TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT-Workshop "Industrial Security" 2015

München, 11.06.2015

Einführung Industrial Security anhand des IEC 62443; Bedrohungslage für Betreiber von ICS (Industrial Control System)

Dr. Thomas Störtkuhl
TÜV SÜD

Choose certainty.
Add value.

Rail

Einführung Industrial Security anhand des IEC 62443; Bedrohungslage für Betreiber von ICS (Industrial Control System)

TeleTrusT-Workshop "Industrial Security"

Dr. Thomas Störtkuhl
Teamleiter Industrial IT Security
TÜV SÜD Rail GmbH

11. Juni 2015

Agenda

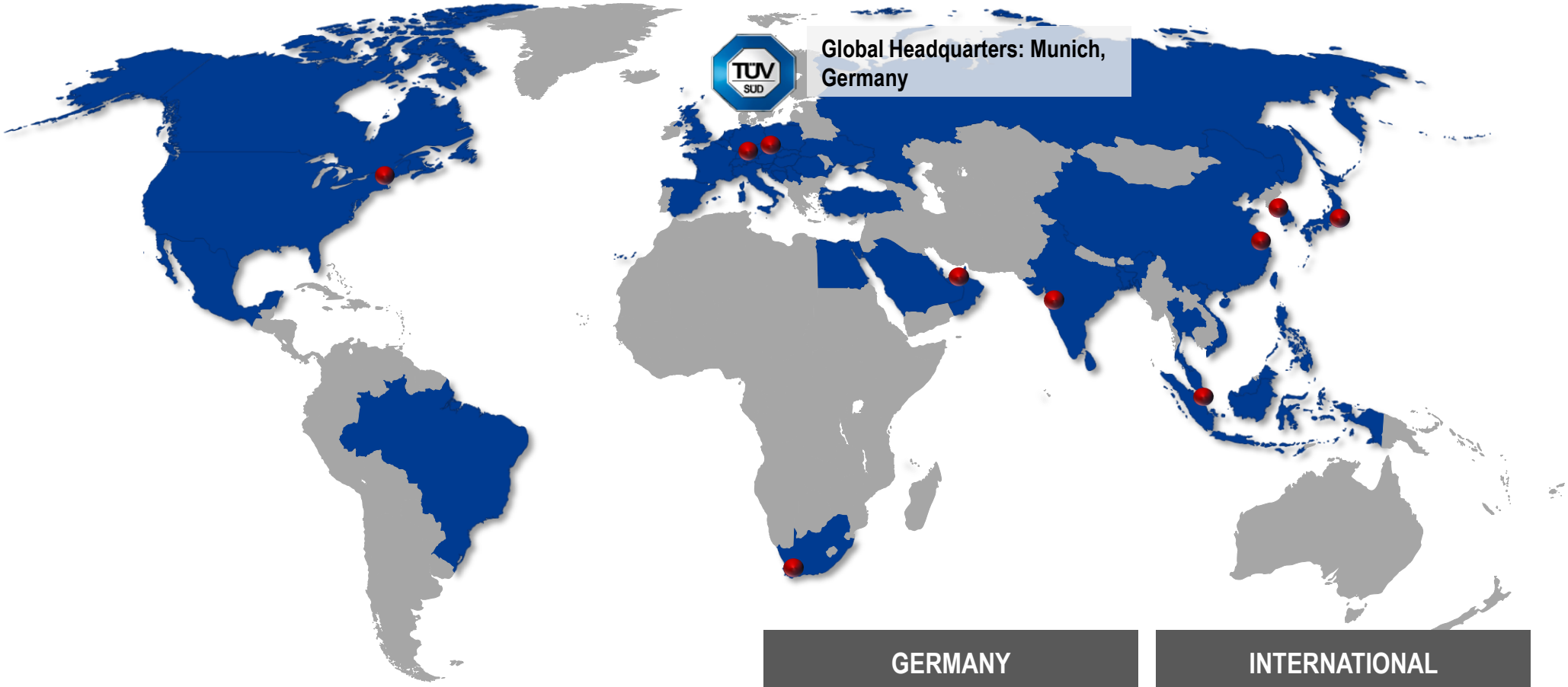
1. Introduction Industrial IT Security Team
2. Security: Status quo
3. Introduction to IEC 62443
4. Best practices and concepts
5. Summary

TÜV SÜD in numbers: Growing from strength to strength

1	One-stop technical solution provider
150	years of experience
800	locations worldwide
1,800	million Euro in sales revenue 2012
18,800	employees worldwide

TÜV SÜD: Global expertise. Local experience.

Rail



Legend:

- Countries with TÜV SÜD offices
- Regional headquarters

GERMANY	INTERNATIONAL
Revenue: Euro 1,100 mio Headcount: 9,900 staff	Revenue: Euro 580 mio Headcount: 7,300 staff

TÜV SÜD's Business Unit Rail: a Partner for homologation bodies

1 one-stop technical solution provider

50 years of experience

28 locations worldwide

500 employees worldwide

TÜV SÜD Rail: End-to-end solutions across all rail sectors

Rail

RAIL PROJECT LIFECYCLE

PLANNING → DESIGN → INSTALLATION → TESTING → COMMISSIONING → OPERATION → DE-COMMISSIONING

RAIL SECTOR

CONVENTIONAL

HIGH SPEED

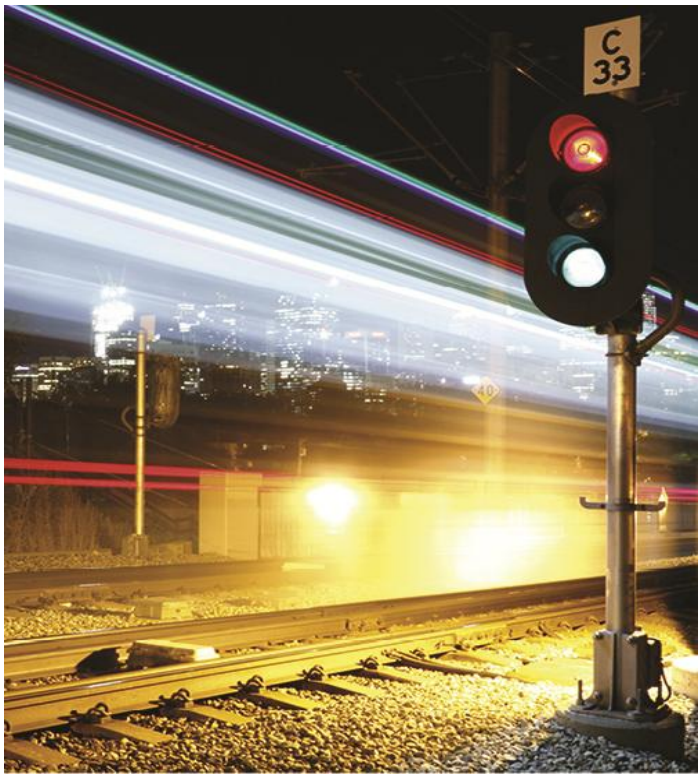
METRO

LIGHT RAIL

TÜV SÜD Rail: Delivering value-added solutions and expertise

Rail

	ENGINEERING SERVICES	CONSULTING SERVICES	TESTING SERVICES	ISA & CERTIFICATION SERVICES	TRAINING SERVICES
INFRASTRUCTURE					
▪ Understructure	●	●	●	●	
▪ Superstructure					
▪ Civil works & tunnels					
ELECTRICAL AND MECHANICAL (E&M) SYSTEMS					
▪ Signalling & telecom	●	●	●	●	
▪ Rail power supply					
▪ Catenary					
ROLLING STOCK					
▪ High speed	●	●	●	●	
▪ Conventional rail					
▪ Light rail/Metro					
GENERIC SAFETY SYSTEM					
▪ Programmable electronics	●	●	●	●	
▪ Safety components					
▪ Rail automation (HW, SW)					
▪ Industrial IT Security					



Agenda

1. Introduction Industrial IT Security Team
2. **Security: Status quo**
3. Introduction to IEC 62443
4. Best practices and concepts
5. Summary

Current security incidents …

Rail

DIE WELT

DIGITAL VERNETZTE PRODUKTION 15.10.13

Industrie ist gegen Hacker schlecht gerüstet

Bedrohung für die Industrie: Durch die Vernetzung von Maschinen wird die Produktion zunehmend ein Sicherheitsrisiko. Derzeit eingesetzte Software hilft kaum gegen die künftigen Angriffe.

FORBES 7/24/2013 @ 9:00AM | 523.286 views

Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)

This story appears in the August 12, 2013 issue of Forbes.

Süddeutsche.de

24. Februar 2013, 10:14 Medienbericht über Cyber-Attacken

Chinesische Hacker greifen EADS und ThyssenKrupp an

Deutsche Konzerne werden einem Medienbericht zufolge immer öfter von chinesischen Hackern angegriffen. Und auch die Bundesregierung wurde demnach im vergangenen Jahr von ausländischen Nachrichtendiensten attackiert - mehr als tausend Mal.

INDUSTRIE 4.0 VDI nachrichten

Produktionsindustrie im Visier der Hacker

Von Peter Kellerhoff | 23. Januar 2015 | Ausgabe 04

Sicherheit in „Industrie 4.0" ist eine lebenswichtige Voraussetzung für Produktionsunternehmen. Viele Maschinen und Kontrollgeräte sind immer noch unzureichend geschützt. Sicherheitsanbieter bieten erste Schutzprodukte an, aber effektiver Schutz sollte in den Netzen erfolgen

heise Security News Hintergrund Tools Foren Kontakt

Security > News > 7-Tage-News > 2014 > KW 50 > Zugang über Umwege – Hacker nutzen Zulieferer als Einfallstor

09.12.2014 09:16 « Vorige | Nächste »

Zugang über Umwege – Hacker nutzen Zulieferer als Einfallstor

Täglich greifen Hacker deutsche Firmen an. Einige haben ihre Sicherheitsvorkehrungen deshalb in den vergangenen Jahren ausgeweitet. Doch die eigene Sicherheit liegt nicht mehr allein in den Händen der Unternehmen.

DIE WELT

Home Politik Wirtschaft Geld Sport Wissen Panorama Feuilleton ICON Reise PS WELT Regional Meinung Videos Markt

Wirtschaft > Digital > IT-Sicherheit: Hacker legen Hochofen von Stahlhersteller lahm

DIE WELT DIE WELT Digital 2 Monate für nur 0,99 €! Jetzt testen!

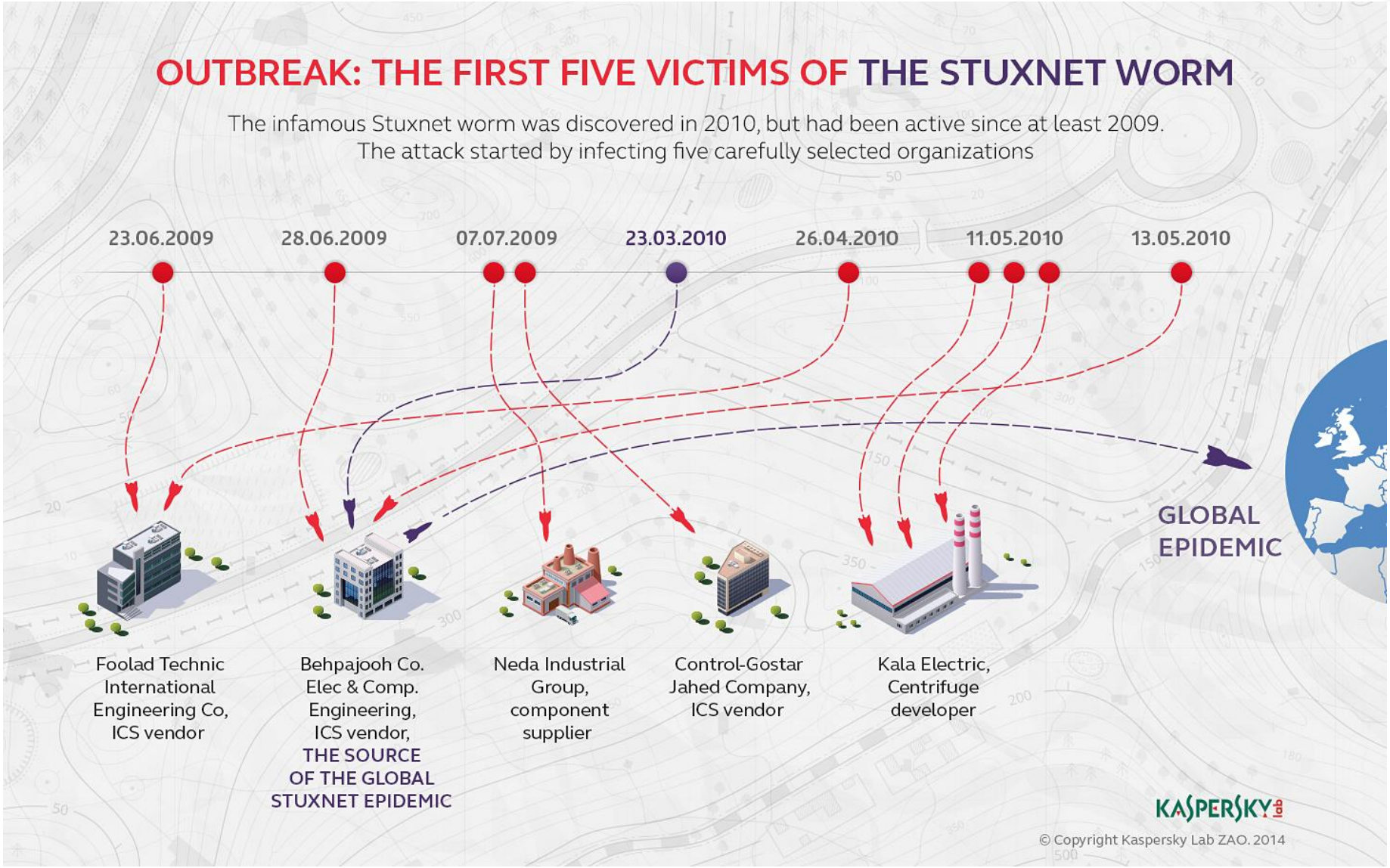
Digital PC & Notebooks Smartphones Tablet-PC Sicherheit Internet WLAN TV & Video Audio Kamera Spiele

DIGITAL IT-SICHERHEIT 18.12.14

Hacker legen Hochofen von Stahlhersteller lahm

Attacks: Stuxnet

Rail



Security Shortfalls in Industrial IT Environments

Rail

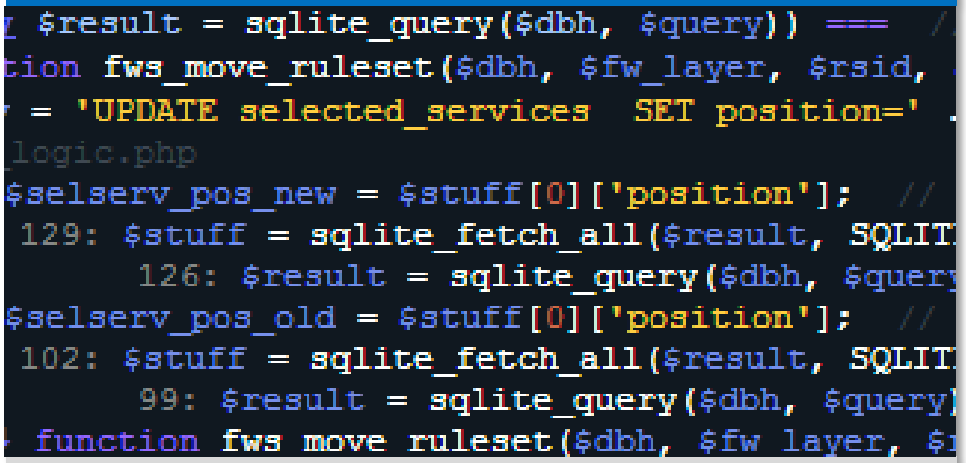
General

- Personnel without security awareness / skills
- No or only limited processes (policies, procedures, guidelines)
- Limited understanding of the information to be protected
- Risk management?
- Asset management?
- Complete overview of the network topology and communication channels are missing
- No or only a minimum of network segmentation
- Periodic IT security audits?
- Security monitoring?
- Incident handling (technology & process)?
- Patch management?

Security Shortfalls in Industrial IT Environments

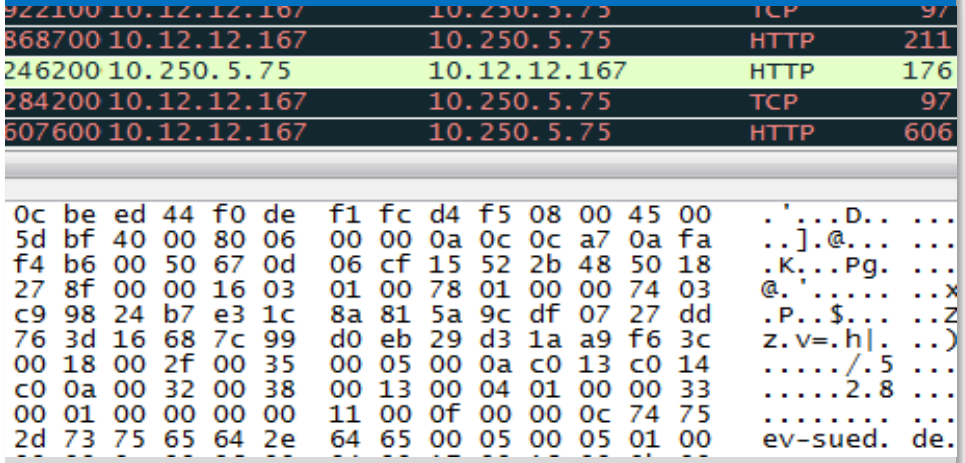
Rail

Applications



- Security is not integrated into the development process
- Security is not covered in the procurement process
- Missing Change and Configuration Management
- No security testing, incl. 3rd party software
- “Security through Obscurity”
- Incorrect implementation of cryptographic algorithms
- Possibility of attacks (DoS, Cross Site Scripting, …)

Authentication



- Default passwords
- Weak / trivial passwords
- Password in clear text
- Passwords on Post it®
- Generic password for user groups
- Root passwords are group passwords for suppliers
- No Two / Multi-Factor-Authentication

Security Shortfalls in Industrial IT Environments

Rail

Use of Engineering Workstations (EWS)

- Any accessible interfaces in the industrial IT infrastructure is used
- EWS is used in different networks for different customers
- EWS is often used as a standard computer

Remote Access & Maintenance

- Different supplier solutions are implemented and allowed
- Remote Access without dedicated DMZ
- Remote access is always enabled and therefore can be used at any time without control
- Group accounts
- Multi-factor authentication not used

Security Shortfalls in Industrial IT Environments

Rail

Protocols

```
                    Version 1.8.2-win
                http://www.titania.co.uk
          Copyright Ian Ventura-Whiting 2009
       Compiled against OpenSSL 0.9.8m 25 Feb 2010

Testing SSL server 192.168.1.1 on port 443

  Supported Server Cipher(s):
    Accepted  SSLv2   56 bits  DES-CBC-MD5
    Accepted  SSLv3   56 bits  DES-CBC-SHA
    Accepted  TLSv1   56 bits  DES-CBC-SHA

  Prefered Server Cipher(s):
```

- Unprotected communication channels
- Use of weak cipher suites
- Wireless communication without authentication and encryption
- Incorrectly implemented cryptographic algorithms

USB-Token

- No regulations for the use of USB Tokens
- Uncontrolled USB tokens are used by suppliers
- No virus scanning for USB tokens
  (not to think about “Bad USB”!)

Agenda

1. Introduction Industrial IT Security Team
2. Security: Status quo
3. **Introduction to IEC 62443**
4. Best practices and concepts
5. Summary

Holistic approach of IEC 62443

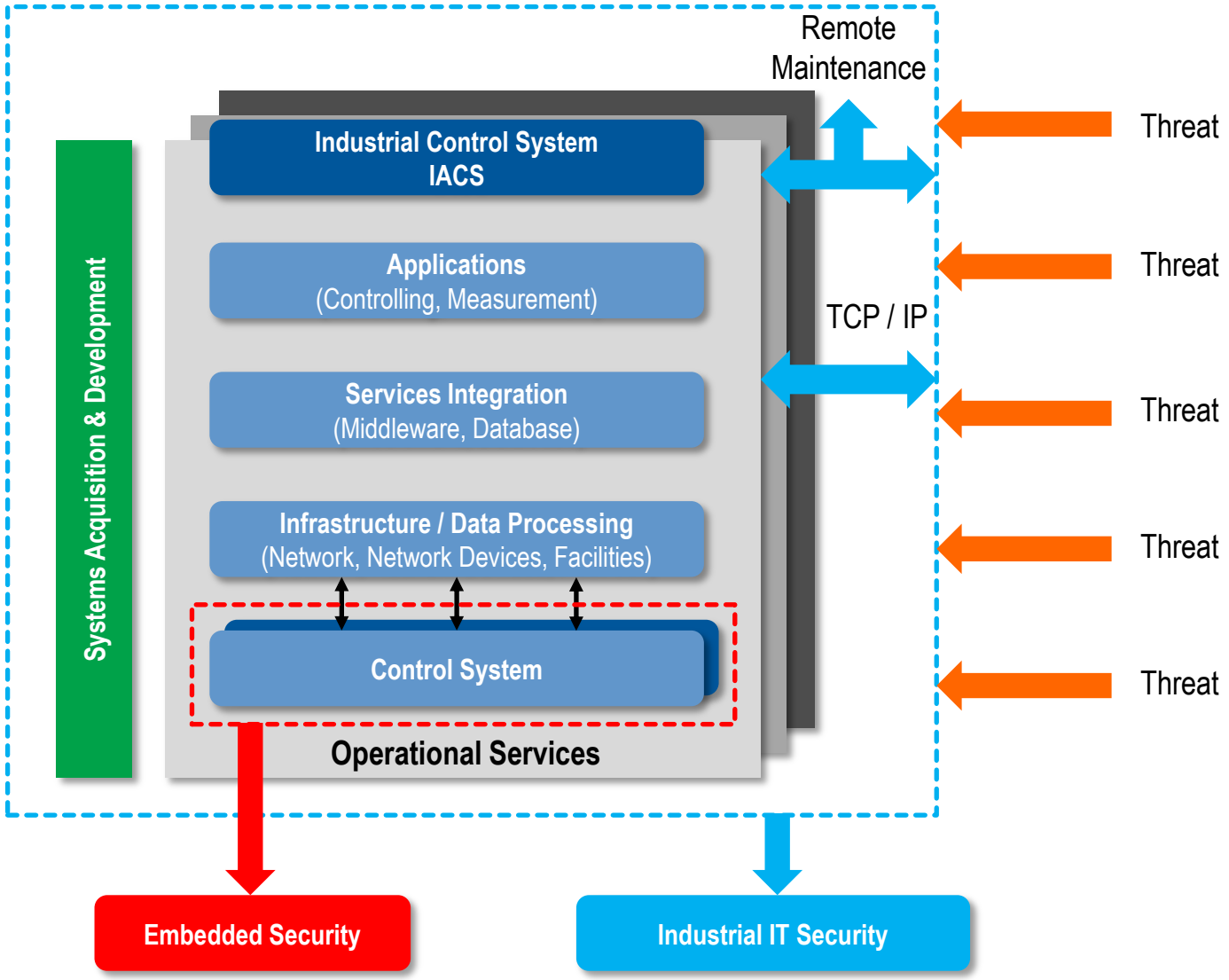
Rail

IEC 62443 Series

General	Management System	Industrial IT Security, IACS	Embedded Security, Component
1-1 Terminology, concepts and models	2-1 Establishing an IACS security program	3-1 Security technologies for IACS	4-1 Product development requirements
1-2 Master glossary of terms and abbreviations	2-2 Operating an IACS security program	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	
	2-4 Requirements for IACS solution suppliers		

Relevant documents for assessment / certification

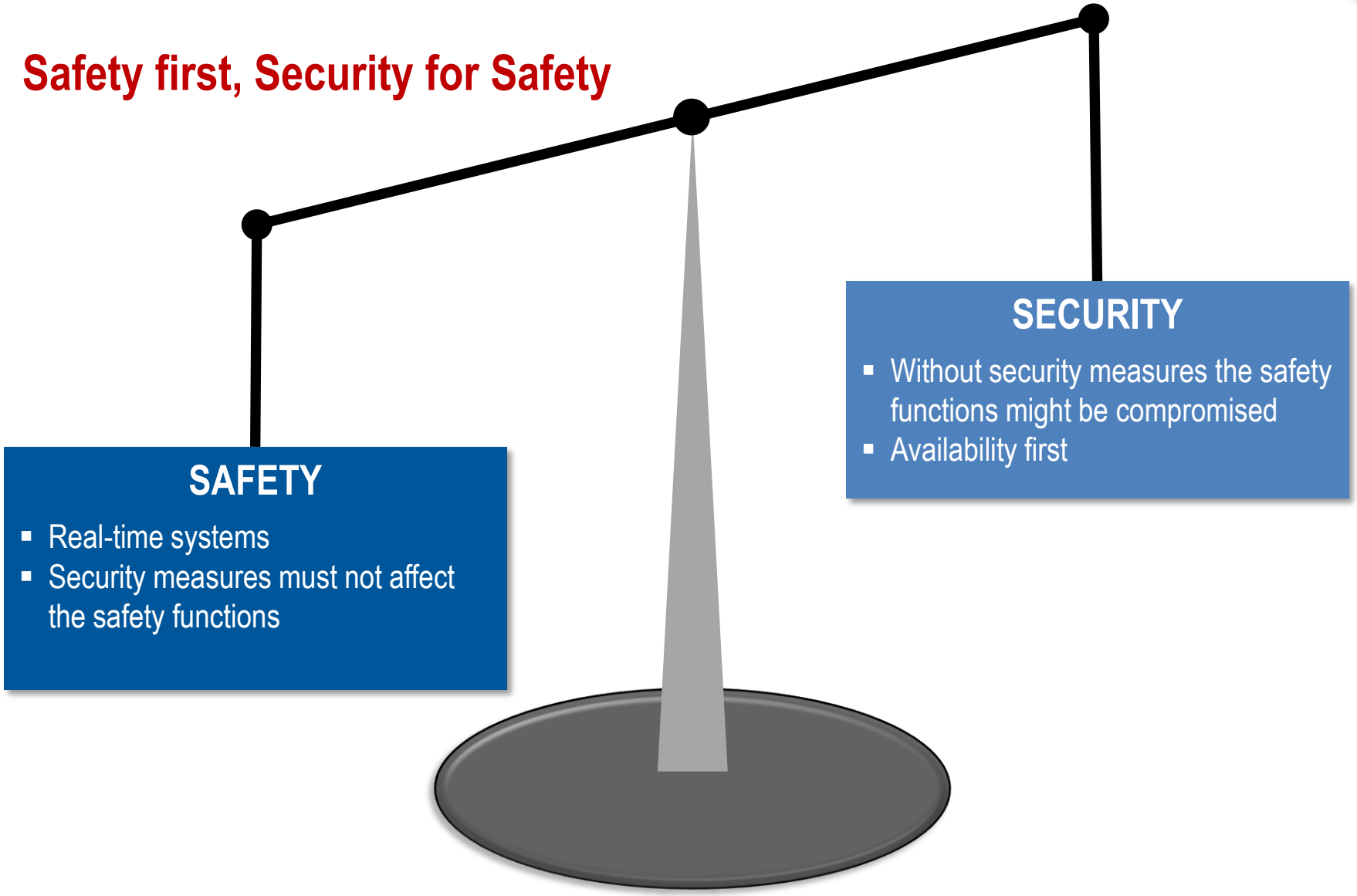
Holistic Approach



Rules for ICS (Industrail Control Systems)

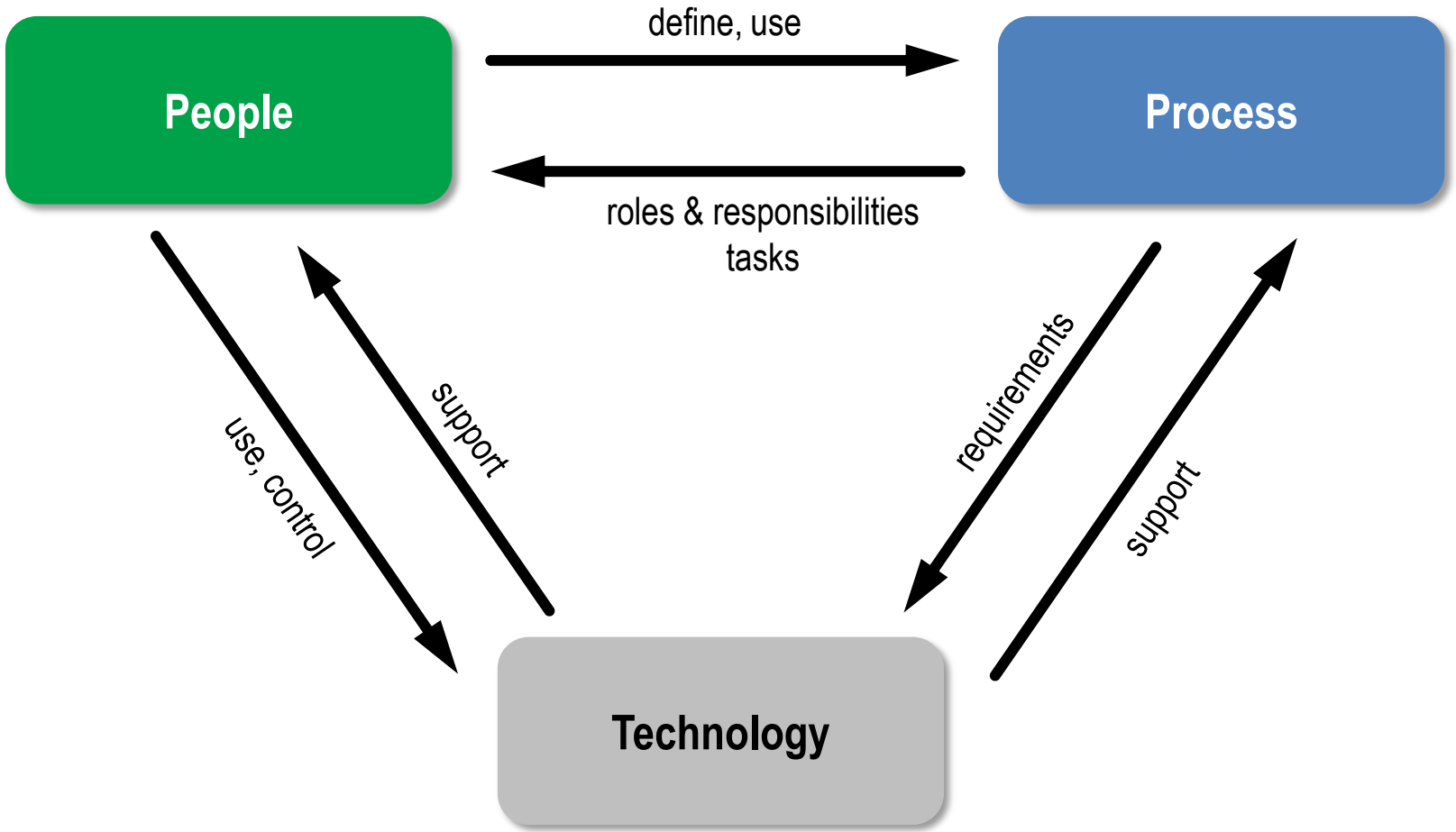
Rail

Safety first, Security for Safety

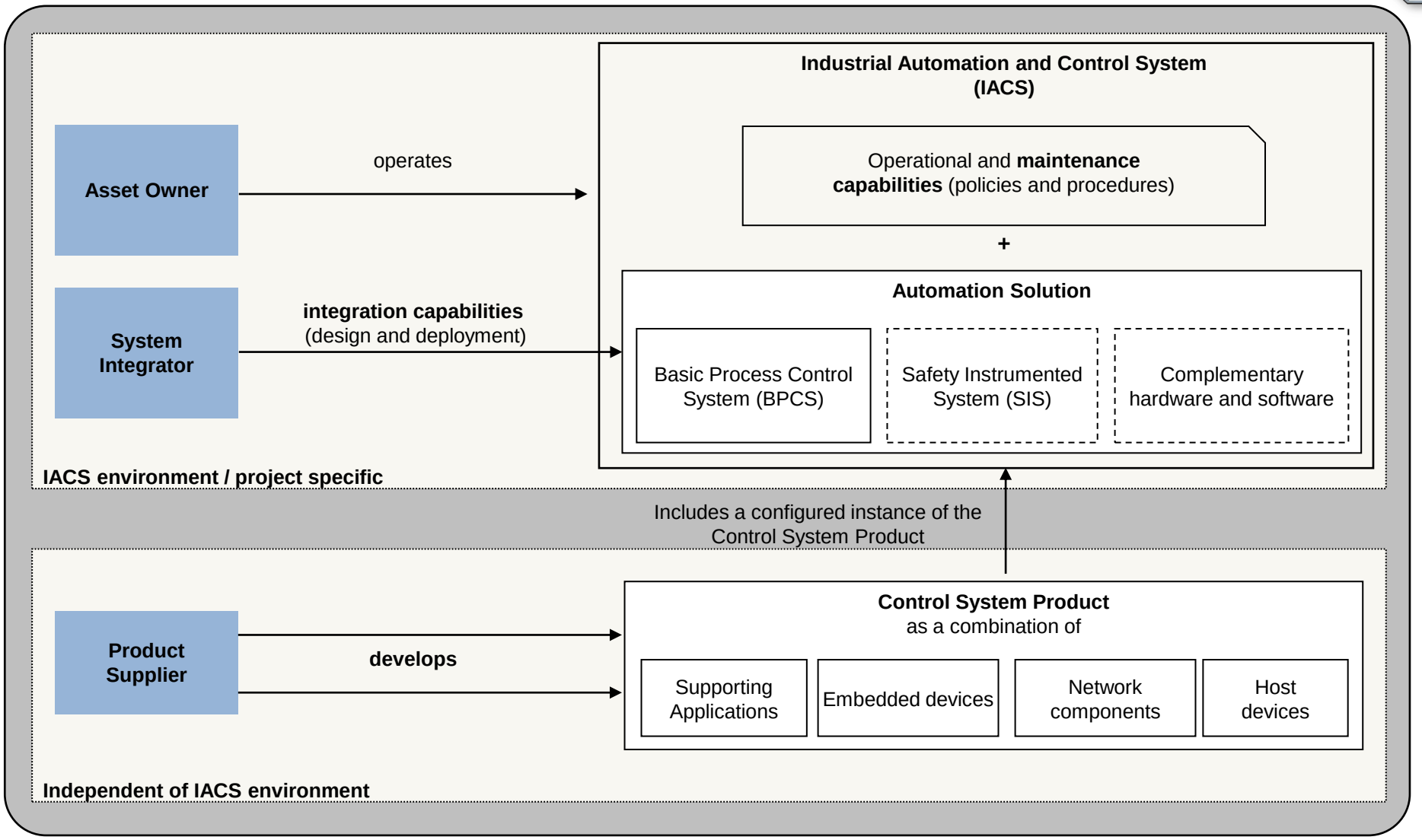


People, Process, Technology

Rail



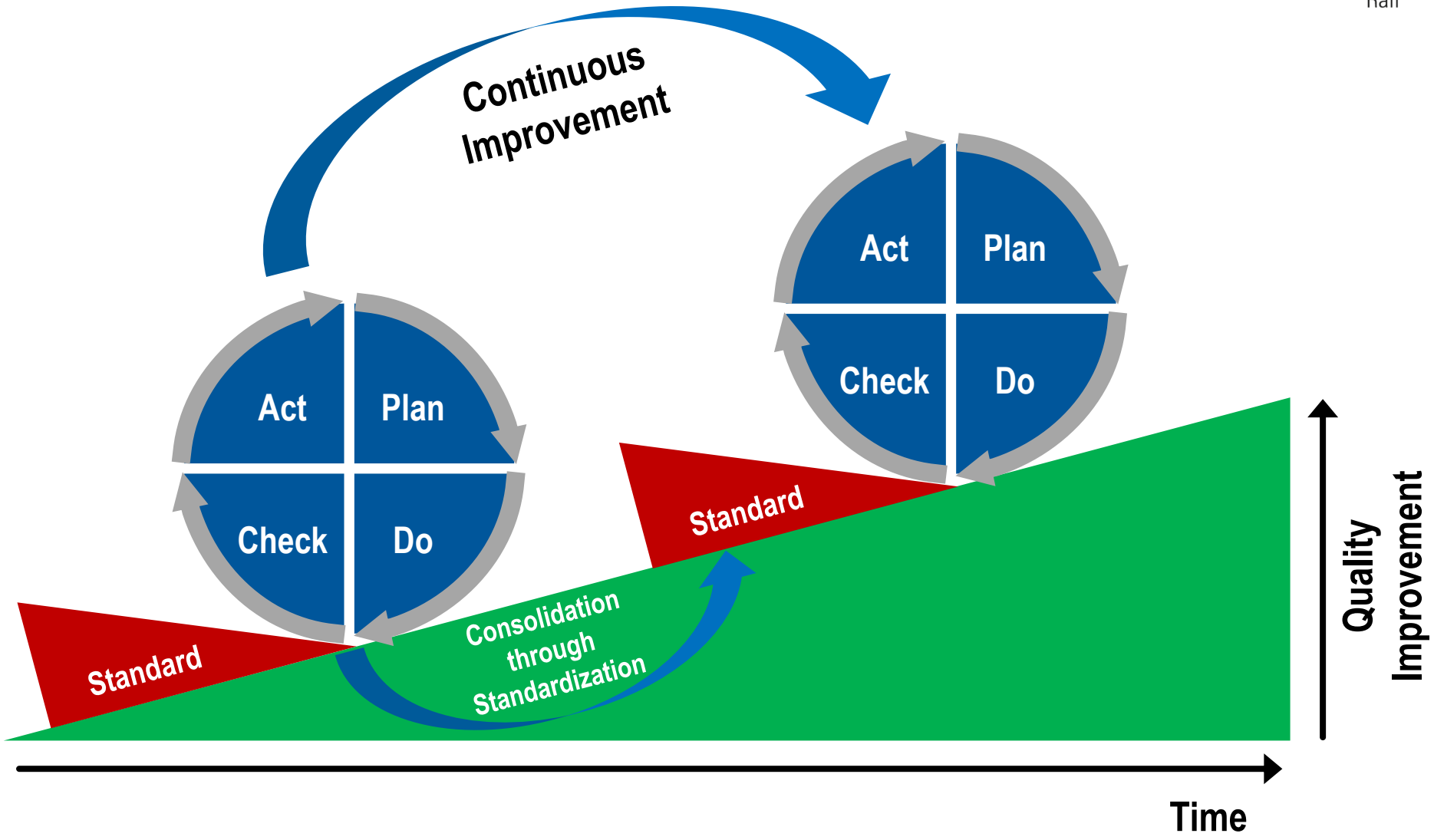
IEC 62443: Roles



Agenda

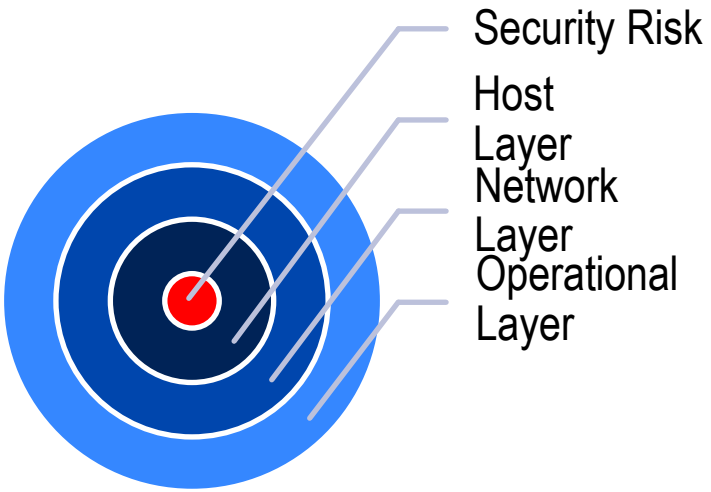
1. Introduction Industrial IT Security Team
2. Security: Status quo
3. Introduction to IEC 62443
4. **Best practices and concepts**
5. Summary

Continuous Improvement



Defense-in-depth strategy

- Security policies and guidelines
- Physical protection (physical zoning)
- Network segregation (zones and conduits)
- Need-to-Know: Restriction of access to components, systems, zones and conduits
- Minimum installation: hardening of components
- Living processes
- Skilled and trained employees



cf. Homeland Security (2009) Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies figure 5

Zones & Conduits

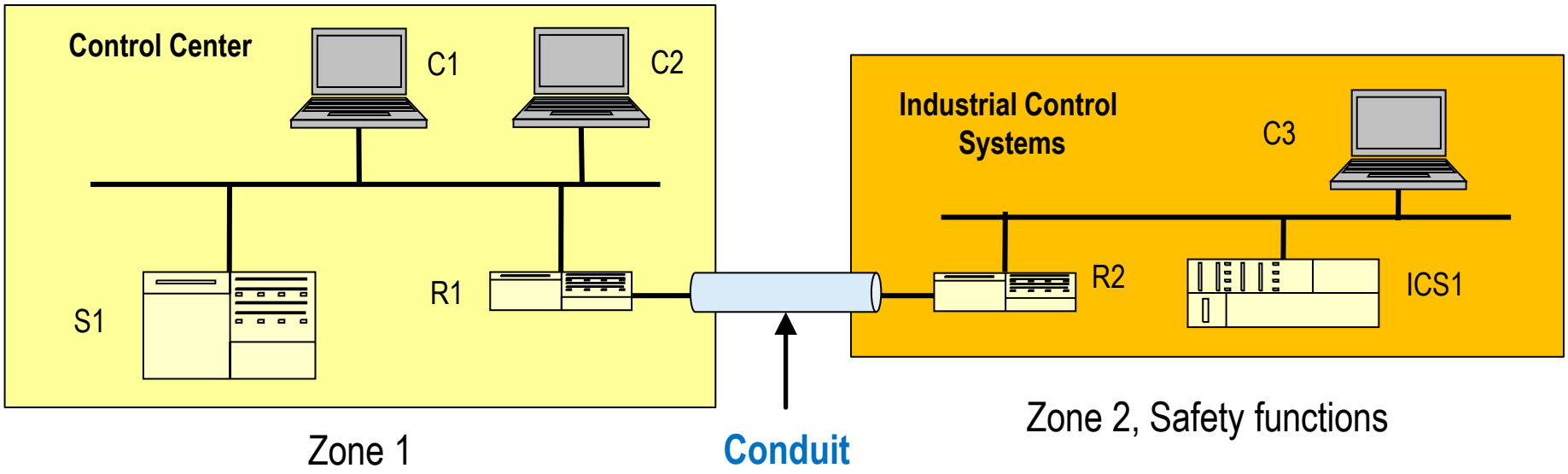
Rail

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"*

Conduit

"Logical grouping of communication channels, between connecting two or more zones, that share common security requirements"



General Concepts of IEC 62443: Security Levels

Rail

Security Level

"Measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner."

Definition of risk-based Security Levels:

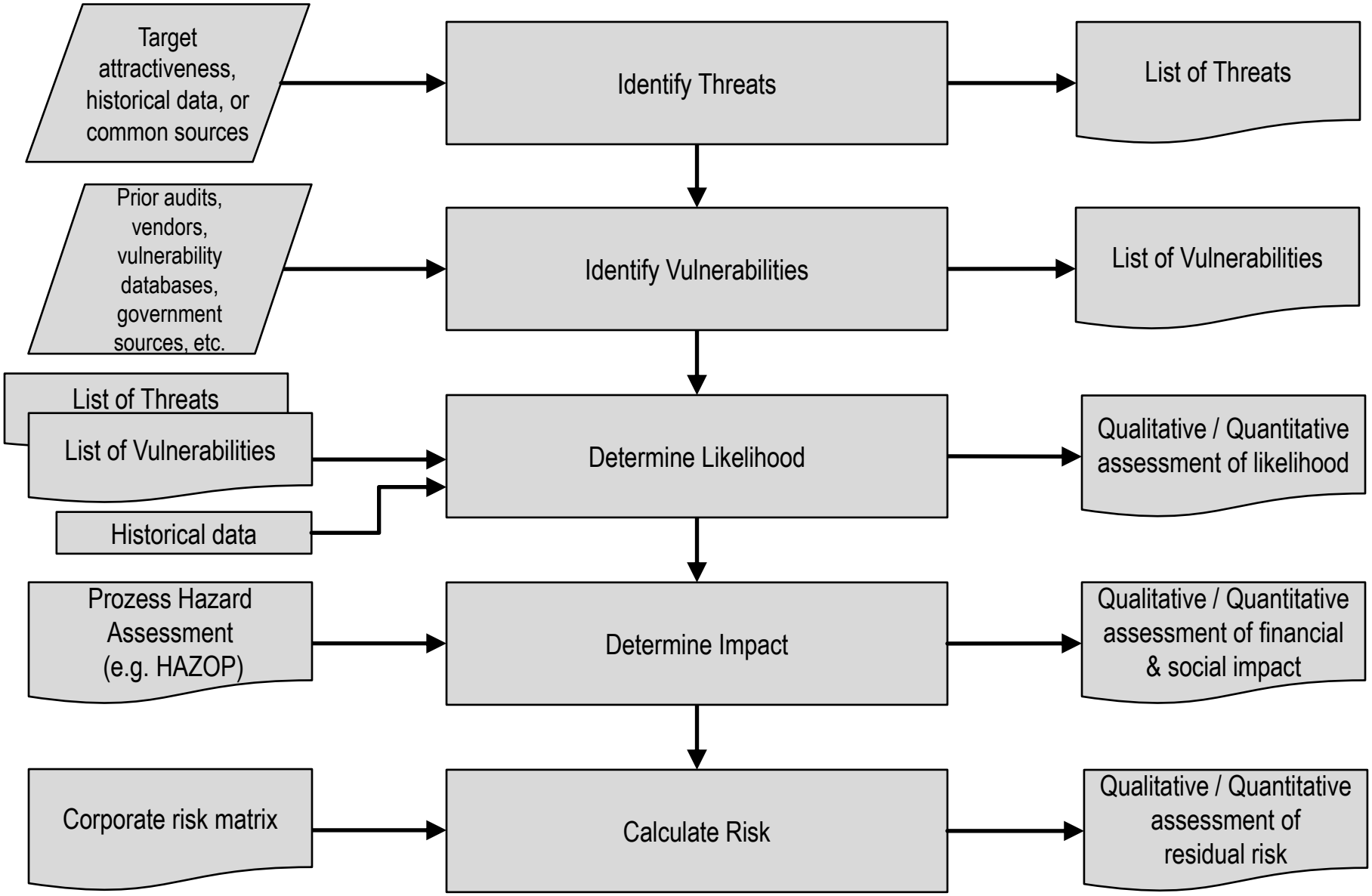
- **Security Level 0 (SL0)**
  No protection requirements.
- **Security Level 1 (SL1)**
  Protection against **casual** or **coincidental violation**.
- **Security Level 2 (SL2)**
  Protection against **intentional** violation using **simple means** with **low resources**, generic skills and low motivation.
- **Security Level 3 (SL3)**
  Protection against **intentional** violation using **sophisticated means** with **moderate resources**, system specific skills and moderate motivation.
- **Security Level 4 (SL4)**
  Protection against **intentional** violation using **sophisticated means** with **extended resources**, system specific skills and high motivation.

Security Requirements (Example)

Rail

	SL1	SL2	SL3	SL4
FR 1 – Identification and Authentication Control (IAC)				
SR 1.1 – Human user identification and authentication	**X**	**X**	**X**	**X**
The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.				
RE (1) Unique identification and authentication		**X**	**X**	**X**
The control system shall provide the capability to uniquely identify and authenticate all human users.				
RE (2) Multifactor authentication for untrusted networks			**X**	**X**
The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 4.14, SR 1.12 – Access via untrusted networks).				
RE (3) Multifactor authentication for all networks				**X**
The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.				

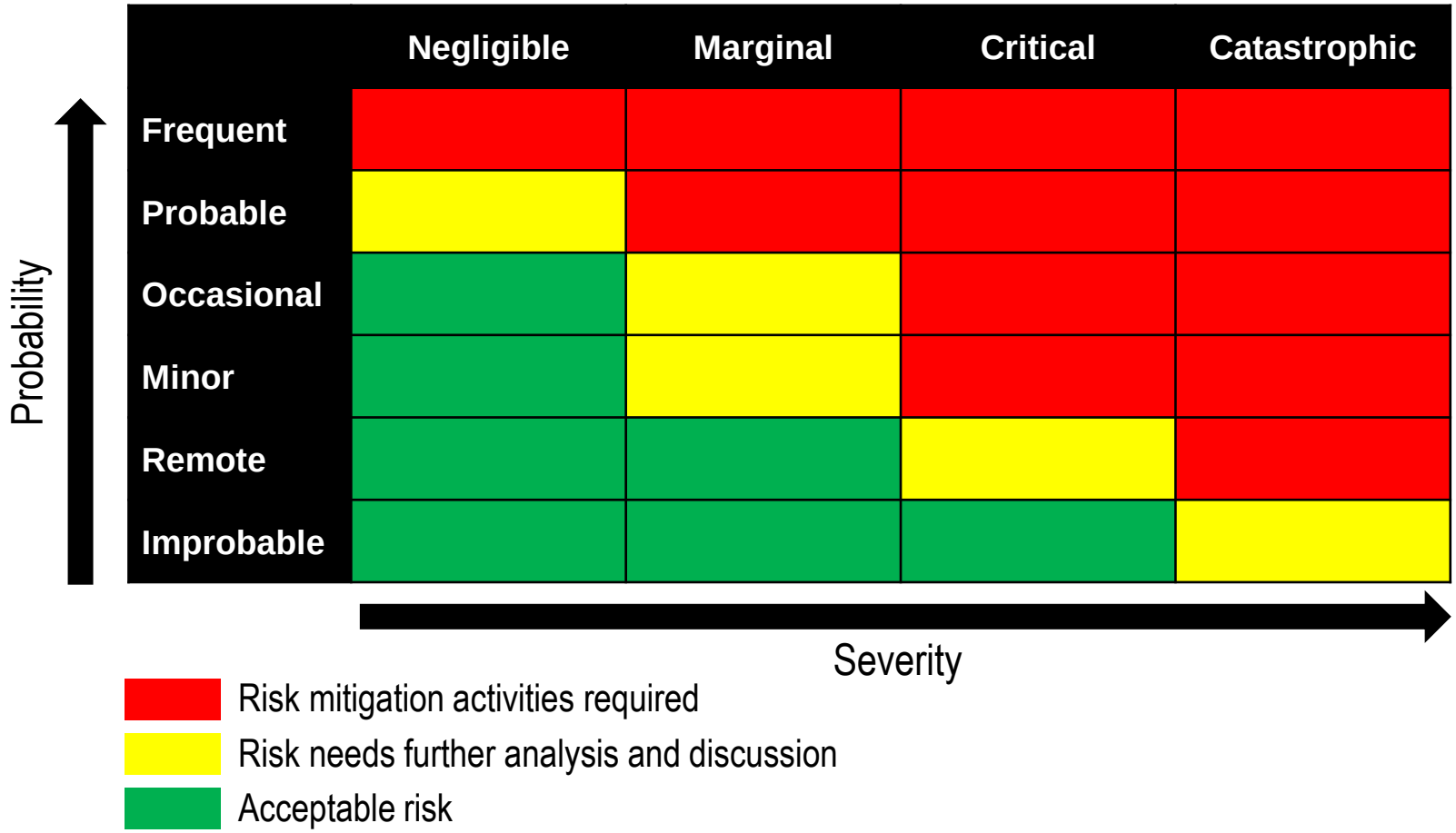
IEC 62443-3-2: Detailed Security Risk Assessment



Definition: Risk Matrix

Rail

- **Risk Matrix**
  - **System / Domain specific!!**



Agenda

1. Introduction Industrial IT Security Team
2. Security: Status quo
3. Introduction to IEC 62443
4. Best practices and concepts
5. **Summary**

Benefits of IEC 62443

Rail

- **The benefits of IEC 62443**
  - **Risk based approach**
  - **Process oriented**
  - **Combination with other standards possible**
  - **Defined requirements**
  - **International**

- **Best Practice approach for Industrial IT Security**
- **Basis for assessment and certification**

IEC 62443 standards family

IEC 62443-1-1, Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models. Bearbeitungsstand: IEC/TS 62443-1-1:2009, Überarbeitung geplant

IEC 62443-1-2, Industrial communication networks - Network and system security - Part 1-2: Glossary. Bearbeitungsstand: 65/465/NP:2011

IEC 62443-1-3, Industrial communication networks - Network and system security - Part 1-3: System security compliance metrics. Bearbeitungsstand: Entwurf IEC 65/557/DTS

IEC 62443-2-1, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program. Bearbeitungsstand: IEC 62443-2-1:2010, Als Entwurf zur Überarbeitung liegt vor: 65/514/DC:2012

IEC 62443 standards family

IEC 62443-2-2, Industrial communication networks - Network and system security - Part 2-2: Implementation guidance for an industrial automation and control system security program. Bearbeitungsstand: geplant

IEC 62443-2-3, Industrial communication networks - Network and system security - Part 2-3: Patch Management. Bearbeitungsstand: Entwurf IEC 65/554/DTR:2014

IEC 62443-2-4, Industrial communication networks - Network and system security - Part 2-4: Requirements for IACS solution providers. Bearbeitungsstand: Entwurf IEC 65/545A/CDV:2014

IEC 62443-3-1, Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems. Bearbeitungsstand: IEC/TR 62443-3-1:2009-07. Überarbeitung geplant.

IEC 62443 standards family

IEC 62443-3-2 Industrial communication networks - Network and system security - Part 3-2: Security levels for zones and conduits. Bearbeitungsstand: Entwurf IEC 65/534/DC:2013

IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels. Bearbeitungsstand: IEC 62443-3-3:2013

IEC 62443-4-1 Industrial communication networks - Network and system security - Part 4-1: Product development requirements. Bearbeitungsstand: 65/546/NP:2014

IEC 62443-4-2 Industrial communication networks - Network and system security - Part 4-1: Technical security requirements for industrial automation and control system components. Bearbeitungsstand: 65/546/NP:2014

NP: New work item proposal
CD: Committee draft
CDV: Committee draft for vote
DTR: Draft technical report
TR: Technical report
DTS: Draft technical specification

Security standards / guidelines / RFCs

Rail

RFC 5246, The Transport Layer Security (TLS) Protocol, Version 1.2, http://tools.ietf.org/html/rfc5246

ETSI, European Telecommunications Standards Institute, http://www.etsi.org/WebSite/homepage.aspx

RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, http://tools.ietf.org/html/rfc5280

RFC 5055, Server-Based Certificate Validation Protocol (SCVP), http://www.rfc-editor.org/rfc/rfc5055.txt

RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, http://www.ietf.org/rfc/rfc2560.txt

RFC 4210, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), http://tools.ietf.org/html/rfc4210

RFC 5273, Certificate Management over CMP (CMC): Transport Protocols, http://tools.ietf.org/html/rfc5273

Security standards / guidelines / RFCs

VDI/VDE 2182, Informationssicherheit in der industriellen Automatisierung, Allgemeines Vorgehensmodell, Blatt 1, Januar 2011

Contact

Rail

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

Phone: +49 89 5791-1930
Fax: +49 89 5791-2933

TÜV SÜD Rail GmbH
Barthstr. 16
80339 Munich
Germany

www.tuev-sued.com