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