Choose certainty.
Add value.

Certification according to IEC 62443 scheme: Burden or added value?

RSA 2016, San Francisco

Dr. Thomas Störtkuhl

TÜV SÜD

29th of February 2016

Agenda

Rail

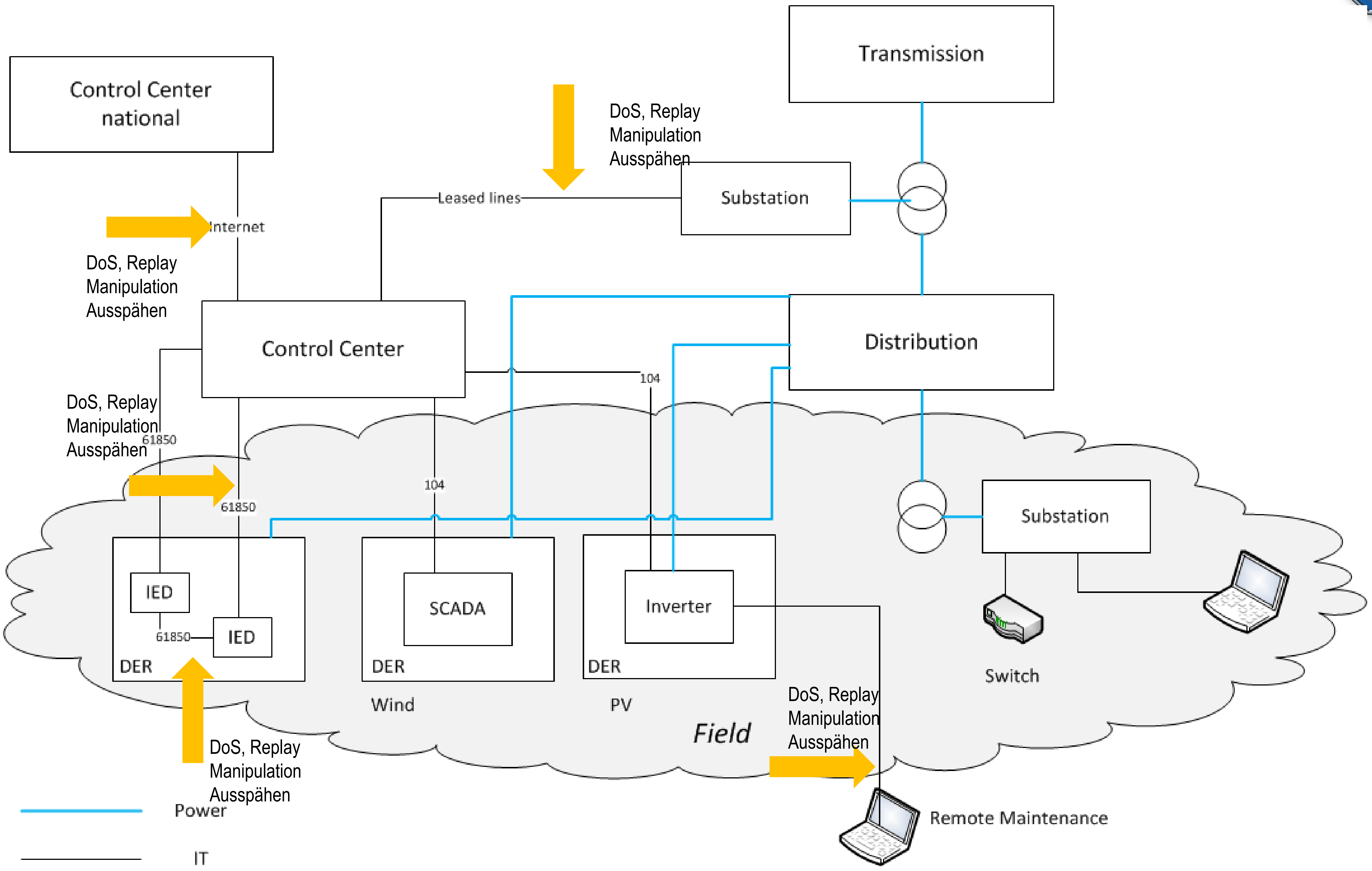
1 Examples of critical infrastructures

2 Concepts of IEC 62443

3 IEC 62443 Certifications

4 Summary

Ganzheitlicher Ansatz



Agenda

Rail

1 Examples of critical infrastructures

2 Concepts of IEC 62443

3 IEC 62443 Certifications

4 Summary

IEC 62443: Overview

IEC 62443

Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Terminology, concepts and models	**2-1** Requirements for an IACS security management system	**3-1** Security technologies for IACS	**4-1** Secure Product Development Lifecycle Requirements
1-2 Master glossary of terms and abbreviations	**2-2** Implementation guidance for an IACS security management system	**3-2** Security Risk Assessment and System Design	**4-2** Technical security requirements for IACS components
1-3 System security compliance metrics	**2-3** Patch management in the IACS environment	**3-3** System security requirements and security levels	
1-4 IACS security lifecycle and use-case	**2-4** Security program requirements for IACS service providers		

🟨 Published Versions

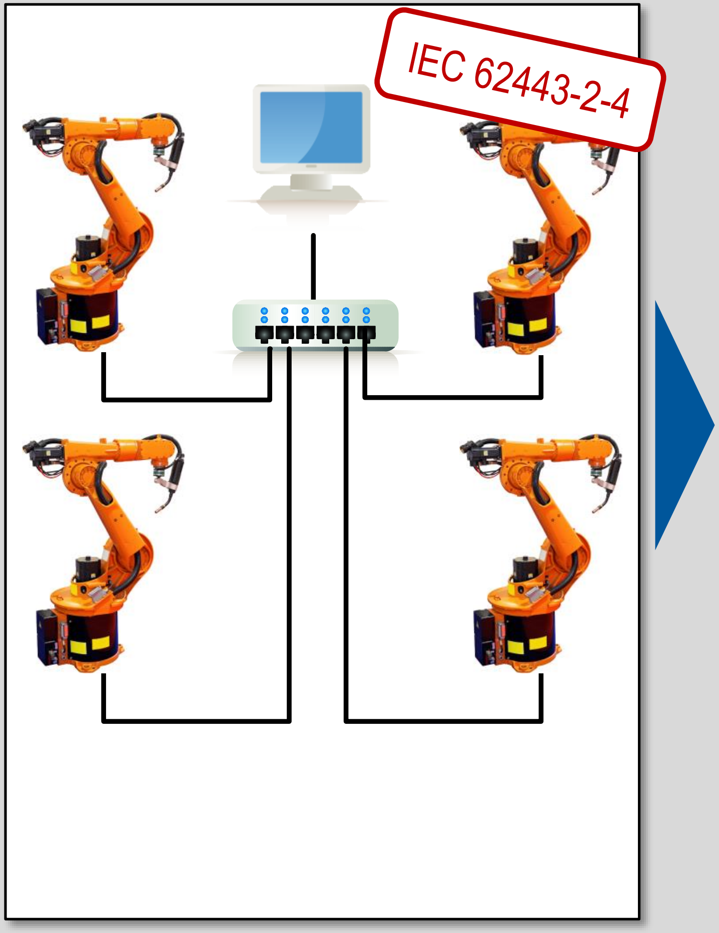
Scope of IEC 62443: Example (Manufacturing Industry)

Asset Owner

IACS (System)

System Integrator

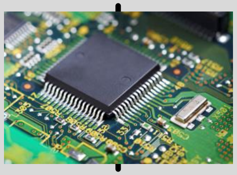
Automation Solution



Product Supplier

Control System / Product

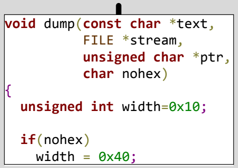
Consisting of



HW

and / or

SW

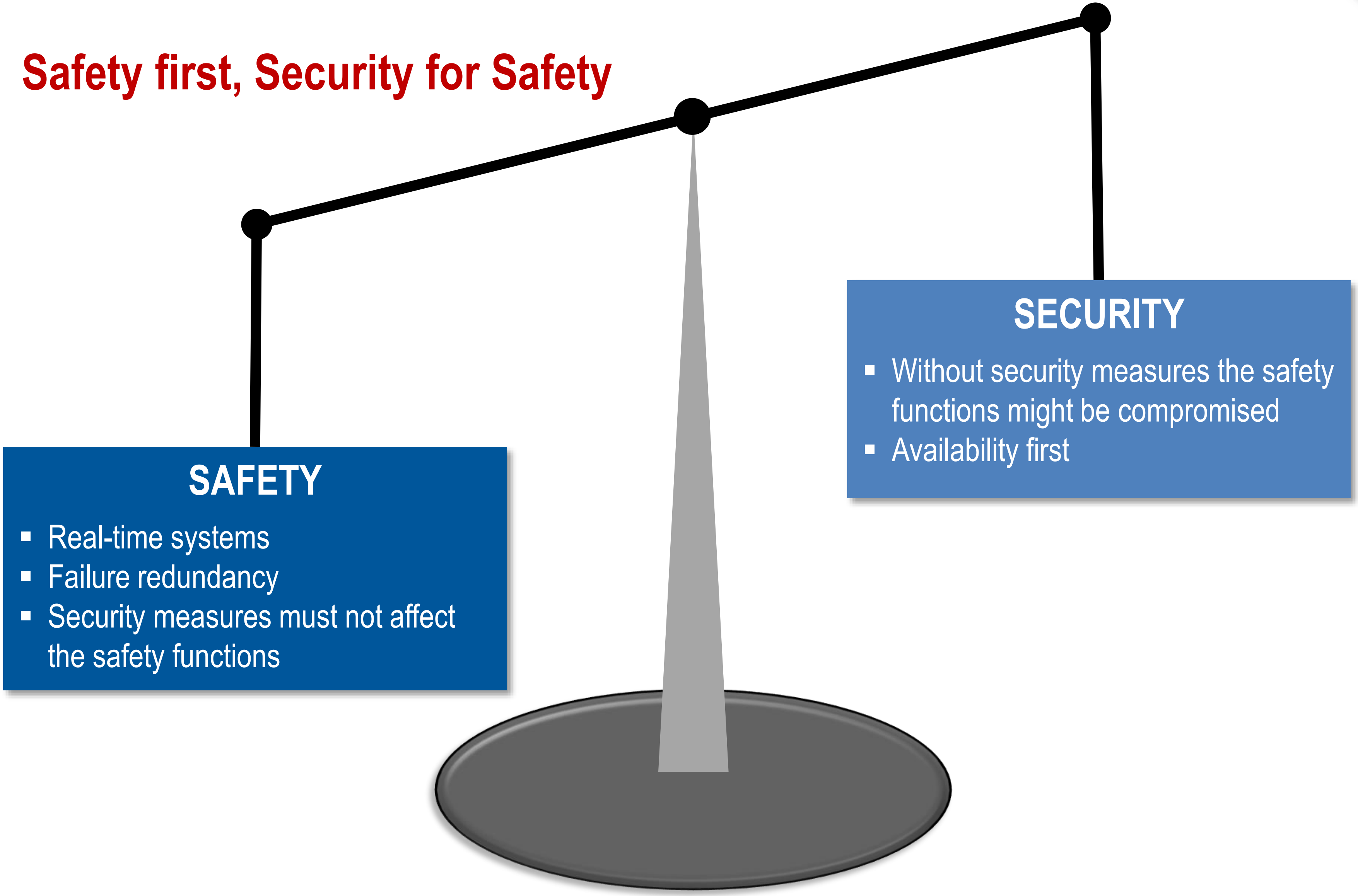


```
void dump(const char *text,
          FILE *stream,
          unsigned char *ptr,
          char nohex)
{
  unsigned int width=0x10;

  if(nohex)
    width = 0x40;
```

First rules for Industrial IT Security

Safety first, Security for Safety



SAFETY

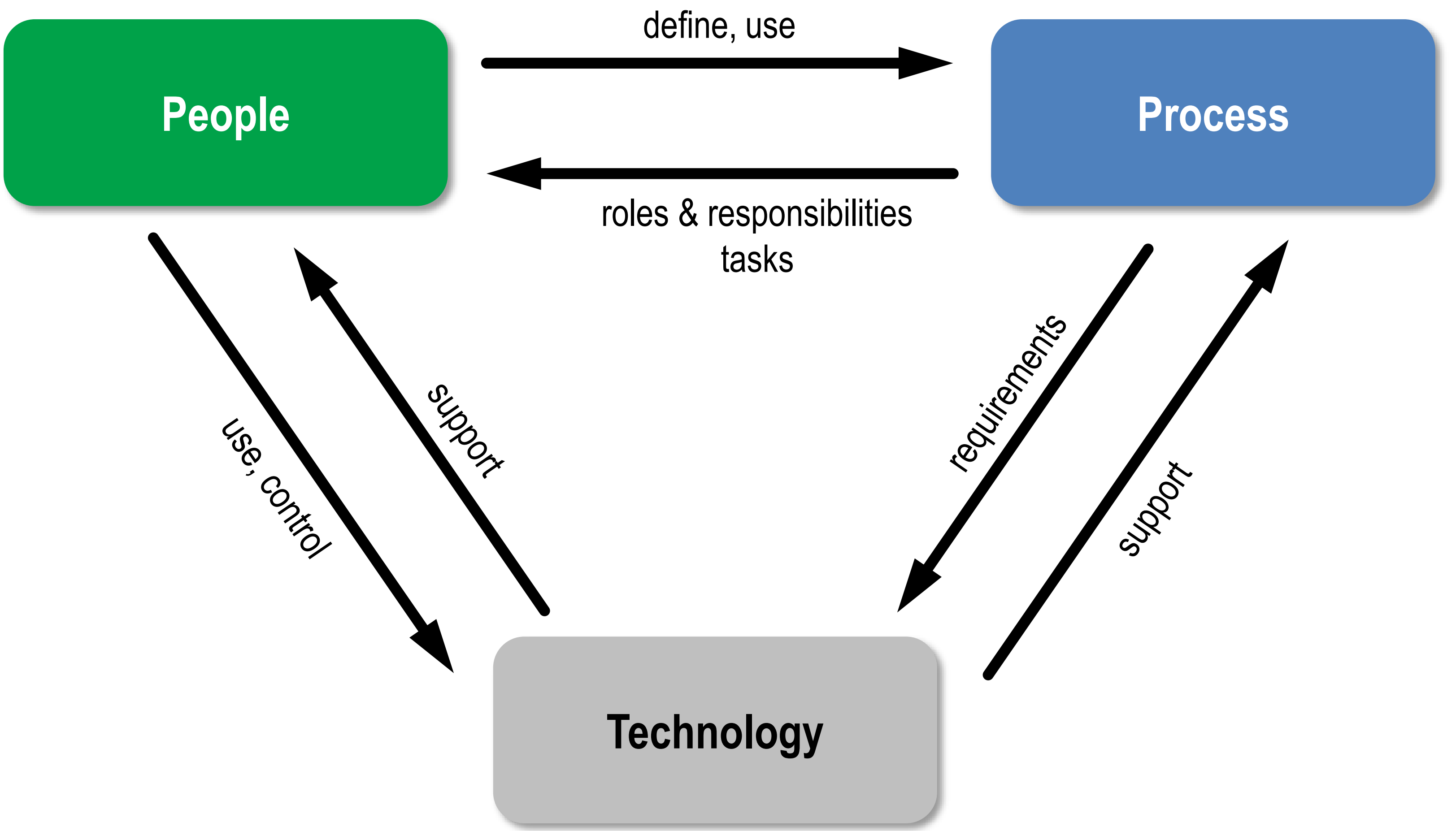
- Real-time systems
- Failure redundancy
- Security measures must not affect the safety functions

SECURITY

- Without security measures the safety functions might be compromised
- Availability first

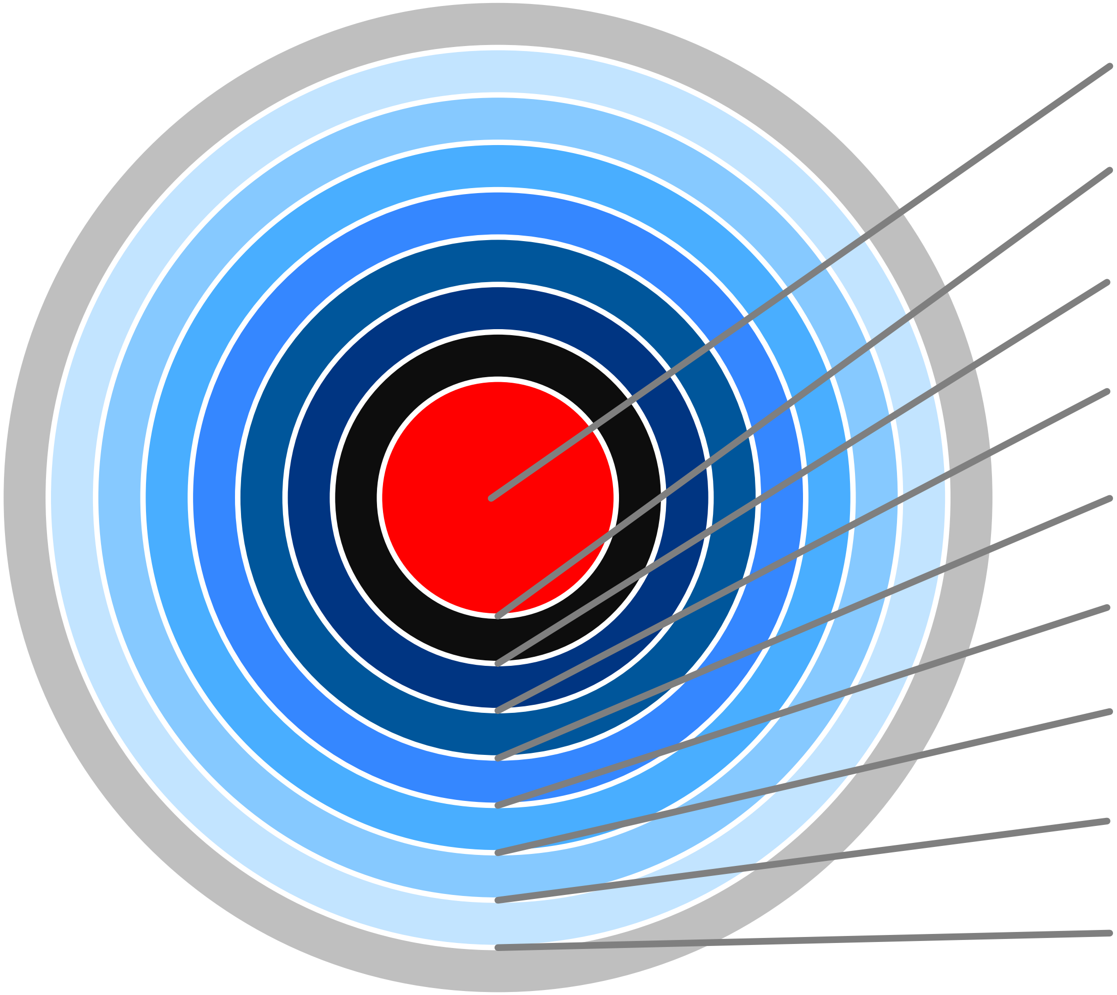
People, Process, Technology

Rail



Defense-in-Depth

Rail



Data Center / Store

Control Center

Access Control

Shop Floor

Access Control

Sensors

Doors / Windows

CCTV

Fence

General Concepts of IEC 62443: Zones & Conduits

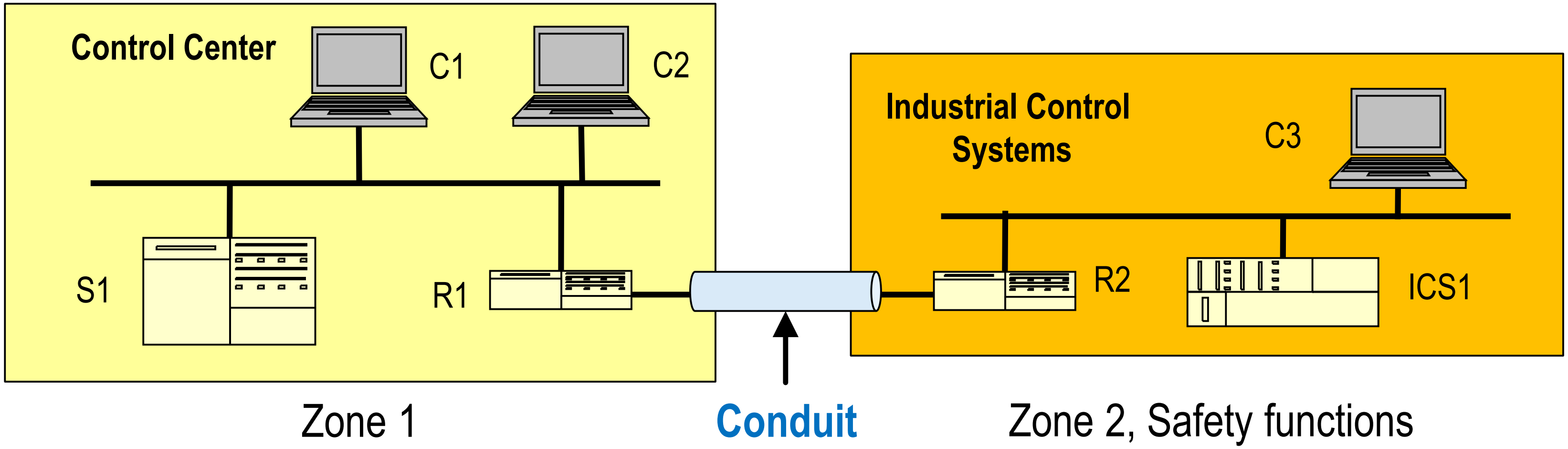
Rail

Zone

- *“Collection of entities that represents partitioning of a System under Consideration on the basis of their functional, logical and physical (including location) relationship.”*
- *“Grouping of logical or physical assets that share common security requirements.”*
- Within a zone the same protection level regarding availability, integrity, confidentiality and safety applies
- Data flow is not restricted

Conduit

- *“Logical grouping of communication channels, between connecting two or more zones, that share common security requirements.”*
- Data flow is restricted



Agenda

Rail

1 Examples of critical infrastructures

2 Concepts of IEC 62443

3 IEC 62443 Certifications

4 Summary

Standards for TÜV SÜD Automation Solution Certification

IEC 62443

Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Terminology, concepts and models	**2-1** Requirements for an IACS security management system	**3-1** Security technologies for IACS	**4-1** Secure Product Development Lifecycle Requirements
1-2 Master glossary of terms and abbreviations	**2-2** Implementation guidance for an IACS security management system	🟩 **3-2** Security Risk Assessment and System Design	**4-2** Technical security requirements for IACS components
1-3 System security compliance metrics	**2-3** Patch management in the IACS environment	🟩 **3-3** System security requirements and security levels	
1-4 IACS security lifecycle and use-case	🟩 **2-4** Security program requirements for IACS service providers		

🟩 Basis for Certification

Standards for TÜV SÜD Product / Component Certification

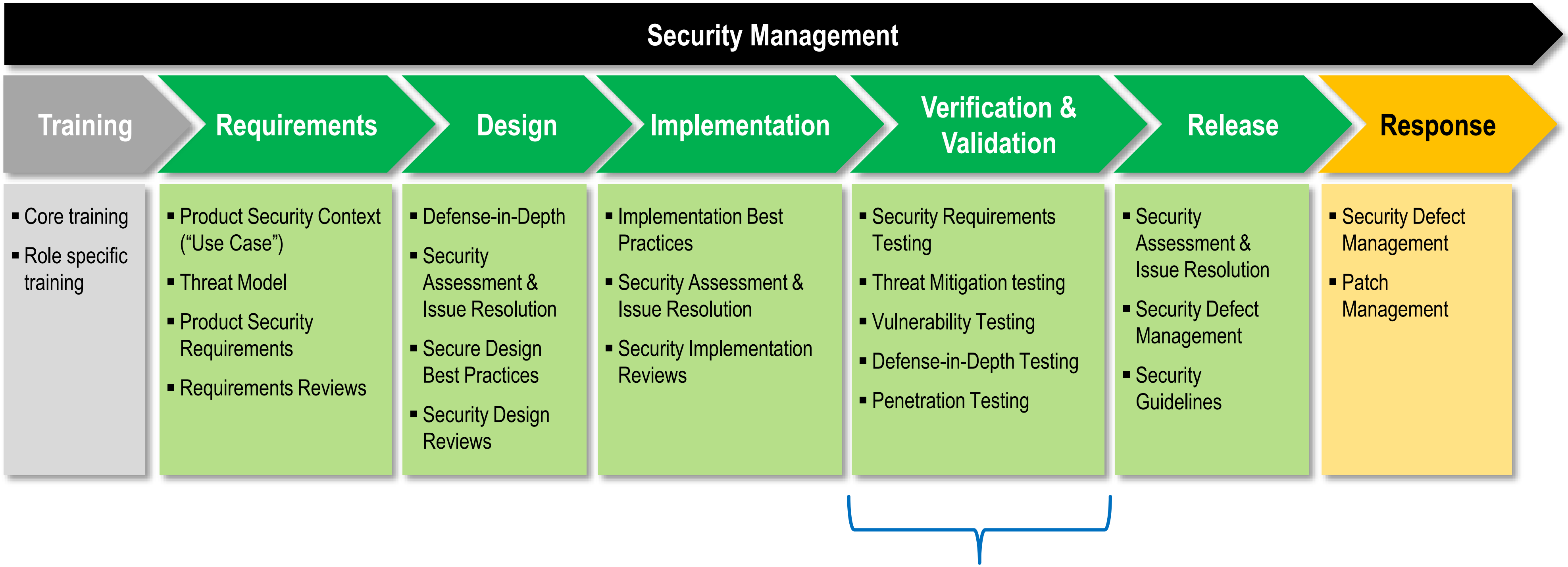
IEC 62443

Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component / Product
1-1 Terminology, concepts and models	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS	🟩 4-1 Secure Product Development Lifecycle Requirements
1-2 Master glossary of terms and abbreviations	2-2 Implementation guidance for an IACS security management system	3-2 Security Risk Assessment and System Design	4-2 Technical security requirements for IACS components
1-3 System security compliance metrics	2-3 Patch management in the IACS environment	🟩 3-3 System security requirements and security levels	
1-4 IACS security lifecycle and use-case	2-4 Security program requirements for IACS service providers		

🟩 Basis for Certification

IEC 62443-4-1: Secure Product Development Lifecycle (SPDL)



Security Management

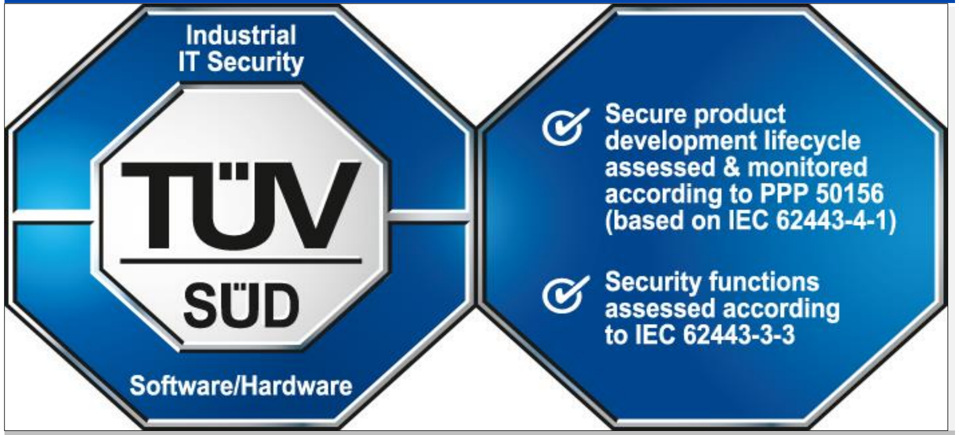
Training	Requirements	Design	Implementation	Verification & Validation	Release	Response
- Core training - Role specific training	- Product Security Context ("Use Case") - Threat Model - Product Security Requirements - Requirements Reviews	- Defense-in-Depth - Security Assessment & Issue Resolution - Secure Design Best Practices - Security Design Reviews	- Implementation Best Practices - Security Assessment & Issue Resolution - Security Implementation Reviews	- Security Requirements Testing - Threat Mitigation testing - Vulnerability Testing - Defense-in-Depth Testing - Penetration Testing	- Security Assessment & Issue Resolution - Security Defect Management - Security Guidelines	- Security Defect Management - Patch Management

V&V activities need to be conducted throughout the development lifecycle!

TÜV SÜD certificates for Industrial IT Security

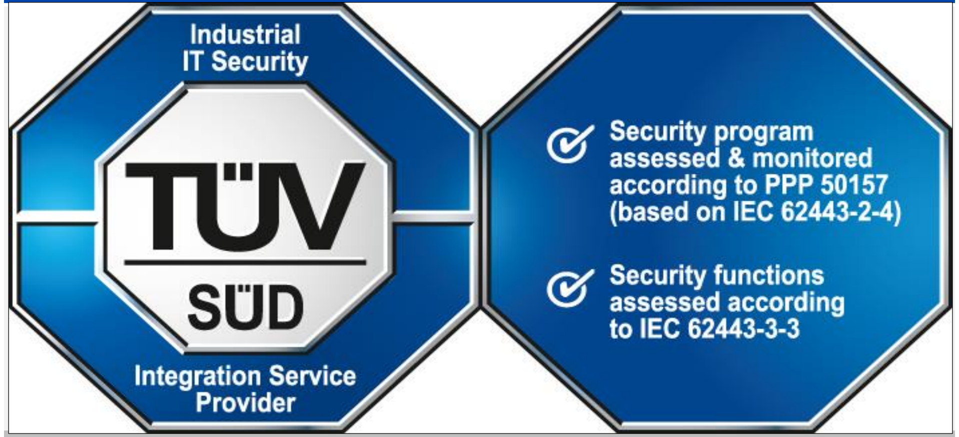
Rail

Product supplier


Industrial
IT Security
TÜV
SÜD
Software/Hardware
Secure product development lifecycle assessed & monitored according to PPP 50156 (based on IEC 62443-4-1)
Security functions assessed according to IEC 62443-3-3

- Assessment of development process on the basis of IEC 62443-4-1
- Assessment of SL of security functions on the basis of IEC 62443-3-3

System Integrator


Industrial
IT Security
TÜV
SÜD
Integration Service
Provider
Security program assessed & monitored according to PPP 50157 (based on IEC 62443-2-4)
Security functions assessed according to IEC 62443-3-3

- Assessment of solution development process on the basis of IEC 62443-2-4
- Assessment of SL of security functions on the basis of IEC 62443-3-3 (reference architecture)

Agenda

Rail

1 Examples of critical infrastructures

2 Concepts of IEC 62443

3 IEC 62443 Certifications

4 Summary

Summary

DIN VDE V 0831-104 and IEC 62443 is useful

- Risk based ✓
- Process oriented ✓
- Combination with other standards possible ✓
- Requirements defined ✓

→

- **Basis for assessment and certification**
- **Best Practice approach**

Contact

Rail

Thank you for your attention!

Dr. Thomas Störtkuhl
thomas.stoertkuhl@tuev-sued.de

Phone: +49 89 5791-1930
Fax: +49 89 5791-2933
Mobile: +49 151 2764 5644

TÜV SÜD Rail GmbH
Barthstr. 16
80339 München

www.tuev-sued.com