IT-SECURITY FOR INDUSTRIE 4.0

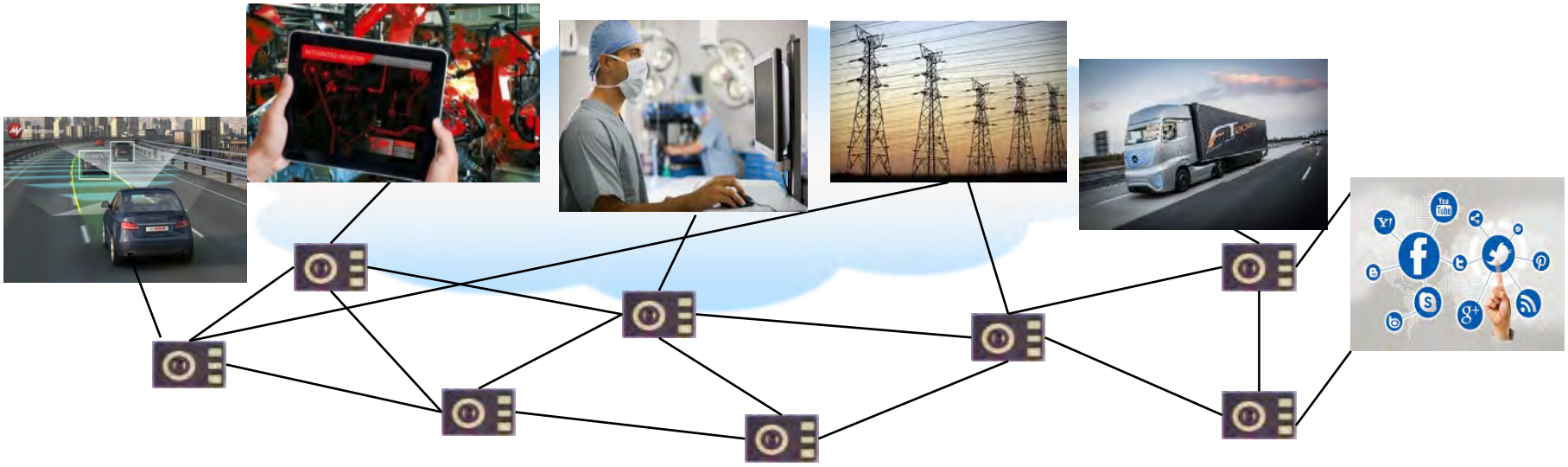
Claudia Eckert
Fraunhofer-Institute for Applied and Integrated Security (AISEC)
TU Munich, Chair for IT Security

Fraunhofer AISEC

Fraunhofer AISEC

Industrie 4.0: Connected Eco-System

- Connected: from Sensors into the Cloud
- Cross-Enterprise, cross-domain
- Software-driven, sensor intelligence
- Every device is network enabled, runs IP
- Remote access, maintenance & administration



Fraunhofer AISEC

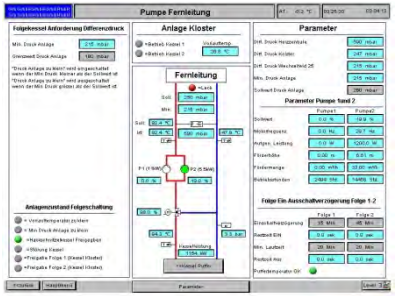
Connected Eco-Systems:

New security risks and threats!


Security Risks

- **Growing number of Vulnerabilities:**
  - Sensors, Embedded Software, Apps, Networks, …

- **Increased damages**
  - Networked systems: IT-problems impair Industrial IT (OT) and vice versa, e.g. safety problems
- **Targeted attacks**: Cyber Attacks are Big Business!
  - E.g. Ransomeware: increased by113%



Examples

(1) Attack on a power station via Internet access

(2) Attack on Jeep Cherokee via WiFi interface

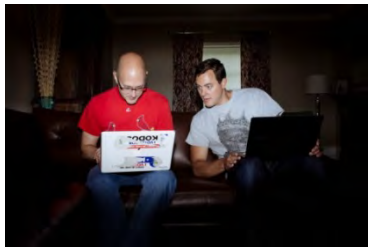
(3) Attack on industrial robots via Web-Browser

Cyber Security Threats

Example: Attack on Jeep Cherokee of Fiat Chrysler (2015)

Remote hacking of the car while it was driving!

- Remote control over safety critical components!



Approach:

- Gaining WiFi access to entertainment unit:
  Basis: weak password based authentication

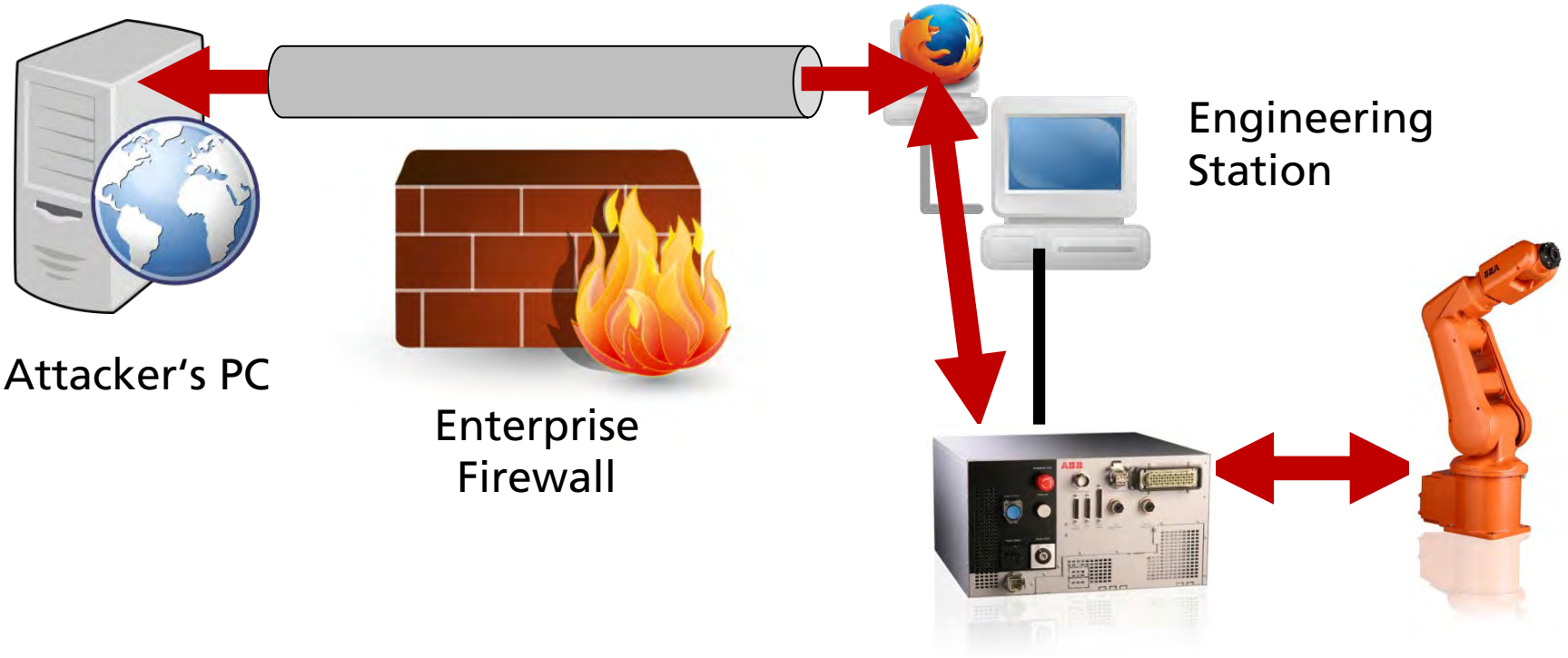
- Access on CAN bus using V850 Controller
  Basis: load malicious firmware on controller,
  no authentication, updates without control

- **Sending commands** over CAN bus:
  Remote control over steering wheel, brakes, door locks

Cyber Security Threats

Example: Hacking a standard **industrial robot at FhI AISEC**

- Exploiting classical Web-vulnerabilities (IT problems!) to connect the attacker PC and engineering station
- Activation of debug-interface of VxWorks: no authentication
- Gaining full remote control of robot! Safety implications …



Fraunhofer AISEC

Office IT Security versus Operational IT

	Operational IT	Office IT
Component Lifetime	Up to 20 years	3-5 years
Availability requirement	Very high	Medium, delays accepted
Real time requirement	Critical	Delays accepted
Physical Security	Very much varying	High (for critical IT)
Application of patches	Slow, certification, liability	Regular / scheduled
Anti-virus	Uncommon / hard to deploy	Common / widely used
Security testing / audit	Occasional	Scheduled and mandated
Security Awareness	Increasing	High
Security Standards	Under development	Existing

Lessons Learned for I4.0

A holistic approach is needed

- Risk- and Threat Assessments methods are required: e.g. be aware of dependencies

Fraunhofer AISEC

Lessons Learned for I4.0

A holistic approach is needed

- Risk- and Threat Assessments methods are required: e.g. be aware of dependencies

- Security Technology must be integrated appropriately: avoid isolated measures
- Security within Life-Cycles: e.g. secure updating

Fraunhofer AISEC

Lessons Learned for I4.0

A holistic approach is needed

- Risk- and Threat Assessments methods are required: e.g. be aware of dependencies

- Security Technology must be integrated appropriately: avoid isolated measures
- Security within Life-Cycles: e.g. secure updating

- Adapted and new Technologies are required: risk-based, tailored to individual needs

Lessons Learned for I4.0

A holistic approach is needed

- Risk- and Threat Assessments methods are required: e.g. be aware of dependencies

- Security Technology must be integrated appropriately: avoid isolated measures
- Security within Life-Cycles: e.g. secure updating

- Adapted and new Technologies are required: risk-based, tailored to individual needs

- Privacy preserving personal assistance systems are required: e.g. aggregation, anonymization

Fraunhofer AISEC

Security for I4.0: Selected German Activities

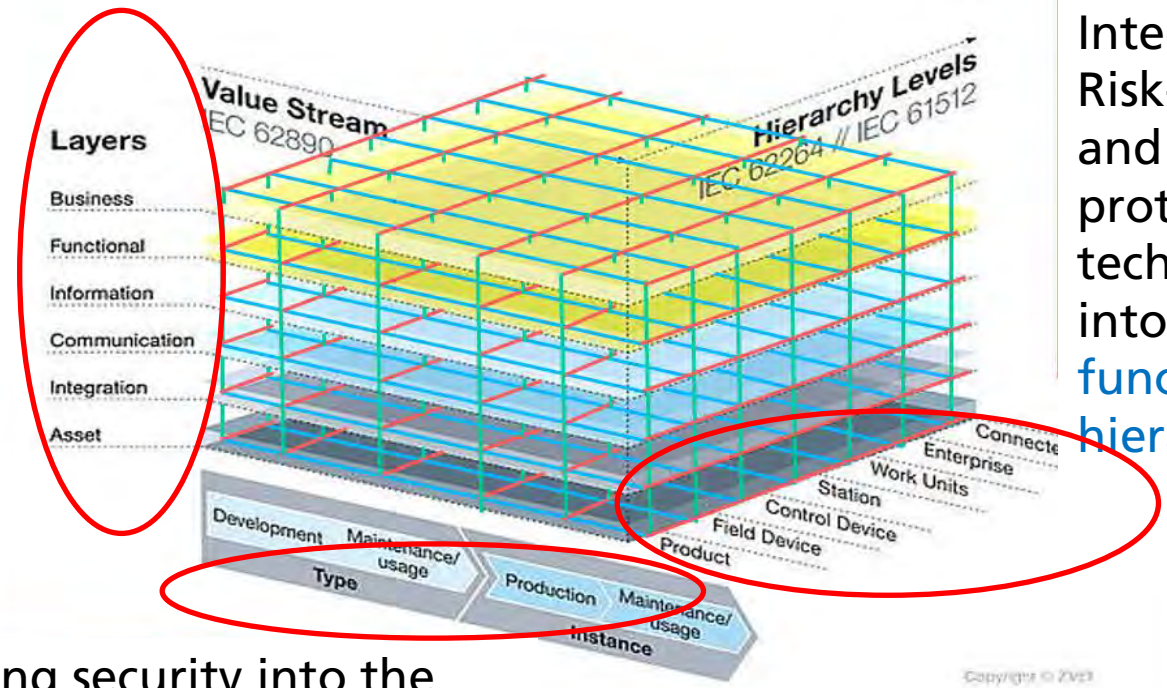
- Integrating security into RAMi4.0 models
- Addressing major R&D challenges: joint forces

  Academia, Security Industry, Application Industry (e.g. OEMs)
- Developing reference architectures, appropriate technology, best practices and guide-lines for SMEs


Integrating Security into RAMI4.0

Towards a holistic approach

Integrating security into each layer



Integrating Risk-Analysis and data protection technologies into the functional hierarchy

Integrating security into the product lifecycle (value stream)

Example: Security within the different layers
R&D Challenges

Business Layer : e.g.

- Transaction Integrity: across value chains

Functional Layer: e.g.

- Identity Management: cross domain

Information Layer: e.g.

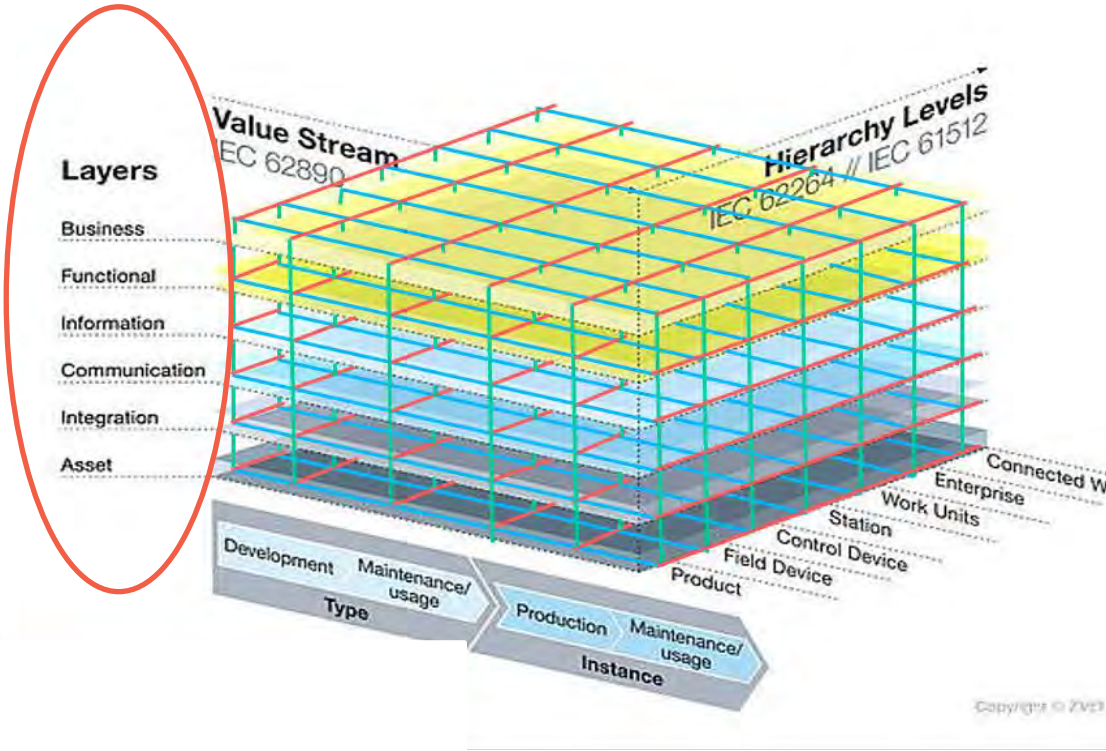
- Data Ownership

Integration Layer: e.g.

- Indrusion Detection

Asset-Layer:

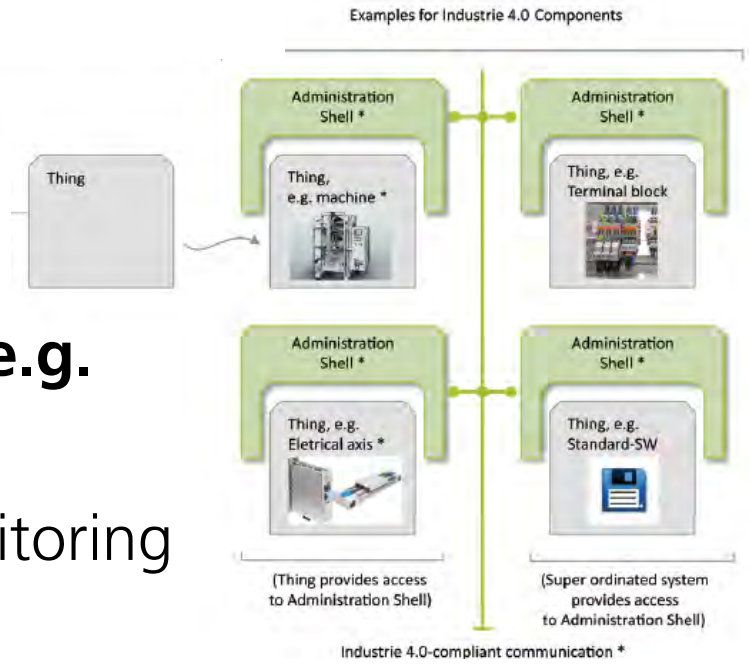
- Object identities,
- Secure communication



Assets: Security for I4.0 Components

I4.0 Component

- Unified model to describe assets (sensor, machine, plant)
- Asset enriched with administration shell
  - Virtual representation of the real asset



Security for I40 Components:

- Protecting physical object
- Protecting administration shells

Means to protect physical objects: e.g.

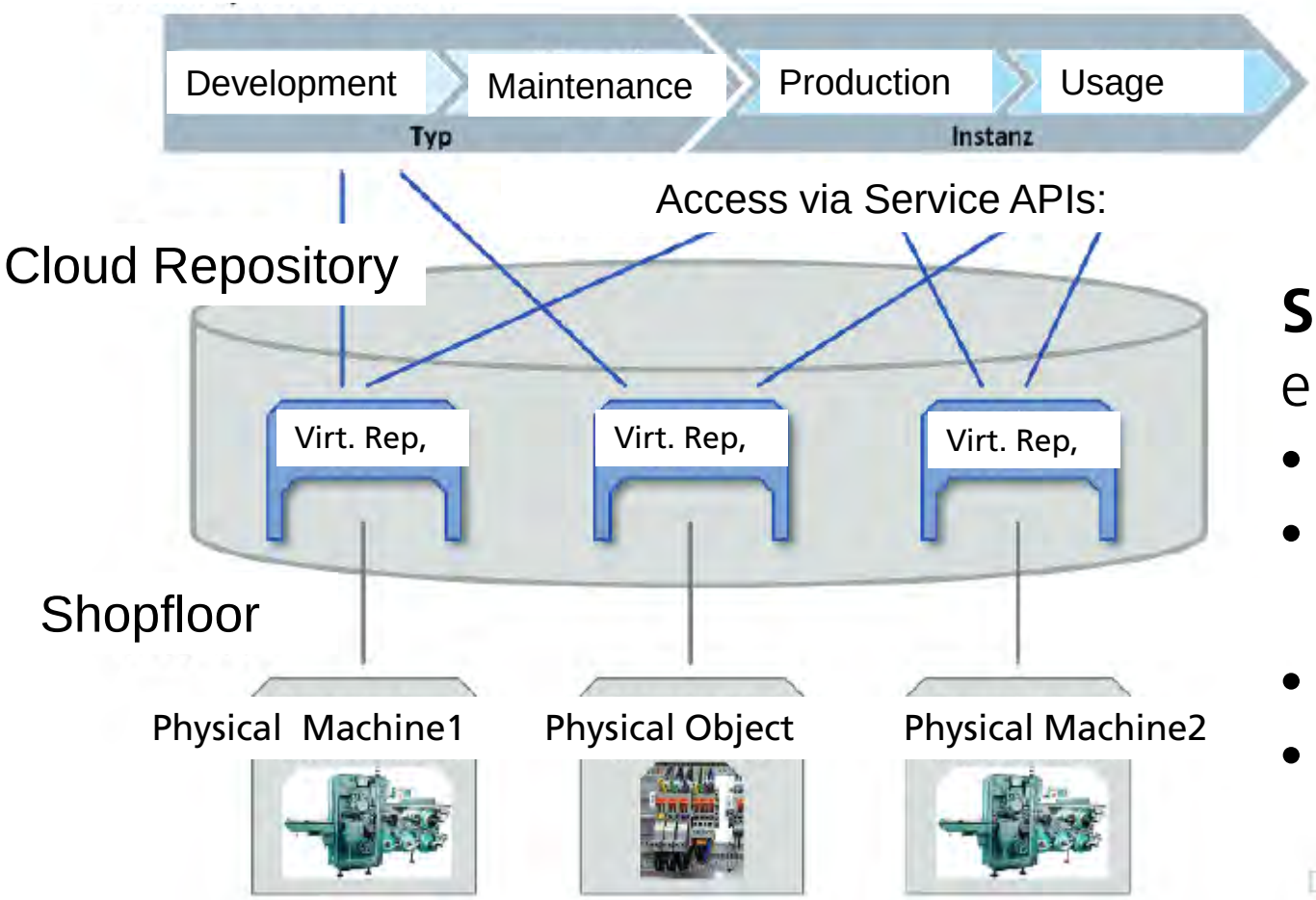
- Increase attack resilience:

  Hardening (e.g. security chips), monitoring
- Security and privacy by design

  Object Identity, Know-how protection, encryption, …

Security for I4.0 Components (cont.)

- Protecting administration shells: e.g.
  Secure Cloud-based collaboration, cross-domain:



Security Services: e.g.

- Usage control
- Continuous certification
- Accounting
- Anomaly detection and reaction

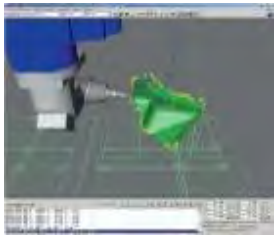
IUNO National Reference Project

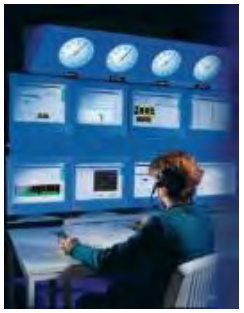
Security in Industrie 4.0

BMBF funded, 21 Partners: Industrie, Academia, 2015 - 2018

IUNO Planned Contributions

- Toolbox with new and adapted technology:
  - Secure Hardware-Token, Object Identity & Management, Access control, Anomaly Detection, Know-how Protection
- Security Engineering Methods:
  - Risk and Threat Assessments with tool supprt
- Best Practices: e.g. supporting migration paths for SMEs
  - Use-Cases, Guide-Lines, Blue Prints
- Demonstrators (with industrial leads)
  - Trustworthy data market place (Trumpf)
  - Secure remote updates (Bosch)
  - Security control center for OT (VW)





Take home Message

Fraunhofer AISEC

Industrie 4.0, Digital Transformation:

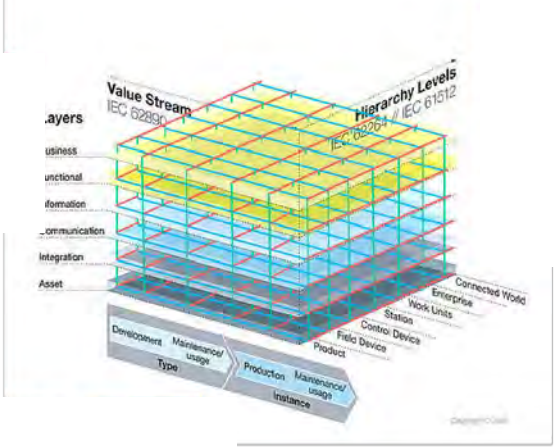
- Open, connected, cross enterprise boundaries

New dependencies & attack surfaces occur:

- Office-IT and Industrial IT and embedded IT and physical objects
- IT-Security flaws impair Safety

Holistic Approach to IT-Security for Industrie 4.0 is key!

- Security in RAMI4.0: Standardization
- Technology and Method Toolboxes
  - Trustworthy security technology
  - Best practices, use-cases, blue prints
- Testbeds, Demonstrators



Thank you for your attention

Claudia Eckert

TU München, Lehrstuhl für Sicherheit in der Informatik

Fraunhofer-Institut AISEC, München

E-Mail: claudia.eckert@sec.in.tum.de

Internet: http://www.sec.in.tum.de

http://www.aisec.fraunhofer.de

Twitter: @FraunhoferAISEC