Security for Industrie 4.0
Trends -- Challenges -- Opportunities

Dr. Wolfgang Klasen
Siemens Corporate Technology and Member of the German Platform Industrie 4.0

Digitalization revolutionizes business and creates major challenges & opportunities for manufacturing companies

- § **Humans, machines, processes, and the flow of goods are connected through networks**
- § **Intelligent devices make autonomous decisions and will perform tasks independently**
- Ø **This will decrease development/production time and costs, and increase efficiency and profitability.**

Platform I4.0 Working Group
“Security of Interconnected Systems” – Identified Key Topics

- **Secure communication for Industrie 4.0**
  - What are the essential requirements for dynamic value creation networks across companies and how to build an infrastructure for this?
- **Identities and their protection / verification**
  - What is a secure identity? Why are secure identities important? How can you verify if an identity is secure?
- **Integrity of data and systems**
  - What is the integrity of data and systems? How to ensure integrity?
- **Trustworthiness**
  - How to determine the trustworthiness of an I4.0 component, e.g. with a uniform metric ? Which level of trust is required within a value creation network?
  - How to determine the real trust level along the value creation network?
- **Security support for legal contracts**
  - Knowledge of the skills and possibilities (of trustworthiness) of the individual participants
- **Security within the company organization, education, and training**
  - How can we introduce and foster security processes and skills within SMEs

Security within Industrie 4.0 = Security-by-Design

Security-by-Design as a superior principle

- Subsequent enrichment of systems is not sufficient.
- Security measures have to be integrated (up to application level).

Security for the digital model

- Security for the physical instance, its digital twin and their interactions must take place in a concerted way.

Adaptive security architectures

- Agile security profiles have to be adaptable in a dynamic way.
- Fast configuration must include security.

Authentication and Secure Identities for Devices

- Unforgeable identities and trust anchors are needed.
- Keys respectively security credentials must be bound to the device.

Industrial Security enables Industrie 4.0

IT Security as enabler of business models

Digitalization of business processes often mandate additional measures regarding IT security. Ease of use and plug & operate are important pre-requisites for their acceptance.

B2B vs. B2C communication

Individual and short-term consideration of customer requests (“batch-size 1”) need enhanced security

Standardization enables secure infrastructures

Security requires standardized specifications of interfaces and protocols to support requirements and to negotiate and operate security profiles (security semantics) between different domains.

Prevention and reaction are still needed

Security will remain moving target. There will be no final I4.0 security solution without a need for further measures.

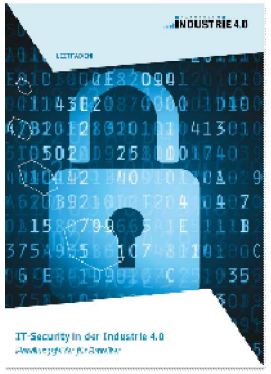
Platform I4.0 WG 3: Security of Networked Systems

Available Publications:

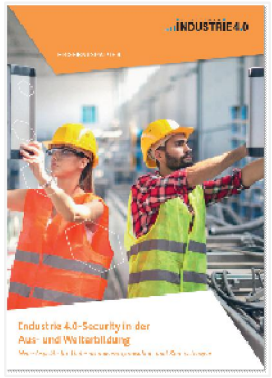
http://www.plattform-i40.de/I40/Navigation/EN/InPractice/Online-Library/online-library.html

Application scenario in practice: order-controlled production of a customized bicycle handlebar

IT-Security in Industrie 4.0



IT-Security in Industry 4.0 fields of action for operators



I4.0-Security in Education and Training

Security in the Administration Shell (yet, only available in German)

Technical Overview: Secure Identities

Technical Overview: Secure cross-company communication

Security in RAMI 4.0

German National Funded Project IUNO

PLATTFORM INDUSTRIE 4.0

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Trust in Industrie 4.0 requires adequate security measures

Basis of the project are four I4.0 application scenarios:

- Customized production
- Market place for technology data
- Remote maintenance platform
- Visual IT security operation center for production

IUNO follows the security-by-design principle to consider appropriate security measures starting with a risk based requirements analysis, the design and implementation of adequate security countermeasure elements and the final evaluation within the application demonstrators.
Project results especially shall give guidance to small and medium enterprises.

https://www.iuno-projekt.de/

IUNO

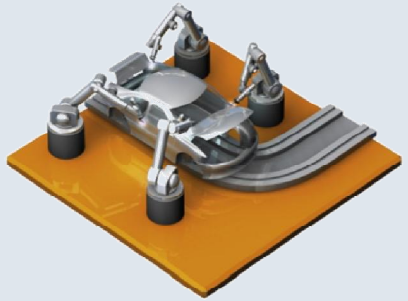
Nationales Referenzprojekt
IT-Sicherheit in Industrie 4.0

accessec · BOSCH · DFKI · DURAVIT
escrypt · Fraunhofer AISEC · Fraunhofer IESE · Fraunhofer SIT
HOMAG GROUP · Infineon · nobilia · PHOENIX CONTACT
Rexroth Bosch Group · SIEMENS · Technische Universität Darmstadt · Technische Universität München
TRUMPF · Universität Kassel · VOLKSWAGEN · WIBU SYSTEMS

Thank you for your attention

Cyber Physical Systems include physical and digital representation

Cyber-Physisches System (CPS)



physical production

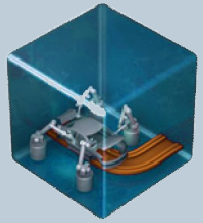
+

digital model

Contains all information on:

- software / HW
- mechanical devices
- electronics
- automation, HMI
- safety, security
- maintenance
- geographical information
- identities
- status information
- release information
- interfaces
- …

The digital twin will be updated and maintained across the entire life cycle



design → production planning → production engineering → production → services