PLATTFORM INDUSTRIE 4.0

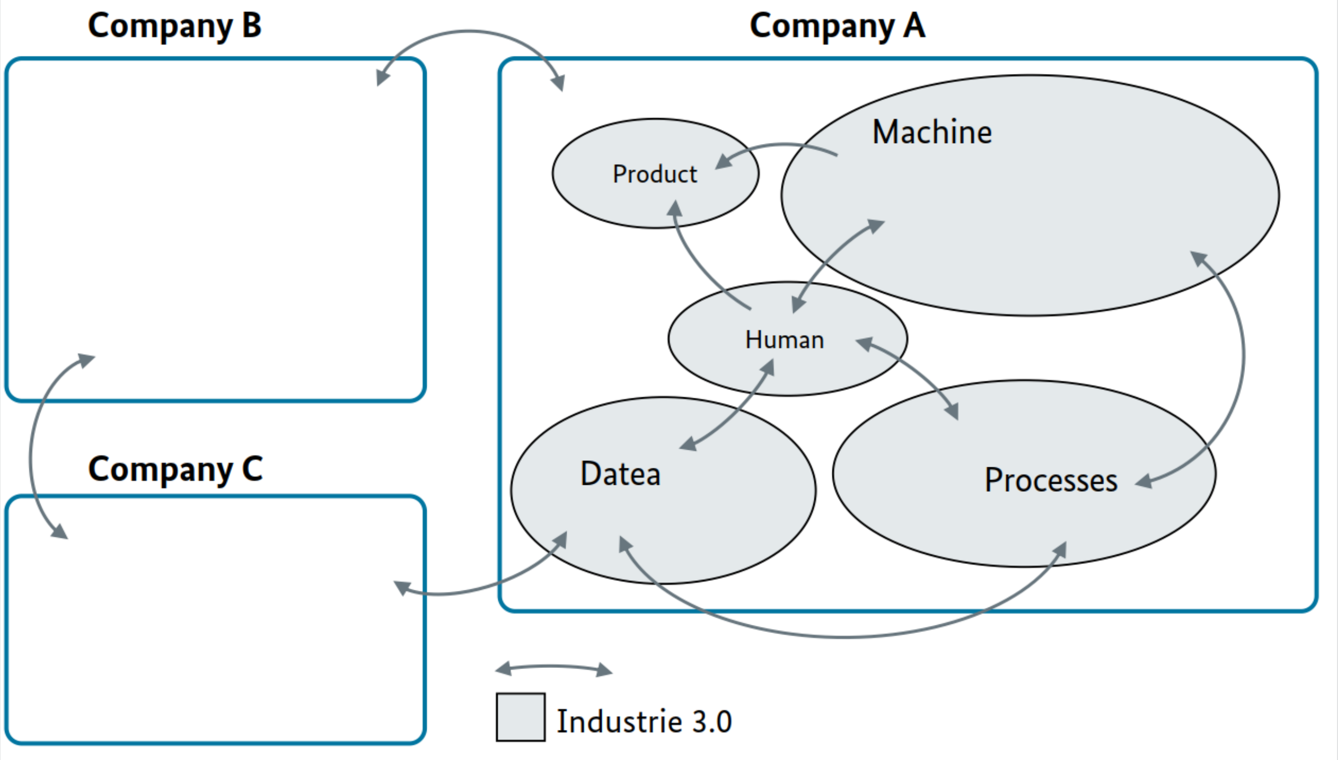
Federal Ministry
for Economic Affairs
and Energy

Secure Communication for Industrie 4.0

Dr. Lutz Jänicke

Product & Solution Security Officer, Phoenix Contact GmbH & Co. KG

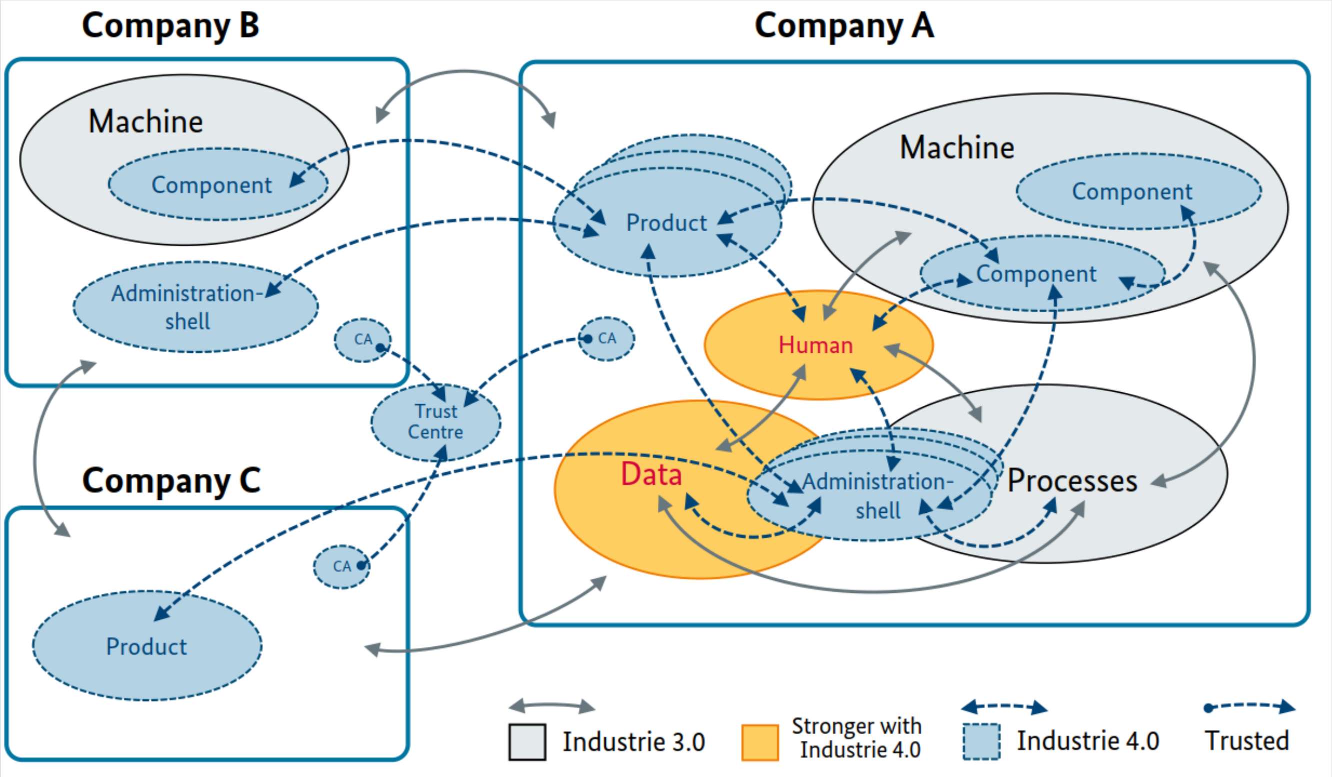
Current Communication Patterns



- Communication occurs between companies
- Connections with specific security requirements may even be manually configured
- Each company constitutes its own security domain

Source: Plattform I4.0

Future Communication Patterns



- Communication occurs between entities across company borders
- Communication is no longer handled inside a security domain
- Connections may be established autonomously/ad hoc

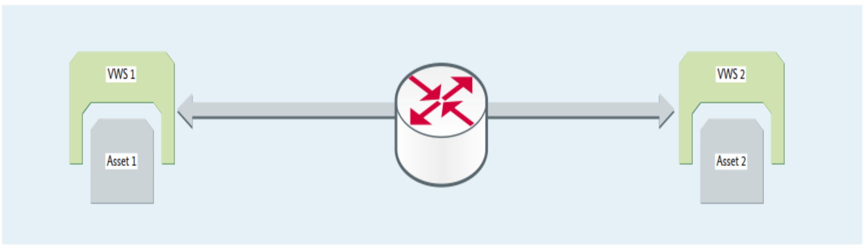
Known Security Technologies used in Communication

- Algorithms for strong encryption and integrity protection
  - AES, SHA-2, …
  - RSA, Elliptic Curves, …
- Strong authentication mechanisms
  - Public Key authentication (X.509 certificates), 2-Factor Authentication
- Protocols implementing security
  - TLS, IPsec, SSH, …
  - OPC UA, …
- **Why discuss secure communication?**

Multi-Stakeholder Challenge

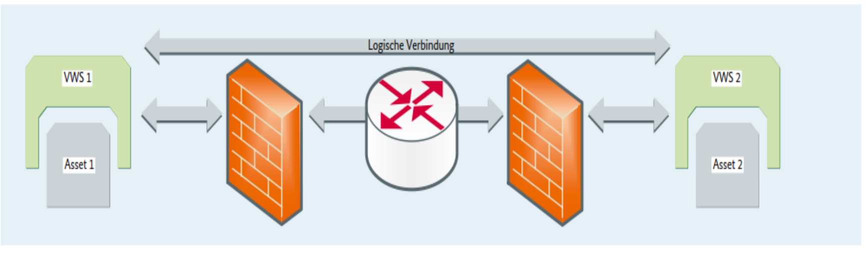
- In Industrie 4.0 communication will cross borders of security domains
- Security Domain
    - A domain that implements a security policy and is administered by a single authority (NIST SP 800-53 Rev. 4)
- Connections have to comply with policies from multiple security domains
- Examples
    - Some data is confidential, therefore needs to be encrypted
    - Every data entering or leaving must be checked for malware
    - Data that is encrypted cannot be checked, therefore may be dangerous and must be blocked

Communication Protocol Challenge: End-to-End



- Both peers can apply all security techniques
- Confidentiality ensured
- Integrity ensured
- Authentication ensured
  - With Public Key/X.509: possible
  - With password: encrypted in connection
- Inspection/Monitoring: **impossible**

Communication Protocol Challenge: Middlebox(es)



Middlebox:

- Firewall
- Proxy
- Webfilter
- …

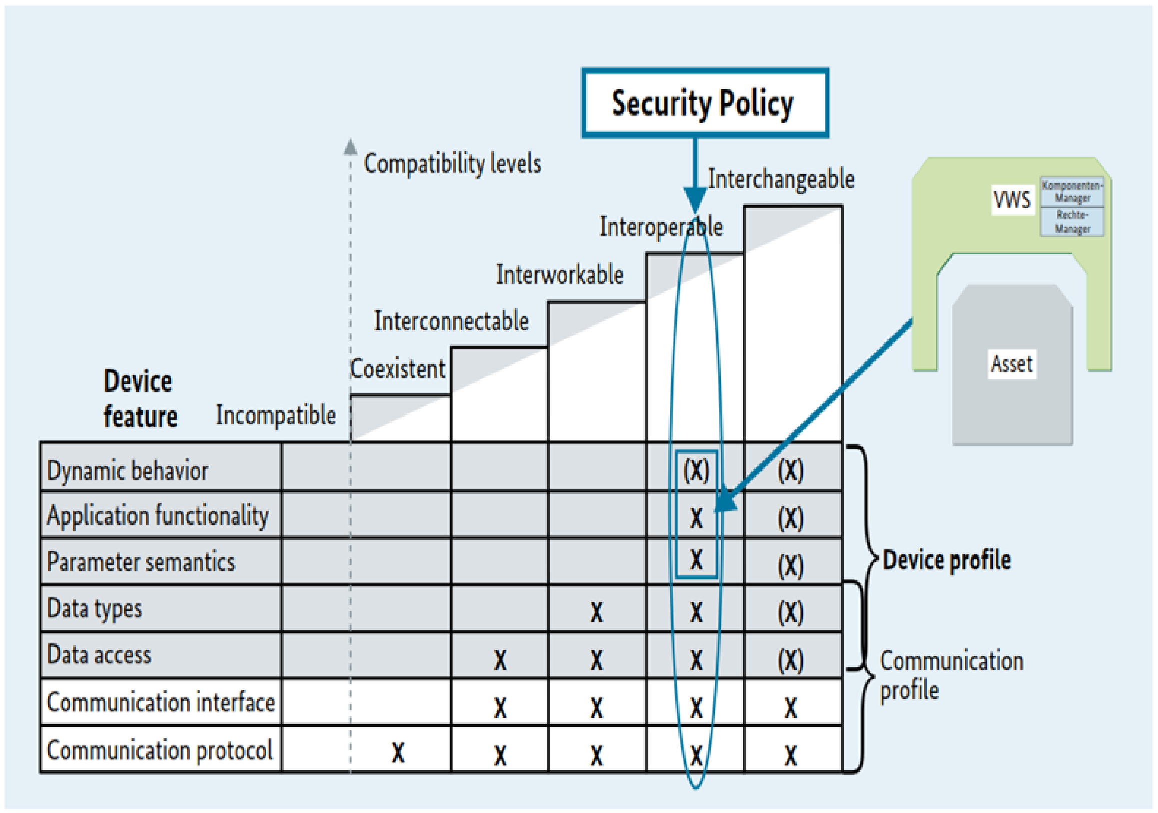
- Only techniques allowed by the Middlebox can be used
  - Middlebox operated by company security administrators

- Example: TLS (HTTPS)
  - Communication may be terminated at middlebox, inspected, new connection to peer
  - Confidentiality broken on middlebox
  - Integrity control broken on middlebox
    - Workaround: integrity protection on message, not connection
  - Authentication
    - with X.509 broken/impossible
    - with passwords (may be read in middlebox)

Security objectives and current protocols

- Security objectives are separate
  - Confidentiality
  - Integrity
- Many scenarios only require integrity protection/authenticity
  - User credentials may need confidentiality
- Most secure communication protocols combine encrypting and signing
- **Architecture and protocols need to take into account end-to-end integrity with inspection options**

Compatibility of Security Policies



Device feature	Incompatible	Coexistent	Interconnectable	Interworkable	Interoperable	Interchangeable
Dynamic behavior					(X)	(X)
Application functionality					X	(X)
Parameter semantics					X	(X)
Data types				X	X	(X)
Data access			X	X	X	(X)
Communication interface			X	X	X	X
Communication protocol		X	X	X	X	X

Source: Plattform I4.0, inspired by IEC TR 62390

- All peers need to have a common understanding of security objectives and requirements
- Compliance with security policies is required to be interoperable
- Technical means to express policy compliance have to be integrated into the interaction and communication models

Enhancing Identity Information

- Participants in Industrie 4.0 communication must be uniquely identifiable
- Secure identification may be implemented by public key methods
  - X.509 certificates combine electronic key with identity information
- Most common X.509 identification schemes are used for web servers
  - X.509 certificates are issued for domain name (www.domain.name)
  - Ownership validation often by “access to postmaster@domain.name” by owner of private key
  - X.509 certificate states “**just this**”
  - X.509 certificate does not imply trustworthiness of services or else
  - “Browser CA” is a business model, not a security concept

Enhancing Identity Information

- In order to foster the Trustworthiness approach, additional information needs to be added into the identification process
  - Compatibility of security policies
  - Current security status of system or organization, …
  - …
- Evaluation of this information must be integrated into communication process
  - In a standardized manner

Reliable Connections

- Security objective: **Availability**
- Business models need high availability
  - No Communication → No Business
- Industrial Communication needs deterministic behavior
  - **Bandwidth** and **latency** requirements
- Confidentiality and Integrity can be achieved by peers
- (Internet) availability involves additional parties
  - Local/international providers
  - Long distance communication
  - Crossing national boundaries
- **Critical international infrastructure**

Key questions

How can we ensure consistent and secure handling of data and information in a multi-peer value creation network?

- Requirements of all stakeholders must be taken into account
- Information must be classified and handled according to a standard scheme
- Information must be labelled accordingly
- Adherence of stakeholders must be ensured as part of **Trustworthiness** in a standardized way

Key questions

How can we determine the authenticity and trustworthiness of peers in ad hoc relationships?

- Infrastructure for secure digital identities is needed
- Technical security can be ensured by algorithm and implementation
- Authenticity can be ensured by registration processes
- Trustworthiness needs an additional evaluation/conformance scheme

Key questions

Which infrastructure support is needed to assure secure and reliable communication in the distributed value chain?

- Performant, highly available Internet
  - Including supporting services like name resolution…
- Secure Identification Framework
  - Technical and organizational, trusted by all peers
- Standardized handling of security objectives
  - Trustworthiness evaluation concepts

Thank you for your attention!

Contact:

Dr. Lutz Jänicke
ljaenicke@phoenixcontact.com