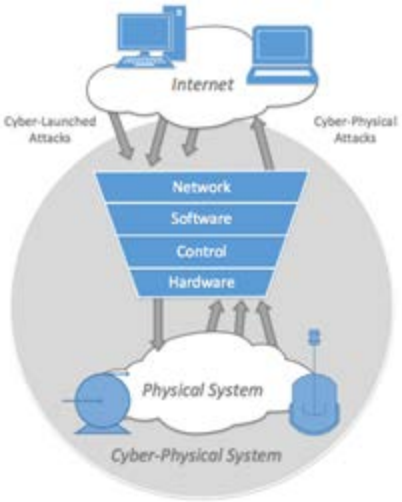
Security Improvement of Information Processing in the Production System Lifecycle

Security Improvement of Information Processing in the Industrial Production System Lifecycle is of major concern in industry practice because of the increasing application of software components and related software engineering activities in global and distributed engineering projects of Production Systems Engineering (PSE).

Industrial production systems, such as robots, manufacturing cells, or steel mills, control powerful and risky physical processes and must meet domain-specific **safety**, **environmental**, and **quality** standards. Meeting these standards is challenging for traditional production systems and even more challenging for **cyber-physical production systems** according to the *Industrie 4.0* vision. During the production system lifecycle and the installation of the system, **information processing** concerns the creation, change, exchange, and use of engineering data and artifacts in order to characterize, design, configure, and verify the future production system and its parts.



Information security and **cyber security** are **essential requirements** in modern networked environments to ensure the delivery of engineering artifacts with the required quality, to mitigate risks of knowledge espionage and theft, to test for security vulnerabilities, and to ensure the consideration of security implications during operations and maintenance. The traditional optimistic assumption of production systems and PSE processes existing in isolated environments without requirements for advanced IT security is obsolete as global PSE is conducted with data repositories that are connected via the Internet in collaboration with partially trusted and untrusted parties. Even legacy production systems may become unintentionally connected to the Internet due to modern replacement components.

Changes in PSE Engineering

The introduction of modern information technologies include a set of changes in PSE processes.

Centrally accessible data repositories. In very simplified terms, the engineering perspective includes functions, mechanics, fluids, electrical engineering, and control software. Today, each domain has specialized tools, and only recently have experts begun to bi-directionally exchange data between these tools; for instance, the electrical engineer might require changes in the mechanic layout because she chooses a different switching box. In order to facilitate this exchange, a central repository stores all the data and the software tools use a common data format, such as AutomationML. The repository is centrally accessible, but the storage and access control might be distributed, similar to federated storage schemes.

Global collaboration with partially trusted and untrusted parties. As the size and complexity of newly built or refurbished plants grow, the number of teams working on any specific project increases as well. In addition, many countries require or at least encourage the collaboration with local suppliers or planning companies. While in many cases their local expertise is very helpful, there might also be cases in which industrial espionage is a strong risk. Protecting IPRs while cooperating in complex projects becomes more and more important.

Modern information technology in a production system environment. There are two major aspects regarding modern information technology used in industrial settings: (i) modern and well-established business software security mechanisms are not or cannot directly be used in industrial settings; (ii) the threat landscape differs from typical business IT systems.

Core Research Directions

Based on the changes, research directions need to be addressed to improve security of information processing in the PSE Lifecycle:

- *Secure Modelling* of attach vectors to be considered in the PSE Life-Cycle.
- *Automated and secure testing* of Industrial Production System Families prior to commissioning.
- Improving *engineering processes* for PSE projects towards secure, flexible, and agile practices.
- Development of flexible, transparent, and *semi-automated tool chains* that support engineering processes in the PSE Life-Cycle.
- The contribution of *AutomationML* can support efficient data exchange within engineering tool chains for quality assurance, test automation, and engineering process improvement.

Key Messages

- Efficient, flexible, and secure **quality assurance** mechanisms and **test automation** in context of PSE.
- **Efficient and secure data exchange** in tool chains in distributed engineering processes.
- **Engineering Process Improvement** for flexible configuration of PSE processes.

Contact:

Prof. Dr. Stefan Biffl
TU Wien
stefan.biffl@tuwien.ac.at
qse.ifs.tuwien.ac.at

Prof. Dr. Arndt Lüder
Otto von Guericke University Magdeburg
Arndt.lueder@ovgu.de
www.iaf-bg.ovgu.de

Dr. Edgar Weippl
Secure Business Austria gGmbH
edgar.weippl@sba-research.org
www.sba-research.org