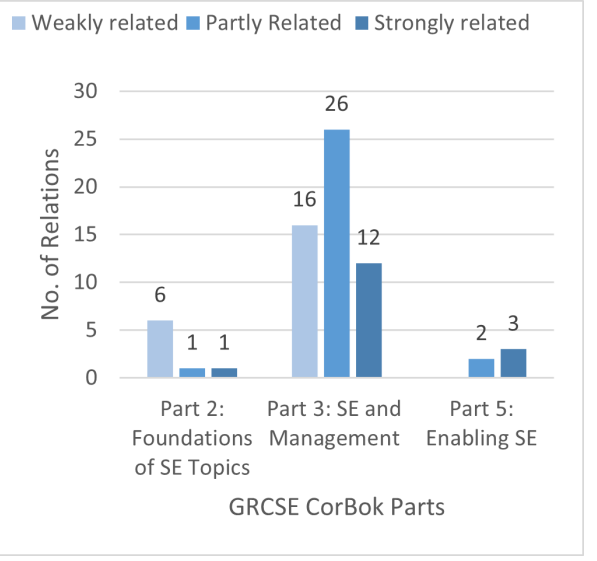


Figure 2. Distribution of the identified relations in GRCSE



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). 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". 22 relations are mapped to GRCSE 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 hinder SwE students' understanding of SE.

Focus Areas

This mapping shows that SwE's graduate curriculum, GSwE2009, shares many similarities with SE's GRCSE.

In the GSwE2009 cybersecurity focus area, 15 topics have been identified that are relevant to GRCSE, including requirements engineering, configuration management, risk management, and verification and validation. No specific mention of CS was made.

There are 19 GRCSE-related topics in the ML focus area. ML algorithms are more than just software development; the topics mapped (Table 3) would not provide SE graduates with enough insight into ML fundamentals. AI and ML 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 CS tools for ICS utilise ML, and they are often developed by IT personnel. However, the tools they develop are intended to communicate possible threats in an understandable and relatable way to OT personnel (M.R., et al., 2021). Three GSwE2009 topics were mapped to GRCSE within the focus area of soft skills (Table 4). Graduates should have a basic understanding of ethical and professional conduct and laws and regulations from the first two topics from the KA "Ethical and Professional Conduct." In contrast, GRCSE has devoted Part 5 to enabling businesses, teams, and individuals in SE. These high-level topics do not focus on communication, teamwork, or leadership methods.

Within systems engineering, 25 GSwE2009 topics relate to GRCSE. These SwE topics include activities across several topics and KAs within GRCSE. This might be attributed to GSwE2009 being organised as a reference manual containing detailed information. GRCSE, on the other hand, is organised more like a "project handbook", providing a more comprehensive view of the entire systems' lifecycle.

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

Connecting Academic and Industry Perspectives

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

The curriculum mapping analysis revealed potential barriers to collaboration between IT and OT, as there are apparent differences between software and systems engineering perspectives. This nuance is most evident 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, suggesting a need for IT and OT educational crossover to bridge the communication gap.

In the curriculum mapping, foundational knowledge plays a significant role. The predominance of relationships allocated to GRCSE CorBOK Part 3, which focuses on SE applications, illustrates deficiencies in basic skills. OT environment is poorly understood by the IT department, as the interviewees expressed. The curriculum mapping can assist in identifying areas of foundational knowledge that can enhance mutual understanding and collaboration. A general suggestion to address the IT-OT complexity and support collaboration can be to increase focus SE through more practical exercises involving IT-OT systems. For SwE students, it could be beneficial with stronger ties between GSwE2009 KA B: "Systems Engineering" and GRCSE Part 2 "Foundations of Systems Engineering". A reverse mapping, from GRCSE to GSwE2009, is needed to identify where to integrate SwE into the SE curriculum.

The considerable differences in terminologies between SwE and SE may pose a barrier to effective communication between IT and OT departments, this is identified both from the mapping and the interviews.

Threats to Validity

Several threats to validity have been identified for the curriculum mapping, the semi-structured interview activity, and with regards to the collected data, data coverage and result applicability. A comprehensive overview of threats can be found in (Mikkelsplass, 2023). A number of activities and work items require subjective decision making. For example, when choosing topics for curriculum mapping, GSwE2009 topic descriptions provide very high-level descriptions of topics. In the curriculum analysis activities, the first author performed the initial mapping. In the interviews, the first author analysed the data and guided the discussion. Mitigation to these included review by co-authors, making all data available (Mikkelsplass, 2023), and creating templates and guidelines for systematic assessment. By introducing Delphi Method (J. E. J., 1976) to merge multiple individual curricula mappings into one agreed upon result, the process could have been improved further. However, the impact of this as a mitigation is difficult to predict as most topics in GSwE2009 are high level. The fact that only SWEBOK was used as information basis for the topics, the general lack of frameworks for e.g., Industry 4.0 skills and competencies, and the existence of several non-aligned frameworks for CS skills and competencies, all impact individual assessments and variability.

As the reported work was part of a MSc thesis, there were several "firsts" in performing the different activities. The two co-authors performed reviews and validation, and the first author supported verification efforts through procedures and checking. The first author holds a Master of Science degree in computer science, recent hands-on experience from Industry 4.0, IT-OT interfacing, and computer networks. Co-authors consist of a senior research scientist on applied safety and security and a full professor in software engineering.

CONCLUSION

The reported work aims to improve understanding of competence provided by graduate-level curricula compared to industry needs within Industrial Control Systems (ICS) cybersecurity (CS). ICS presents unique and complex challenges in the evolving CS 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.

A comprehensive curriculum mapping 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, revealing differences in knowledge acquisition and application within the IT and OT fields.

The mapping suggests an insufficient overlap between the topics and activities of GSwE2009 and GRCSE to impart the needed knowledge within these focus areas. The topic descriptions do not detail focus areas sufficiently to support a conclusion on their significance to ICS CS. Consequently, the result is a mapping of a broader set of skills and competencies, highlighting the differences and similarities between SwE and SE 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 seems a viable, and implementable solution.

Interviews with experienced IT and OT professionals provided in-depth, experiential insights on industry needs, and on the IT-OT gap, hereunder:

- It is crucial to interchange knowledge involving ITs CS expertise and OTs control system proficiency.
- IT and OT personnel must be better educated in each other's 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 results presented indicate that paradigm shift is needed, moving from a silo approach to a collaborative framework where knowledge and skills from both disciplines are applied collaboratively. This would require curriculum-driven cross-disciplinary competence, fostering a strengthened common understanding between IT and OT professionals.

AUTHORS NOTE

Ricardo Colomo-Palacios is now at the Escuela Técnica Superior de Ingenieros Informáticos, Universidad Politécnica de Madrid, Spain.

Correspondence concerning this article should be addressed to Stine A. Mikkelsplass, Institute for Energy Technology, P.O. Box 173, NO-1751 Halden, Norway. Email: stine.mikkelsplass@ife.no

ACKNOWLEDGMENT

The authors wish to thank Dr. Bjørn Axel Gran and Dr. Sizarta Sarshar for internal review and valuable input to this paper. Acknowledgements are also given to the reviewers of the journal to further clarify the paper.

This paper was funded by Østfold University College and the Institute for Energy Technology. The corresponding author confirms on behalf of all authors that there have been no involvements that might raise the question of bias in the work reported or in the conclusions, implications, or opinions stated.

REFERENCES

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. doi: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

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

Chowdhury, N., & Gkioulos, V. (2021). Key competencies for critical infrastructure cyber-security: A systematic literature review. *Information and Computer Security*, *29*(5), 697–723. doi: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. doi:10.1016/j.compind.2022.103614

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

Fairley, R. E. (2019). *Systems Engineering of Software-Enabled Systems*. John Wiley & Sons. doi:10.1002/9781119535041

Fortinet. (2022). *2022 State of Operational Technology and Cybersecurity Report* (1578659-0-0-EN; p. 25). https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-ot-cybersecurity.pdf

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. doi: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. doi: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/

J. E. J. (1976). Review of The Delphi Method: Techniques and applications. *Technometrics, 18*(3), 363–364. 10.2307/1268751

Joint Task Force on Cybersecurity E. (2018). *Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity*. ACM. doi:10.1145/3422808

Joint Task Force Transformation Initiative. (2011). *Managing information security risk: Organization, mission, and information system view* (NIST SP 800-39; Reports on Computer Systems Technology, p. 88). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf

Karampidis, K., Panagiotakis, S., Vasilakis, M., Markakis, E. K., & Papadourakis, G. (2019). *Industrial CyberSecurity 4.0: Preparing the operational technicians for industry 4.0*. 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*. 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. doi: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. doi: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. In *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*. 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. doi: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. doi:10.1109/MS.2019.2954841

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

Mikkelsplass, S. A. (2023). *Educating ICS cybersecurity professionals—A comparative study of graduate level curricula & industry needs* [Master Thesis]. Østfold University College. https://hiof.brage.unit.no/hiof-xmlui/handle/11250/148015

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. doi:10.1186/s42400-021-00095-5

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). 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., Pennotti, M., Sullivan, K., & Wade, J. (2015). Exploring the relationship between systems engineering and software engineering. *Procedia Computer Science*, *44*, 708–717. doi: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/

Salkind, N. J. (2018). Exploring research: Vol. Ninth, global edition (9th ed.). 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 (Vol. 896, pp. 43–55). Springer International Publishing. doi: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. doi:10.1007/s42979-021-00592-x PMID:33778771

SEBoK Editorial Board. (2021). *Guide to the systems engineering body of knowledge (sebok), version 2.5*. The Trustees of the Stevens Institute of Technology. https://www.sebokwiki.org/

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. doi:10.1002/j.2334-5837.2018.00493.x

Sheard, S., Creel, R., Cadigan, J., Marvin, J., Chim, L., & Pafford, M. E. (2018). INCOSE working group addresses system and software interfaces. *Insight - International Council on Systems Engineering*, *21*(3), 62–71. doi:10.1002/inst.12213

Sheard, S., Pafford, M. E., & Phillips, M. (2019). Systems engineering–software engineering interface for cyber-physical systems. *INCOSE International Symposium*, *29*(1), 249–268. doi: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. doi: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. doi: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. doi:10.3390/fi10080076

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. doi: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. doi: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. doi: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. doi:10.1002/j.2334-5837.1993.tb01667.x

ENDNOTES

1 https://iebmedia.com/technology/iiot-industry-4-0/achieving-successful-it-ot-network-convergence/
2 https://www.techtarget.com/iotagenda/blog/IoT-Agenda/Bridge-the-OT-and-IT-gap-with-IIoT
3 https://www.bbc.com/news/technology-61085480
4 https://www.helpnetsecurity.com/2022/04/12/sandworm-ukraine/
5 https://chat.openai.com/
6 https://www.iso.org/news/ref2655.html

Stine Aurora Mikkelsplass is a research scientist and engineer at the Institute for Energy Technology, department of Risk and Security. Her work focuses primarily on cybersecurity in IT-OT systems, including aspects such as industry 4.0, security for safety, and human-computer interaction.

John E. Simensen is a Senior Research Scientist at the Security and Risk department at the Institute for energy technology. John has 15 years' experience in evaluation and analysis of safety critical systems within nuclear, aviation and military. His main competency is evaluation and analysis methodologies for safety critical digital systems. The last two years John has led a large cross-domain Norwegian research project on practical cyber-security of critical infrastructure systems from nuclear, aviation and energy transmissions domains.

Ricardo Colomo-Palacios, Full Professor at the Escuela Técnica Superior de Ingenieros Informáticos, Universidad Politécnica de Madrid, Spain. Formerly he worked at Østfold University College, Norway and Universidad Carlos III de Madrid, Spain. His research interests include software governance, management information systems, software project management, people in software projects, software and services process improvement and management information systems. He received his PhD in Computer Science from the Universidad Politécnica of Madrid (2005). He also holds a MBA from the Instituto de Empresa (2002). He has been working as Software Engineer, Project Manager and Software Engineering Consultant in several companies including Spanish IT leader INDRA. He is also an Editorial Board Member and Associate Editor for several international journals (IEEE Software, Computer Standards and Interfaces, IET software...).