Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE 4.0

Secure Ecosystem for Smart Manufacturing

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

Berlin, 2018/05/15

Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE 4.0

Key questions of the Session

- Industrie 4.0 connects humans, machines, processes, and the flow of goods along value chains. This requires comprehensive security architectures covering all participants. Integrity of products, processes and machines has to be assured across these value chains and during the whole lifecycle.
  - Which security requirements do we expect for this infrastructure and how can such an infrastructure be established?
  - How can we assure a high trust level along the value creation network?
- Security by design has to be the superior principle. Subsequent enrichments of systems regarding security are not sufficient. Security measures have to be integrated within industrial applications and will support end-to-end security. Security also has to cover the digital model: security for the physical instance, its digital twin and their interactions must take place in a concerted way.
  - How can security-by-design be accomplished for the complete life cycle?
  - How does a road map for an Industrie 4.0 security ecosystem look like?

Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE4.0

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

➢ This will decrease development/production time and costs, and increase efficiency and profitability.

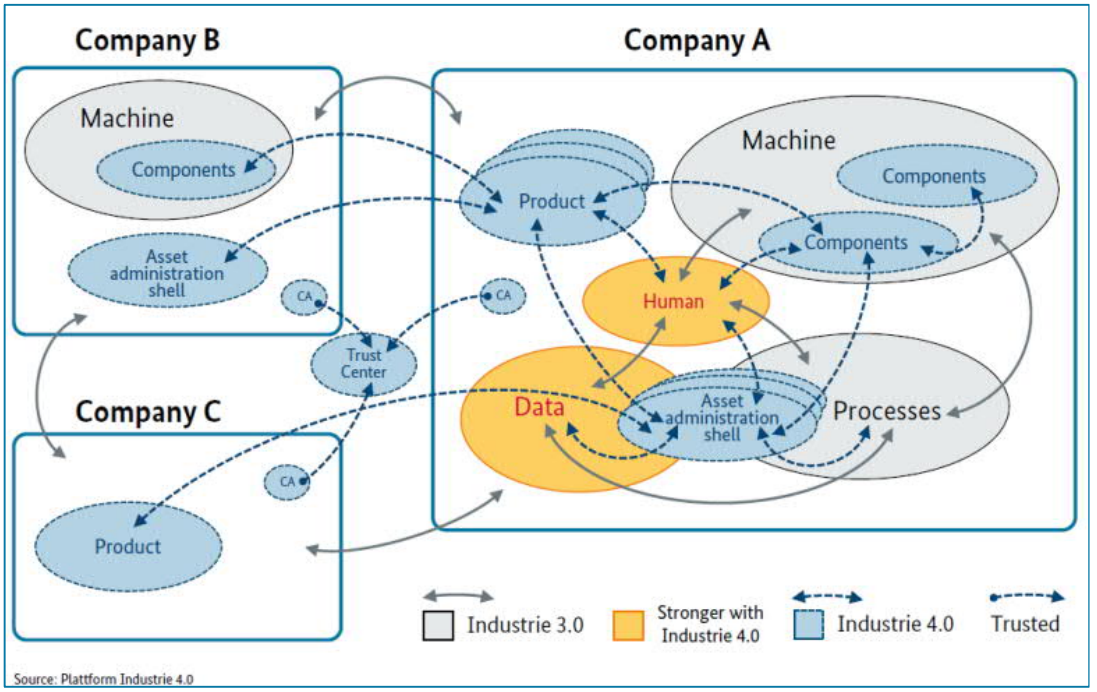
Federal Ministry for Economic Affairs and Energy

PLATTFORM INDUSTRIE 4.0

Cooperation accross security domains characterises I4.0 use cases

- Increasing flexibility and customer-specific production by
  - ad-hoc interconnections realize value creation networks across company boundaries
  - direct data exchange of all entities (people, machines, processes etc.)

→ **Increased attack surface**



Boundary Conditions of Industrie 4.0

- Data exchange between the entities is based on trust of the partners
- Legally relevant communication between machines entities will be necessary to realize ad-hoc interconnections

Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE 4.0

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 + physical representation

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

Authentication and Secure Identities for Devices

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

Adaptive security architectures

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

Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE 4.0

Industrial Security will enable Industrie 4.0

Security for Inter Domain Communication

- Interconnect existing Industrie 3.x security architectures to enable secure inter domain cooperation
- **Global and robust key management infrastructure needed**

Prevention and reaction are still needed

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

Trustworthiness is needed for cooperation

Authenticity and Integrity of data and systems along the value chain support confidence about security levels of involved parties.

Standardization enables secure infrastructures

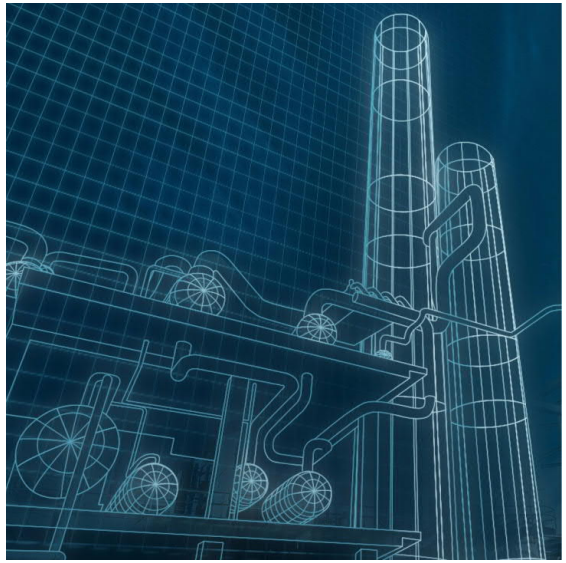
Security requires standardized specifications of interfaces and protocols to support requirements and to negotiate and operate security profiles (security semantics) between different domains.

Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE 4.0

Digitalization meets industry: Securely connecting and improving all steps along the plant lifecycle

Product Design | Process and Plant Design | Engineering and Commissioning | Operation | Service



“Industrie 4.0”

Merging the real plant with its digital twin: consistent data on all levels and throughout all life cycle phases by integrating engineering software and plant automation

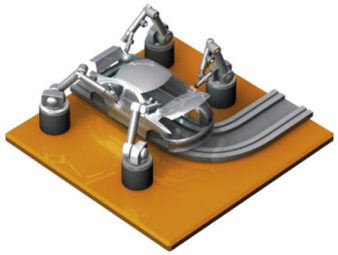
Security needs to protect throughout the complete life cycle

Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE 4.0

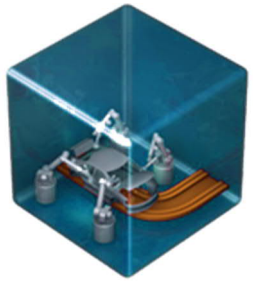
Cyber Physical Systems include physical and digital representation

Cyber Physical System (CPS)



physical production

+

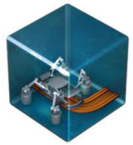


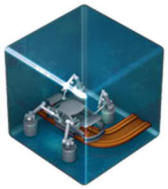
digital model

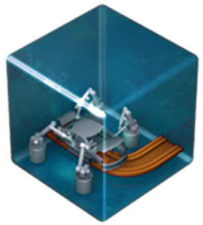
Contains all information on:

- 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

Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE4.0

Security Architectures need to cover systems and processes across the complete life cycle

Organizational Security & Processes

People, Policies, Processes, Governance

- Organizational Preparedness
- Secure Development
- Secure Integration and Service
- Vulnerability and Incident Handling

Products & Systems

Common security technologies need to be implemented and contribute to the overall secure architecture

- Secure System Architecture
- System Hardening
- Access Control and Account Management
- Security Logging & Monitoring
- Data Protection and Integrity
- Security Patch Management
- Malware Protection
- Backup and Restore
- Secure Remote Access
- Privacy

Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE 4.0

Corner stones / Pillars / Mechanisms of a I4.0 capable security infrastructure

- Credential Management, e.g., PKIs of different stakeholders
- Secure Communication (e.g. End2End/Application Layer, Hop-By-Hop/TransportLayer)
- Support of Secure WAN Infrastructure (5G – „Security Confirmation“ by technical means)
- Overarching Security Monitoring + Event Handling / Inter Domain Cooperation
- Long Term Capable Security Mechanisms (crypto agility, protocol agility)
- Resilience
- Secure supply chain mechanisms, trustworthiness
- Auditability (Non Repudiation,…)
- Security Infrastructure Services: e,g. Secure Time Service, DNSsec+, ABAC

- Approach: Take state-of-the-art security Infrastructure
  and focus on additional requirements introduced by Industrie 4.0.

Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE 4.0

Why do we need “Security – by –Design”

Overall Goal

- Provide cost efficient security features within products and systems, which protect against (critical) threats, which are assumed to happen (sometime).
- Ensure, that security part of your solution can integrated within existing logistics, service infrastructure, and life cycle of environment.
- Ensure, that the security part of your solution can be operated (and understood) by existing team members.

Federal Ministry for Economic Affairs and Energy

PLATTFORM INDUSTRIE 4.0

Managing Cyber Security in Critical Environments through Standards and Regulations (some examples)

IEC ISO

- IEC 62351 – Power systems management and associated information exchange – Data and communications security
- IEC 62443 – Industrial communication networks - Network and system security
- ISO/IEC 15118 – Road vehicles -- Vehicle to grid communication interface

ISO JTC 1 IEC INFORMATION TECHNOLOGY STANDARDS

- ISO 27001 – Information technology - Security techniques - Requirements
- ISO 27002 – Code of Practice for information security management

IEEE

- IEEE 1588 – Precision Clock Synchronization
- IEEE 1686 – Intelligent Electronic Devices Cyber Security Capabilities

IETF

- RFC 4301 – Security Architecture for the Internet Protocol
- RFC 5246 – Transport Layer Security TLS v1.2
- RFC 6347 – Datagram Transport Layer Security DTLS v1.2

FERC FEDERAL ENERGY REGULATORY COMMISSION

Homeland Security

NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

- Critical Infrastructure Protection CIP 001-014
- Executive Order EO 13636 improving Critical Infrastructure Cyber Security
- IoT Cybersecurity Improvement Act 2017

Bundesamt für Sicherheit in der Informationstechnik

- IT Security Act
- B3S Standards
- BNetzA Security Catalogue
- German Energy Act

- Network Information Security Directive

ANSSI Agence nationale de la sécurité des systèmes d'information

- Critical Infrastructure Protection
- Certification and Key Measures

CPNI Centre for the Protection of National Infrastructure

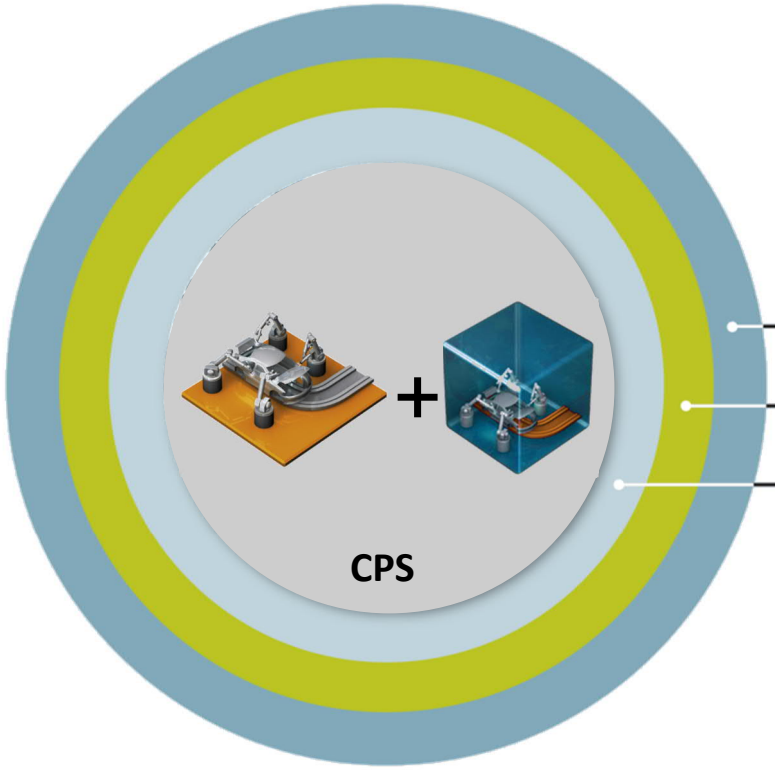
- Cyber Essential Scheme
- Direct adaptation of European NIS Directive and GDPR (General Data Protection Regulation

Note: the stated organizations and standards are just examples and are not complete

Federal Ministry for Economic Affairs and Energy

PLATTFORM INDUSTRIE 4.0

Developing I4.0 Security based on IEC 62443 (e.g.)



Plant security

- Intelligent access to buildings, plants and virtual assets
- Self synchronizing access control

+

Security management performs dynamic threat analysis and agile adaption of technical measures

+

Network security

- Dynamic, flexible network architectures
- Permanent monitoring of networks and communications

+

System integrity

Protection and proof of integrity of the overall system during the whole lifecycle incl. supply chain

+

- Integrity of systems of systems
- Self healing security

+

Federal Ministry for Economic Affairs and Energy

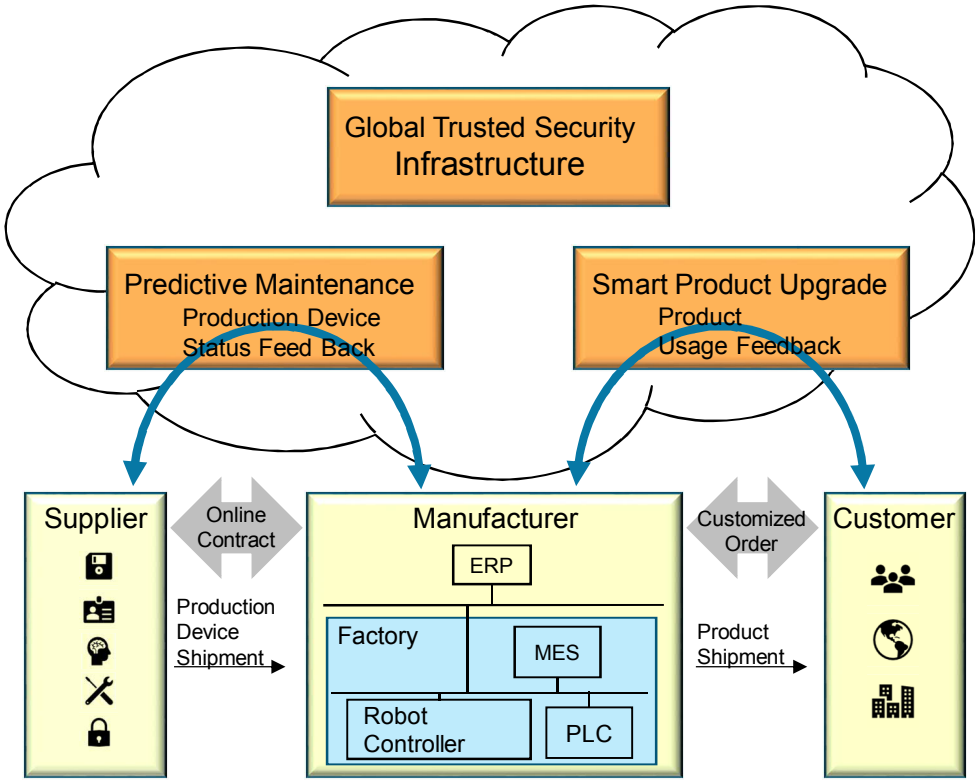
PLATTFORM INDUSTRIE 4.0

Robot Revolution Initiative / Industrie 4.0 cooperation for Secure Industrial Internet of Things / Industrie 4.0

In order to achieve security and trustworthiness we aim to:

- Incorporate trustworthiness in the lifecycle of services, products, production systems and IT/OT systems - on a risk-based approach
- Implement secure communications (company-wide/ cross-company)
- Establish open, clear and transparent indicators and profiles for trustworthiness on company-, system-, and product-level
- Provide reliable information and assurances regarding the trustworthiness of their products to the customer
- Accomplish that each partner's trustworthiness can be identified along the entire supply chain

➢ Develop a common roadmap with joint next steps and priorities and provide input for the ongoing international standardization work



Federal Ministry
for Economic Affairs
and Energy

PLATTFORM INDUSTRIE 4.0

Plattform Industrie 4.0: Working Group „Security of Networked Systems“

Thank you for your attention!

Contact:
Name: Dr. Wolfgang Klasen
Email: wolfgang.klasen@siemens.com