Future (inter-) network communication in Industry 4.0

14. 3. 2016

Prof. Dr.-Ing. Georg Sigl

Lehrstuhl für Sicherheit in der Informationstechnik
Technische Universität München

Fraunhofer Institut für Angewandte und Integrierte Sicherheit, AISEC

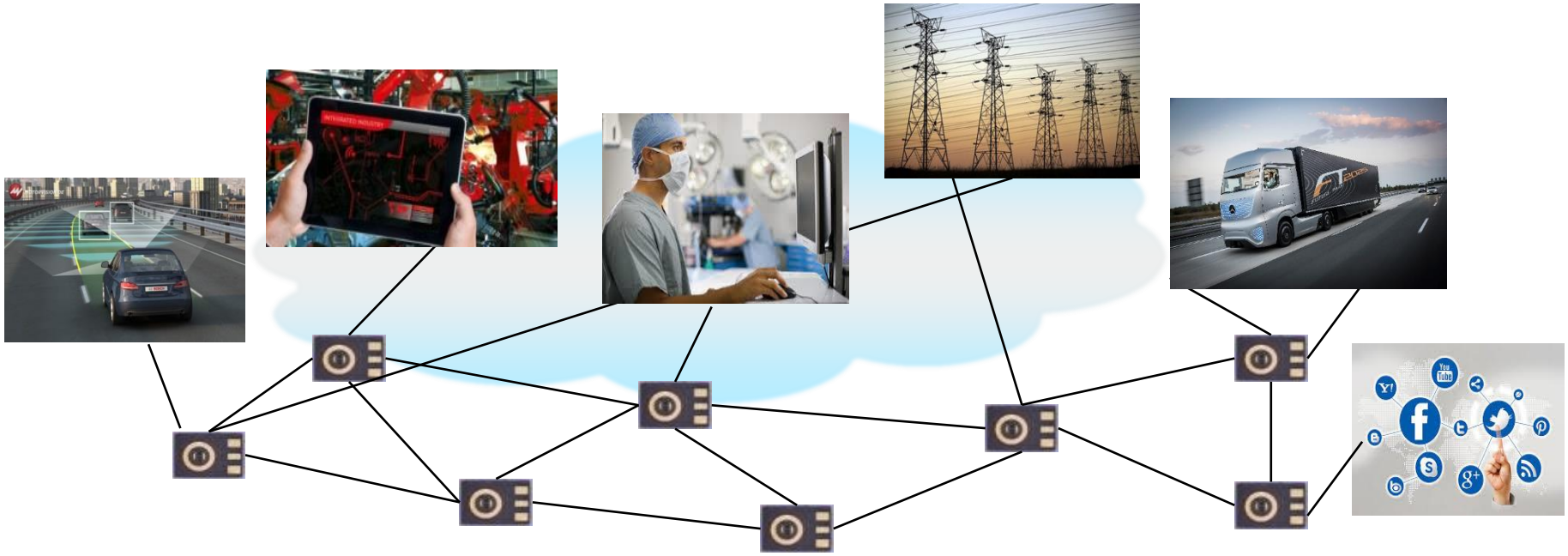
Fraunhofer AISEC

Agenda

1. Connected Eco-Systems
2. Industry 4.0: Characteristics
3. Security Risks: Examples
4. Industry 4.0: Security Challenges
5. Security Research
6. Take Home Message

Industry 4.0: Connected Eco-Systems

- Connection of industrial IT and business IT
- Communication across companies
- Communication from sensors into the cloud

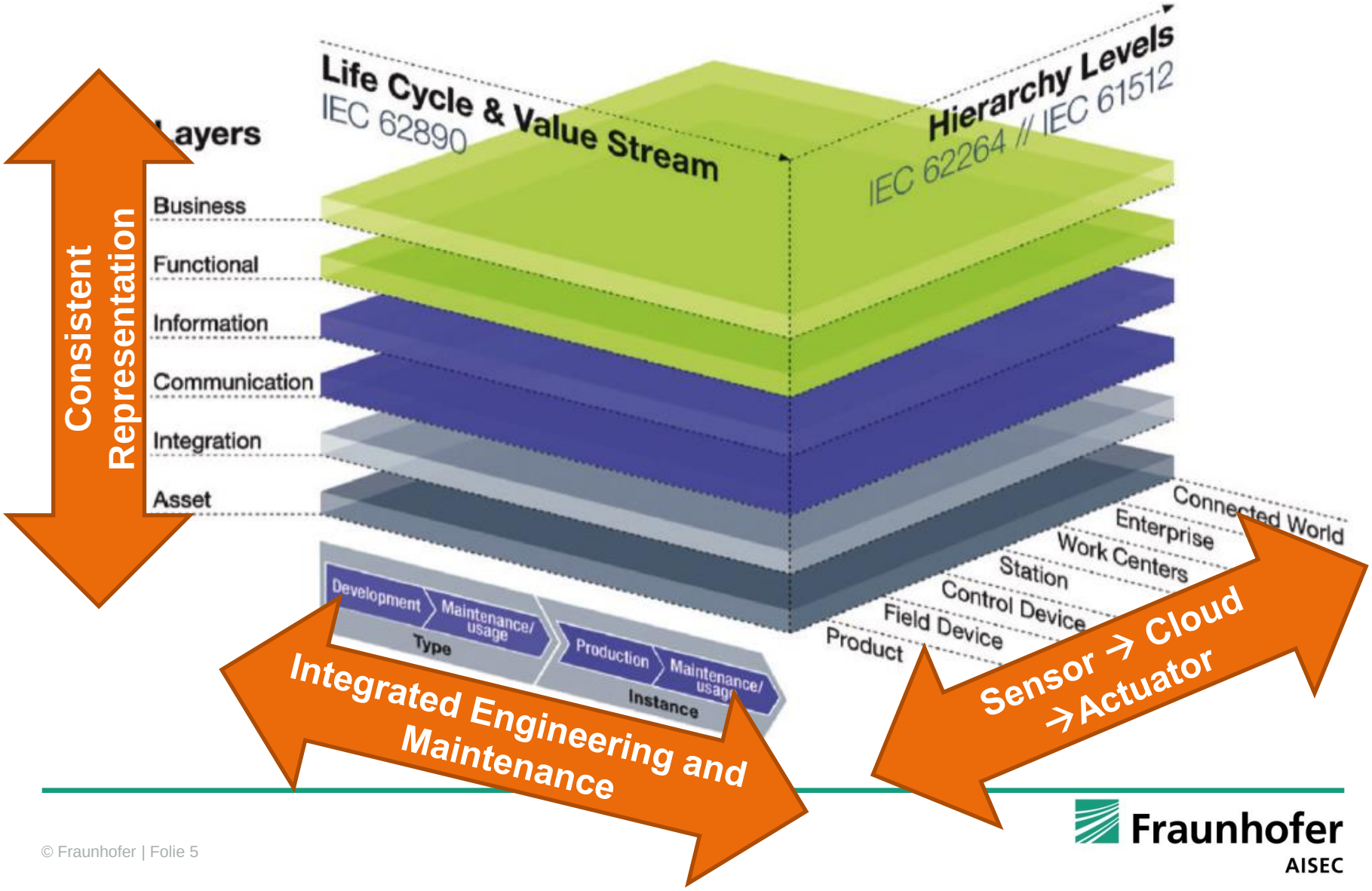


Fraunhofer AISEC

Agenda

1. Connected Eco-Systems
2. **Industry 4.0: Characteristics**
3. Security Risks: Examples
4. Industry 4.0: Security Challenges
5. Security Research
6. Take Home Message

Reference architecture model RAMI 4.0



Fraunhofer AISEC

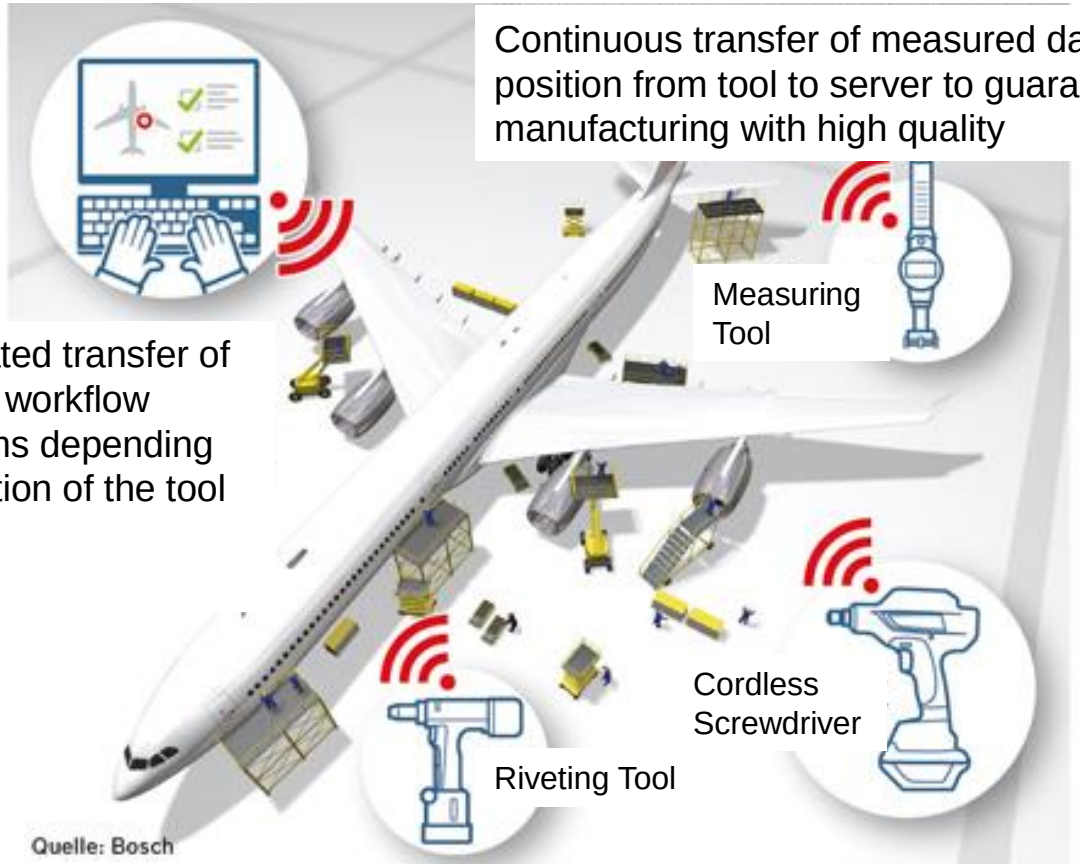
Interaction between hierarchy levels

- Smart products & tools: Decentralized production
  active parts in assembly control their own production

Example:

Airbus

Assembly

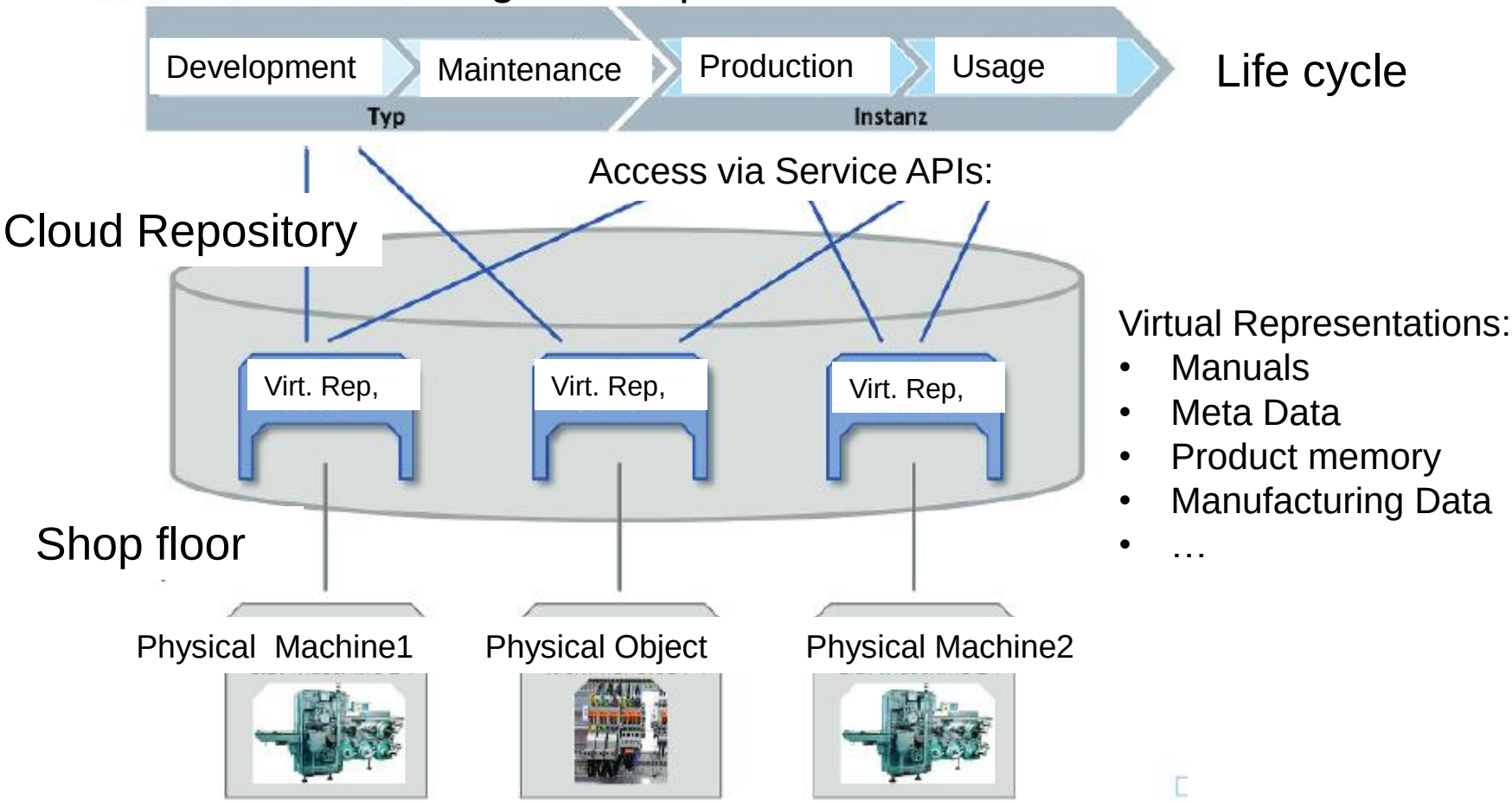


Source Bosch/Rexroth

Fraunhofer AISEC

Interaction between layers

- Cloud-based collaboration cross-domain:
  access controls: heterogeneous policies, roles, IDs



Virtual Representations:
- Manuals
- Meta Data
- Product memory
- Manufacturing Data
- …

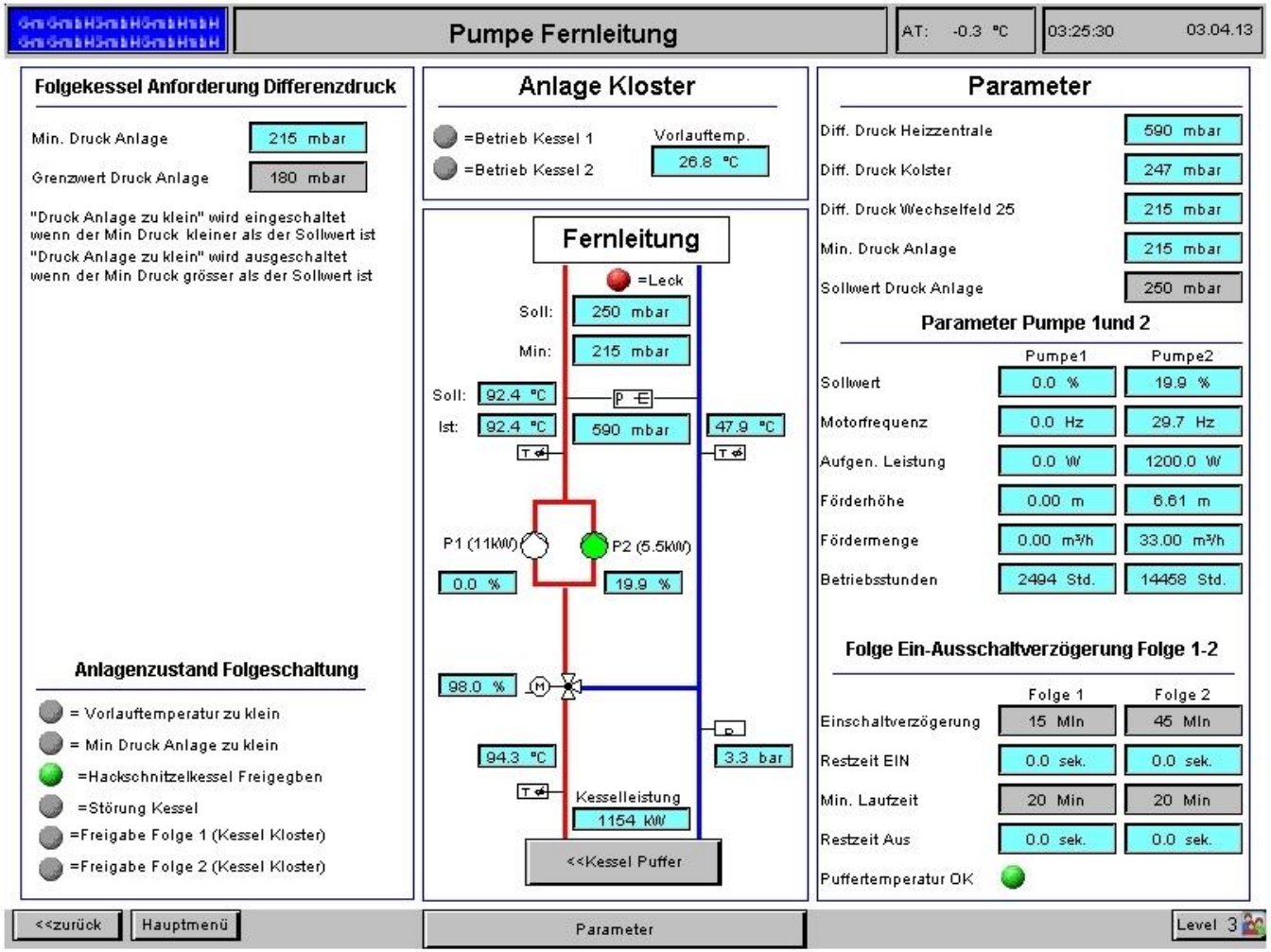
Fraunhofer AISEC

Agenda

1. Connected Eco-Systems
2. Industry 4.0 : Characteristics
3. **Security Risks: Examples**
4. Industry 4.0: Security Challenges
5. Security Research
6. Take Home Message

Security Risks

Internet access to control-units in power station

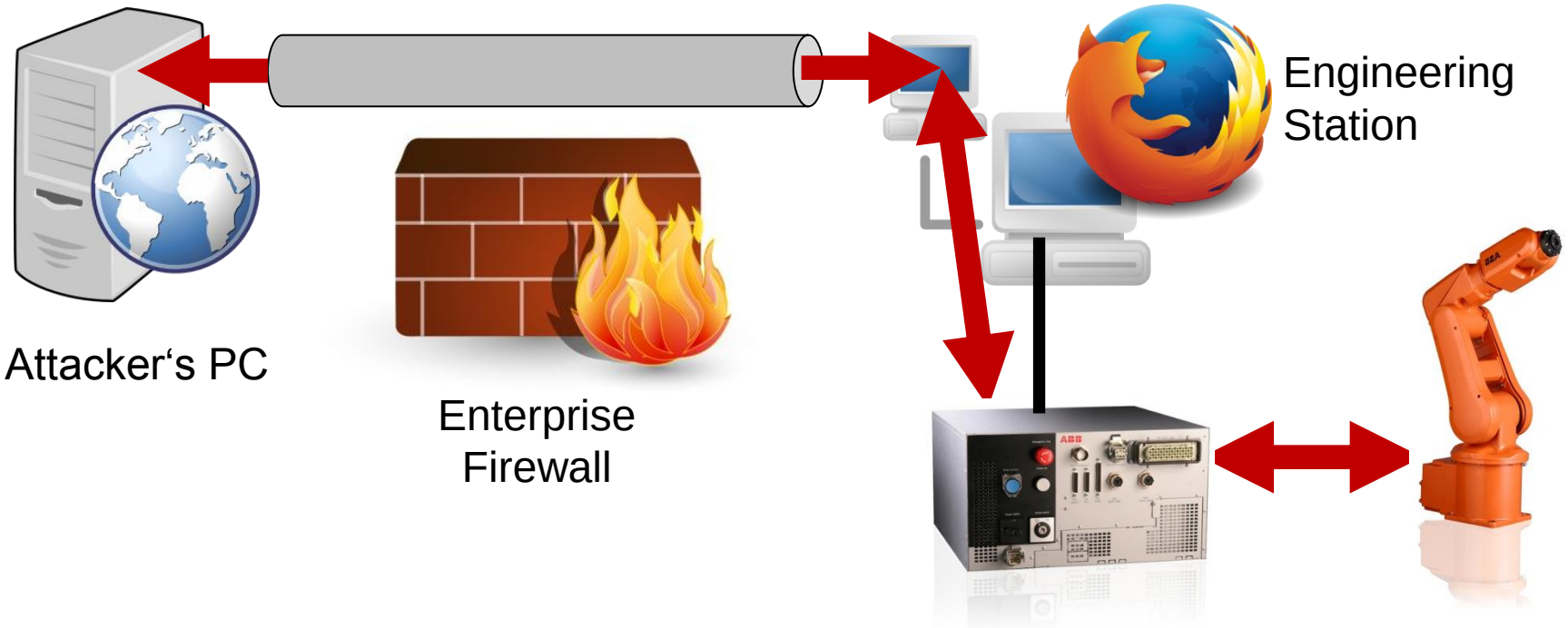


Fraunhofer AISEC

Security Risks

Hacking a standard industrial robot

- Exploiting classical Web vulnerabilities to connect the attacker PC and the Engineering Station
- Activation of debug-interface of VxWorks: full control



Fraunhofer AISEC

Agenda

1. Connected Eco-Systems
2. Industry 4.0 : Characteristics
3. Security Risks: Examples
4. **Industry 4.0: Security Challenges**
5. Security Research
6. Take Home Message

Security Challenges

Challenges derived from Characteristics:

1. Smart, connected products, tools, machines

⇒ Secure M2M communication, product integrity

2. Cloud-based cross-domain collaboration

⇒ Identity & Access management, confidentiality


Fraunhofer AISEC

Security Challenges

Challenges derived from Characteristics:

3. Service-orientation, Data Analytics

⇨ Data owner-ship, trustworthy platforms, integrity

4. Software-based configuration, individualization

⇨ App Security, secure communication, availability


Fraunhofer AISEC

Security Challenges

Challenges derived from Characteristics:

5. Human-Machine collaboration

➡ trustworthy robots, safety implications, privacy

6. Connected Eco-System

➡ trustworthy mobile devices, protected networks

Fraunhofer AISEC

Agenda

1. Connected Eco-Systems
2. Industry 4.0 : Characteristics
3. Security Risks: Examples
4. Industry 4.0: Security Challenges
5. **Security Research**
6. Take Home Message

Protect the chips: Biometry of silicon chips

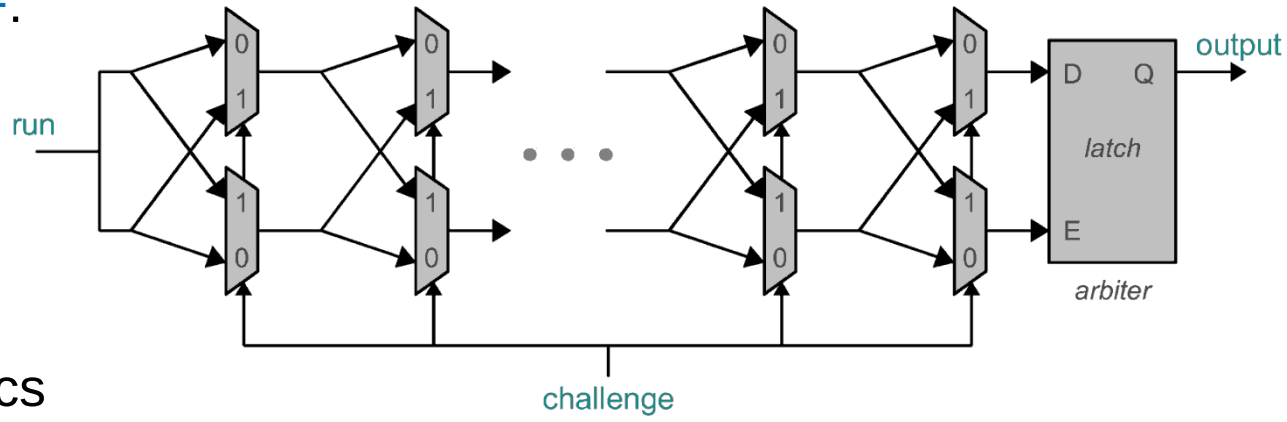
Unclonable Object ID: Biometry of objects

- Physically Unclonable Function (PUF)

Concept: Physical characteristics of integrated circuits define unclonable PUF behavior: extraction of secrets

Example: Arbiter PUF:

- 1-bit output,
- Input signal: race through the two delay paths
- Delay characteristics define PUF behavior

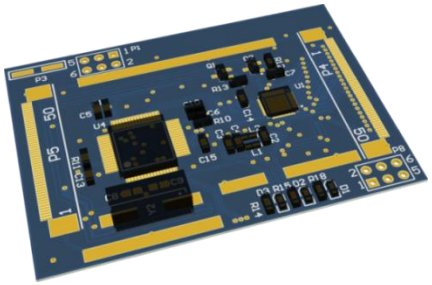


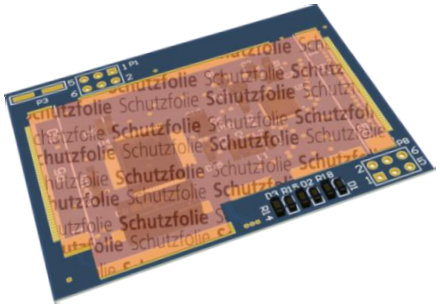
Fraunhofer AISEC

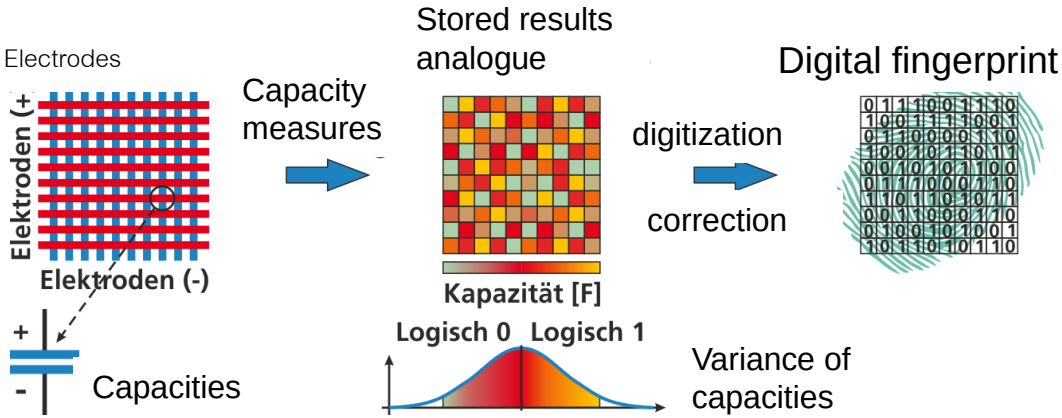
Protect the parts: Product Protection Foil

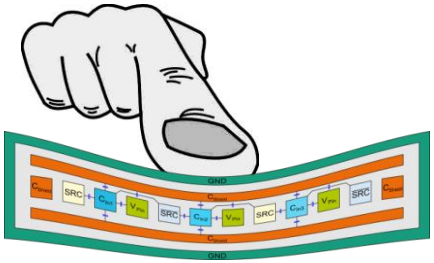
Smart foil (PUF): protecting component

- PUF: capacity measurements
- Material defines digital fingerprint
- Keys K derived from PUF, no storage
- Firmware encryption with K
- Manipulated foil: key K is lost







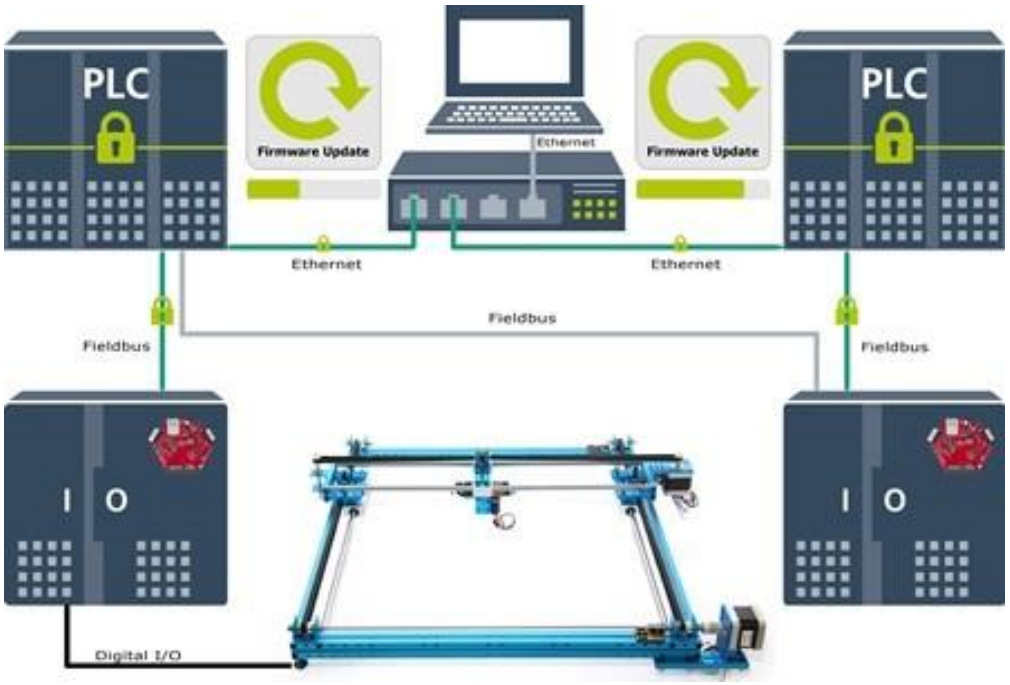


Fraunhofer AISEC

Protect the machines

Authentication in Industrial control systems:

- Integrating Secure Elements in PLC: plug & trust
- PLC-Authentication, certificates, PKI
- Controlled access
- Encrypted PLC Firmware
- Signed Code
- Secure Updates



Fraunhofer AISEC

Protect the networks

Controlling Flexible Industrial Networks:

SDN: Decouples network logic from physical devices

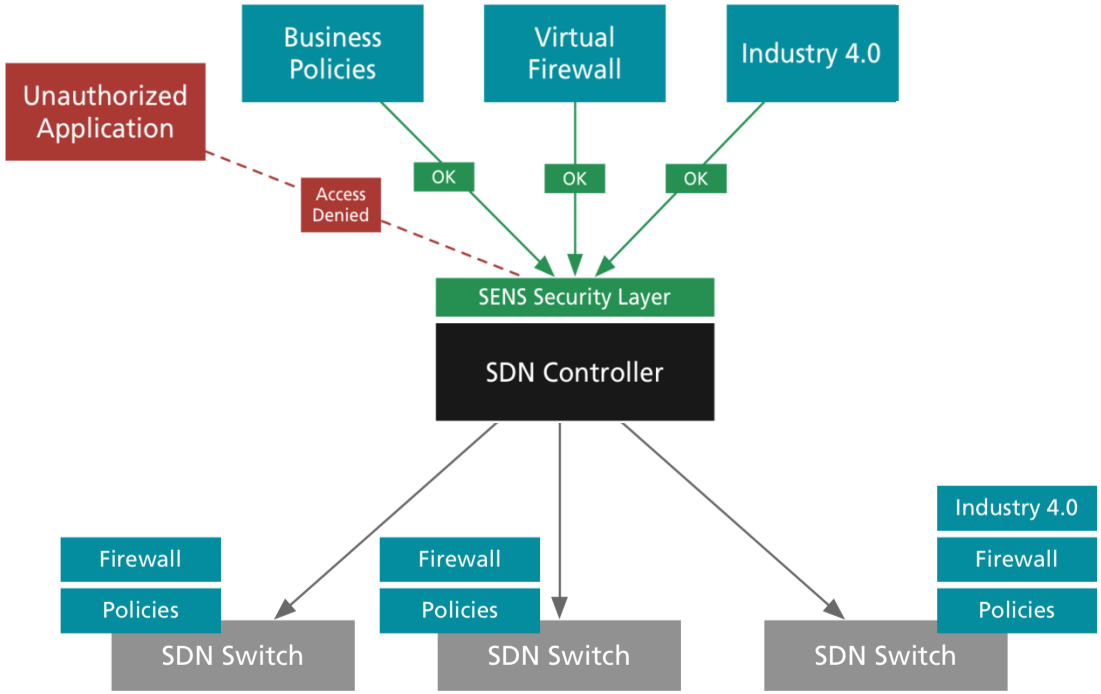
- Decision making in software → flexible
- Packet handling / forwarding in hardware → fast

SDN Controller:

- API to SDN applications

Protected Access → SENS

- Access permissions
- Authenticated access



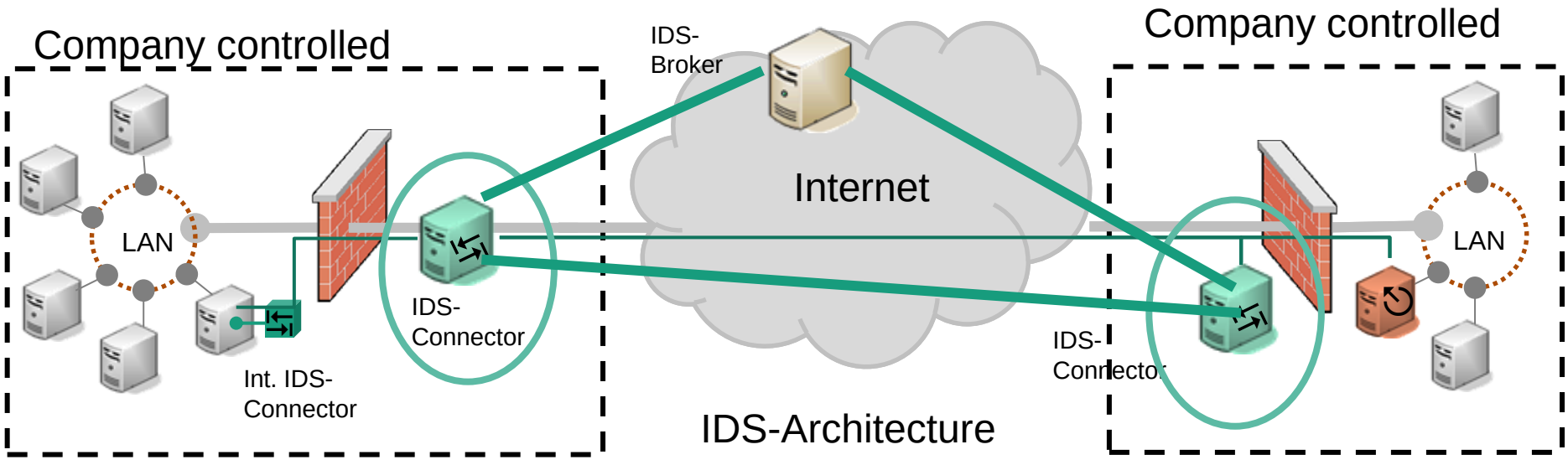
Fraunhofer AISEC

Protect the data

Security architecture for IDS (Industrial Data Space)

Connector as central component; Different Security Levels:

- L0 (secure connection),
- L1, L2,
- L3 (integrity and authenticity of receiver and provider, reliable accounting, data usage control)



Fraunhofer AISEC

Take home message

- Industry 4.0
  - Individualized
  - Connected
  - Data driven

- Security needs
  - Authentication of every Thing
  - Integrity over all representations
  - Secure communication over all hierarchies
  - Trusted data exchange

Thank You for Your Attention

Georg Sigl

TU Munich, Institute for Security in Information Technology

Fraunhofer-Institute AISEC, Munich

E-Mail: sigl@tum.de
georg.sigl@aisec.fraunhofer.de

Internet: http://www.sec.ei.tum.de
http://www.aisec.fraunhofer.de

Twitter: @FraunhoferAISEC

Fraunhofer AISEC