

Security for Industrie 4.0

Platform Economy and Trustworthiness Standardization

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

Industrie 4.0

Connecting business processes – across company borders

- ▶ Internet is available everywhere, simple and cheap.
- ▶ Devices are becoming intelligent.
- ▶ Industrie 4.0 connects all parties involved in business processes in manufacturing, process industry and supply chain.
- ▶ Information from suppliers, customers and within your own company is connected and transparently available.
- ▶ Work pieces and machines manage the production autonomously – flexible, efficient, resource-saving.
- ▶ There are transitions between companies and sectors.
- ▶ Using the new technologies in a smart way opens up a new world of value-add services and functions.



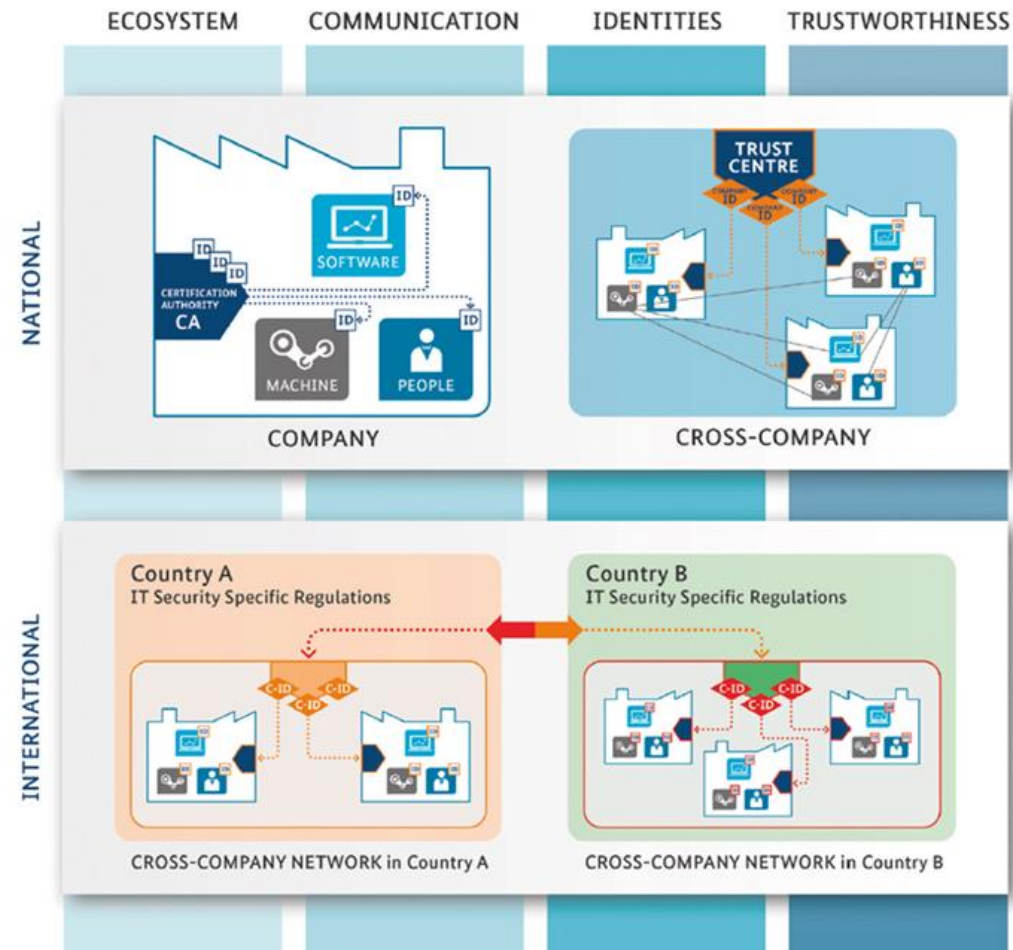
Graphic © Anna Salari, designed by freepik

Working Group „Security of Networked Systems“

Challenges and coordinated approaches

Structuring key issues and consolidation into key challenges and solutions results in various approaches:

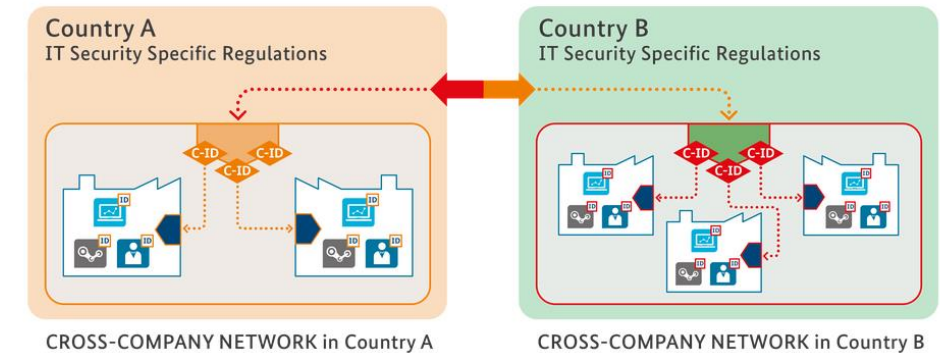
- ▶ Secure ecosystems
- ▶ Secure communication
- ▶ Secure identities
- ▶ Trustworthiness



Working Group „Security of Networked Systems“

Approach: Secure Ecosystems

- ▶ Establish Security-by-Design as a superior principle
 - ▶ Subsequent enrichment of systems is not sufficient.
 - ▶ Security measures must be integrated (up to the application level).
- ▶ Security for the digital twin + physical asset
 - ▶ Security for the physical asset, the digital twin, and their interactions must be aligned.
 - ▶ Digital twin is challenge AND opportunity for security
- ▶ Interoperable Security Policies are needed
- ▶ Coordinated political framework is prerequisite

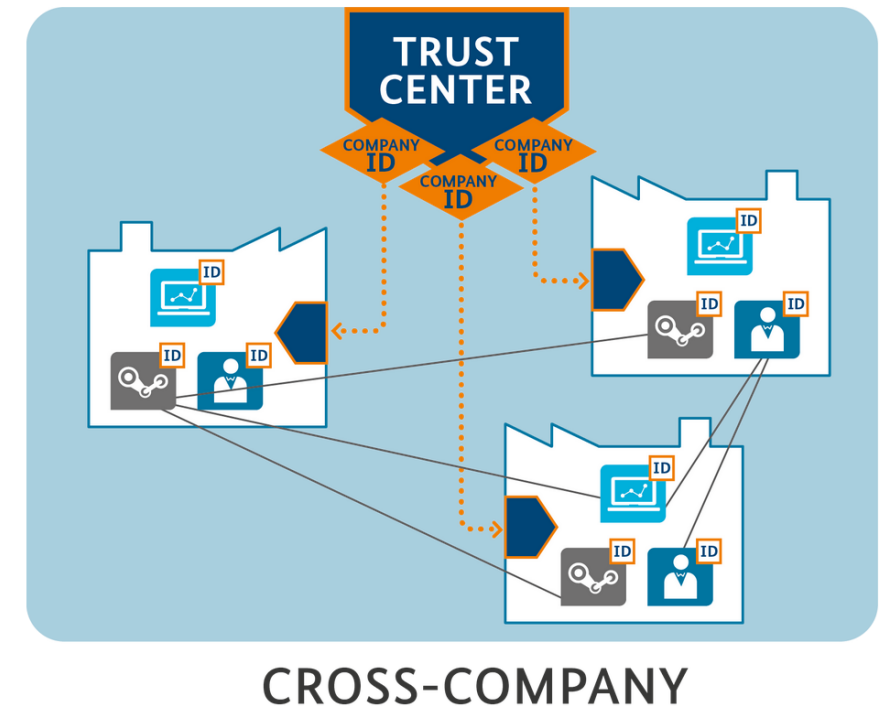


© Plattform Industrie 4.0

Working Group „Security of Networked Systems“

Approach: Secure Communication

- ▶ Always consider security in the communication architecture
- ▶ Develop a standardized classification of data depending on the protection goals
- ▶ Ensure standardized interoperable security policies of all participating partners within the value chain
- ▶ Enable detection and response for the data streams

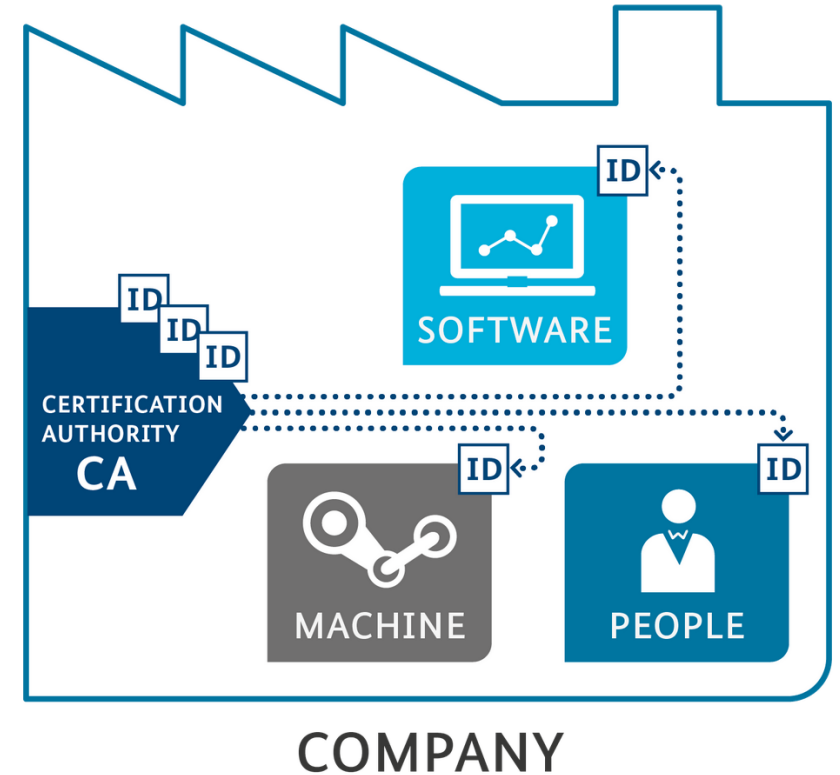


© Plattform Industrie 4.0

Working Group „Security of Networked Systems“

Approach: Secure Identities

- ▶ Every entity involved in the communication (human, machine, product, software) of a company must have at least one secure identity
- ▶ Secure identities must be issued within a company by an trusted authority.
- ▶ In case of machine-entities, secure identities must be inseparably bound to the entities itself
- ▶ For the processing on the bases of secure identities between companies/security domains, the mutual recognition of the entities and the setting of a commonly agreed security level is prerequisite



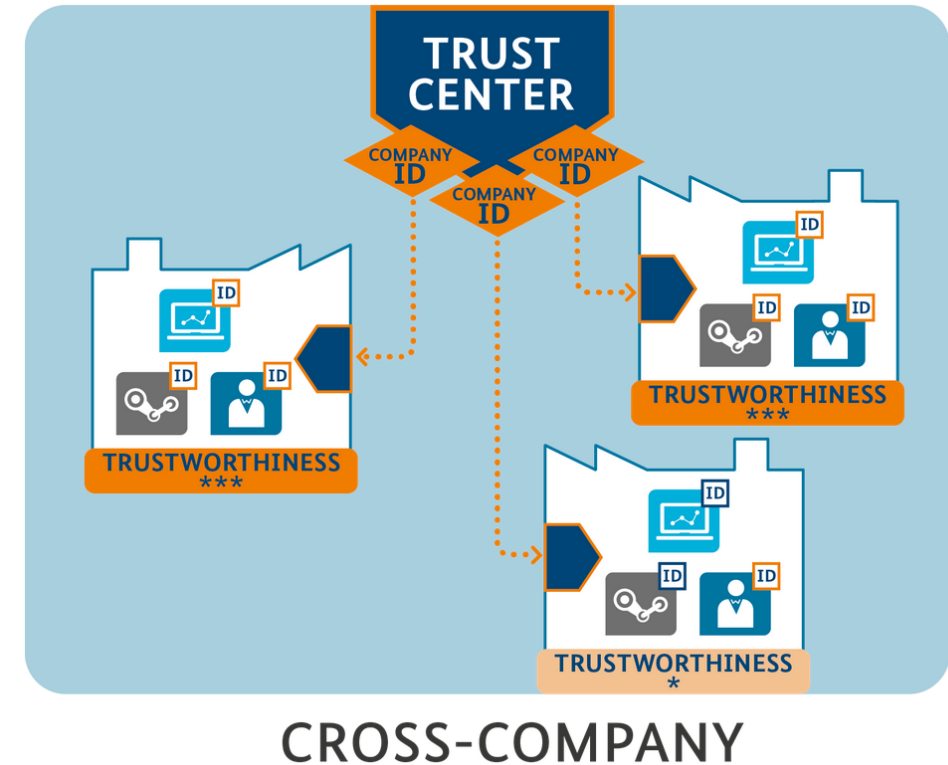
© Plattform Industrie 4.0

Working Group „Security of Networked Systems“

Approach: Trustworthiness

- ▶ Qualitative decision criterion for business-related actions along the entire value chain
 - ▶ Authenticity and integrity of data and systems along the value chain
 - ▶ Reliable and verifiable security concept of the communication partners

- ▶ International standardization of trustworthiness and integrity protection concepts



© Plattform Industrie 4.0

Trustworthiness – perspective from Industrie 4.0

Business P2P

- ▶ Trustworthiness often rely on reputation, intuition (guts feeling) and further business indicators like credit worthiness

M2M

- ▶ At the end, a machine, must be able to assess the trustworthiness of logically connected systems before engaging and proceeding with transactions

International standardization started working on “Trustworthiness” recently (ISO/IEC JTC1)

Managing Cyber Security through Standards and Regulations (some examples)



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



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



- 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



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



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



- Network Information Security Directive



- Critical Infrastructure Protection
- Certification and Key Measures



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



Working Group „Security of Networked Systems“

Proposed Security Standardization Topics

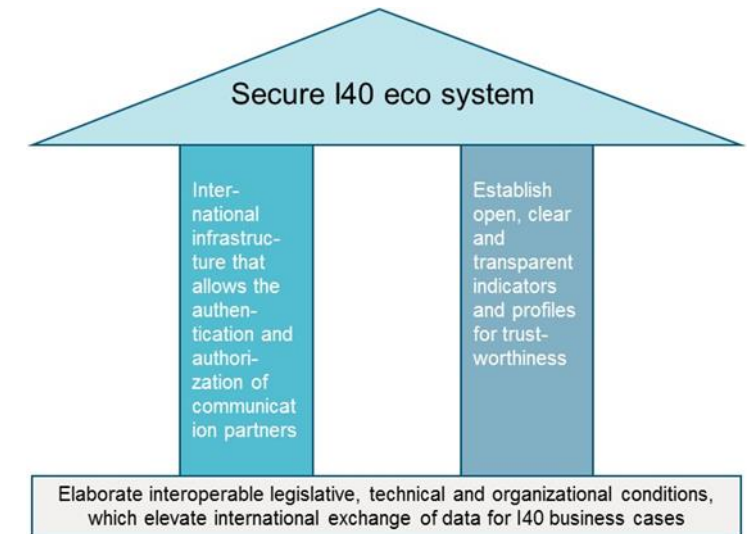


- ▶ Security-Infrastruktur trusted inter-domain communication
- ▶ Security for agile Systems
- ▶ Trustworthiness of the Value Add Network
- ▶ Standardized Rolls and Rights Management for I4.0 Entities
- ▶ Standardized Security-Engineering-Prozess (for Integrators and Operators)
- ▶ Security level modelling for composite products

Working Group „Security of Networked Systems“

What do we need?

- ▶ International collaboration of industry and politics to elaborate an compabile legal, technical and organizational conditions to allow the cross-border exchange of data fostering new data driven business models.
- ▶ International infrastructure that allows the authentication and authorization of the communication partners
- ▶ Open, clear and transparent indicators and profiles for security may including the allowed usage of the data
- ▶ International standardization of trustworthiness and integrity protection concepts



© Plattform Industrie 4.0

▶ Cooperation between RRI and Plattform Industrie 4.0 will support this approach

Thank you
for your attention !

