Christian Haas*, Georg Bretthauer and Jürgen Beyerer

Cybersecurity for industrial automation and control systems

Industrial automation and control systems are vital for the functioning of various industries such as energy, transportation, healthcare, and manufacturing. These automation and control systems encompass complex networks of machines, devices, and software applications that control, monitor, and automate critical operations. Any disruption or compromise to these systems can lead to significant economic losses, public safety risks, and potential national security threats.

In the digital age, industrial automation and control systems have become increasingly interconnected and reliant on information technology infrastructure. The protection of critical infrastructures, manufacturing processes, and sensitive data has become a paramount concern for industries worldwide. Consequently, industrial cybersecurity has emerged as a crucial research topic that demands attention and comprehensive studies.

Cybersecurity for industrial automation and control systems must consider specific requirements which are not as relevant in an office environment, in the case of PC workstations or Internet servers. The control of industrial processes is often associated with real-time requirements which make it difficult or even impossible to modify the systems. Software patches on the systems or the installation of monitoring software, malware scanners and antivirus programs, for example, can have an adverse effect on the functionality, while firewalls in the network and encrypted connections between the systems can be detrimental to the real-time conditions. In addition, the relatively long lifetime of hardware and software in industrial automation and control systems differs considerably from other areas of IT application. For this reason, new strategies and methods must be found to protect industrial automation and control systems, not only in new systems, but also in existing installations, above all.

This special issue aims to present new cybersecurity research results and methods to help to protect industrial automation and control systems in various industries. Knowledge about the automation and control systems that need to be protected is the first step to designing and implementing a cost-efficient security architecture. Therefore, an asset inventory with as much information as possible about e.g., the network infrastructure and devices is needed. The first article by Klaus Biß et al. “Device discovery and indentification in industrial networks” gives an overview on requirements and challenges to perform device discovery and identification in industrial networks and offers a first integration in the open-source tool Malcolm.

The next four contributions are method-oriented ones.

In distributed agent-based automation and control systems communication and data exchange between agents are a necessity. Especially if sensitive data are transmitted, security and privacy issues might arise if malicious attackers are able to eavesdrop data. The paper by Philipp Binfet et al. “Towards privacy-preserving cooperative control via encrypted distributed optimization” addresses this issue by presenting a novel privacy-preserving cooperative control scheme based on encrypted distributed optimization.

Future industrial automation and control systems will be composed of physical as well as virtual devices, which must be managed and orchestrated. Bootstrapping these devices and establishing the initial trust are a crucial step to operate the corresponding automation and control system securely. The article by Sören Finster et al. “Secure bootstrapping for next-gen industrial automation systems” therefore presents such a secure bootstrapping concept for next generation industrial automation and control systems.

Security by design is an important design paradigm while developing new automation and control systems. Security should be considered starting from the design phase of the system. One important aspect of security by design is the transparency and traceability

***Corresponding author: Christian Haas**, Fraunhofer IOSB, Karlsruhe, Germany, E-mail: christian.haas@iosb.fraunhofer.de
Georg Bretthauer, Karlsruhe Institute of Technology, Karlsruhe, Germany, E-mail: georg.bretthauer@kit.edu.
Jürgen Beyerer, Karlsruhe Institute of Technology, Karlsruhe, Germany; and Fraunhofer IOSB, Karlsruhe, Germany,
E-mail: juergen.beyerer@iosb.fraunhofer.de. https://orcid.org/0000-0003-3556-7181

of design choices. The paper by Sarah Fluchs et al. “Nachvollziehbare Security by Design-Entscheidungen für Automatisierungssysteme mittels funktionsbasierter Diagramme und Security-Bibliotheken” describes a design decision method that aims at enabling system engineers without comprehensive security knowledge to identify, make, and substantiate security decisions autonomously.

Cybersecurity standards and best-practice like e.g., IEC 62443, usually propose a risk-based approach for securing industrial automation and control systems. Consequently, a risk assessment is usually the first step to implement a security program. Different risk assessment methods have been proposed in the past. The article by Sine Canbolat et al. “A new hybrid risk assessment process for cybersecurity design of smart grids unsing fuzzy analytic hierarchy processes” presents a new hybrid risk assessment method based on fuzzy logic that leads to more precise risk assessment results.

The next two papers are application-oriented ones.

Energy systems are a prime example of a critical infrastructure that encompasses industrial automation and control systems. There, the digitalization of e.g., energy substations, leads to a high degree of automation, but on the other hand increases the risk of successful cyber-attacks. The paper by Dennis Rösch et al. “Transformation in substation automation: Cyber-Resilient Digital Substations (CyReDS) in power grids” deals with cyber resilience for digital substations as a basis for a cyber resilience monitor as a central instance for recording, assessing, and responding to security threats and incidents.

Cyber threat intelligence provides information about cyber attackers, including their intentions and attack techniques. The last paper by Markus Karch et al. “Integration of Cyber Threat Intelligence into Security Onion and Malcolm for use case of industrial networks” analyzes the availability of open-source cyber threat intelligence for industrial automation and control systems, with a particular focus on technical indicators that can aid in detecting cyberattacks. It concludes by presenting *CTIExchange*, a tool that facilitates the integration of cyber threat intelligence into security information and event management systems by connecting Threat Intelligence Platforms with detection tools.

This special issue is a starting point to encourage an in-depth discussion on cybersecurity for industrial automation and control systems. We wish you an inspiring lecture of the interesting contributions to this important and fascinating research field.