Choose certainty.
Add value.

IT Security for control systems of ropeways

Dr. Thomas Störtkuhl
Team Leader Industrial IT Security
TÜV SÜD Rail
April 2016

Contact

Dr. Thomas Störtkuhl
thomas.stoertkuhl@tuev-sued.de
Phone: +49 89 5791-1930
Fax: +49 89 5791-2933

- Team leader Industrial IT Security
- 25 years experience in IT
- More than 15 years experience in information security
- Projects for companies; branches: critical infrastructures, automotive, production, administration, finance
- Certificates: CISSP, CISA, CISM, ISO/IEC 27001 Auditor

Current security incidents …

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.

The New York Times

POLITICS

Utilities Cautioned About Potential for a Cyberattack After Ukraine's

By DAVID E. SANGER FEB. 29, 2016

Email Share Tweet

WASHINGTON — The Obama administration has warned the nation's power companies, water suppliers and transportation networks that sophisticated cyberattack techniques used to bring down part of Ukraine's power grid two months ago could easily be turned on them.

BBC BBC iD Menu Search

NEWS

Hack attack causes 'massive damage' at steel works

22 December 2014 | Technology

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

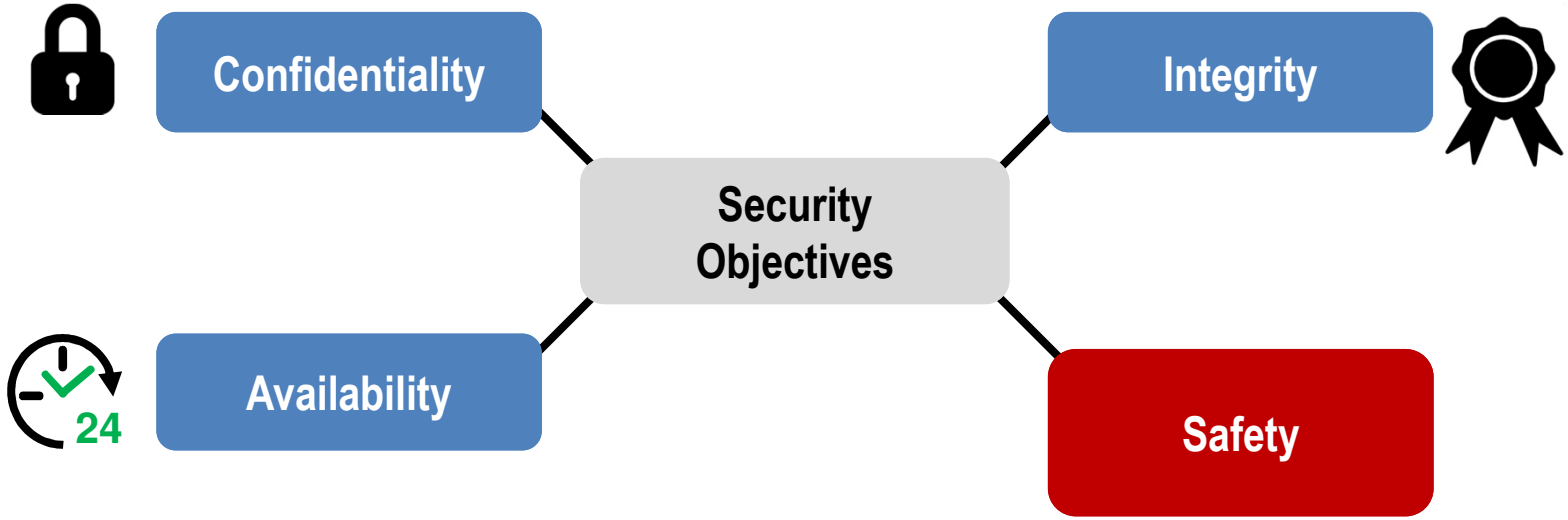
Täglich greifen Hacker deutsche Firmen an. Einige haben ihre Sicherheitsvorkehrungen deshalb in den vergangenen Jahren ausgeweitet. Doch die eigene Sicherheit liegt nicht mehr allein in den Händen der Unternehmen.

BloombergBusiness

Mysterious '08 Turkey Pipeline Blast Opened New Cyberwar

by Jordan Robertson and Michael Riley

What is (information) security?



Information Security is the preservation of (see ISO/IEC 27000)

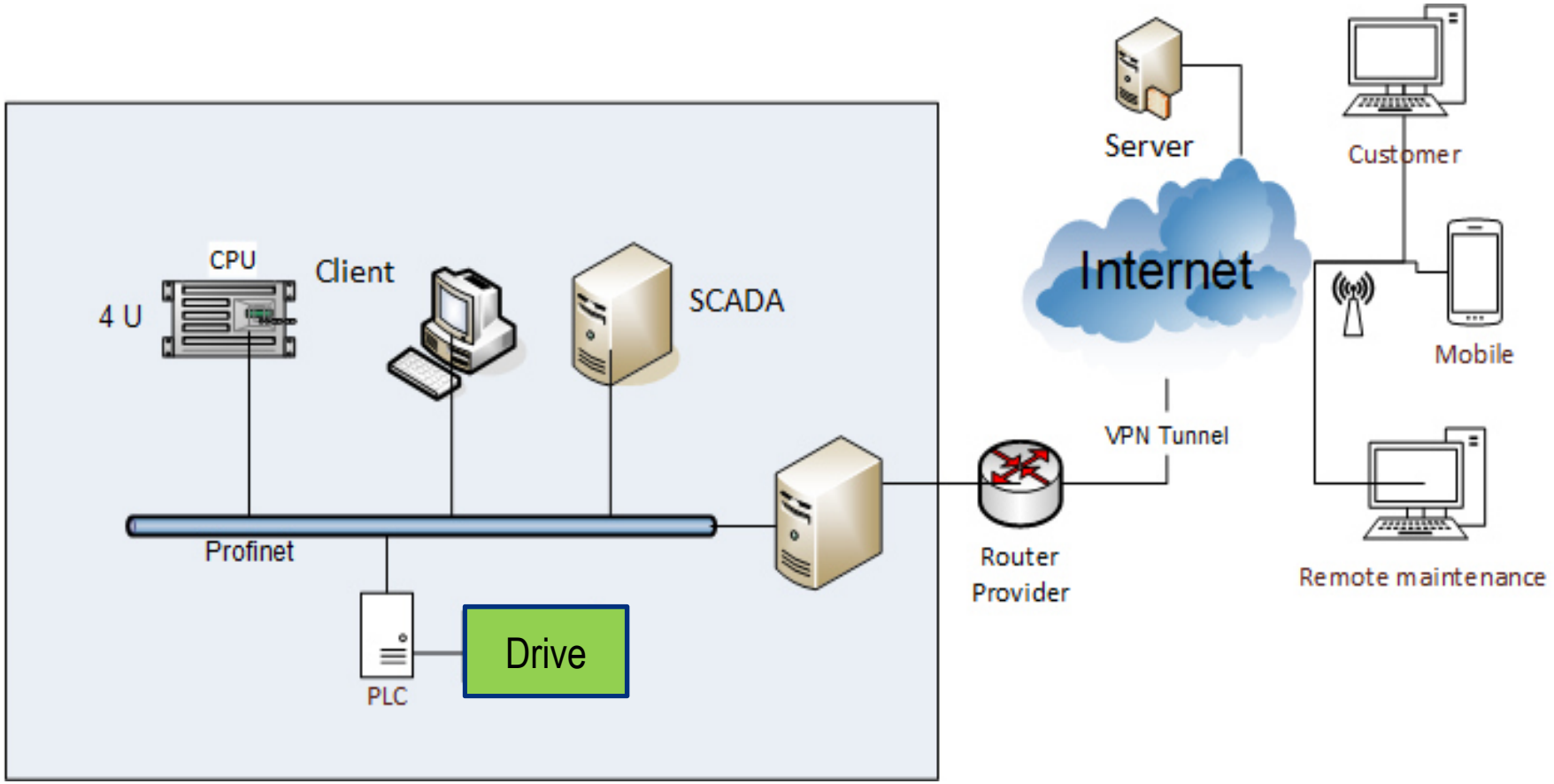
- **Confidentiality**
  The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- **Integrity**
  The property of protecting the accuracy and completeness of assets.
- **Availability**
  The property of being accessible and usable upon demand by an authorized entity.

and for control systems also

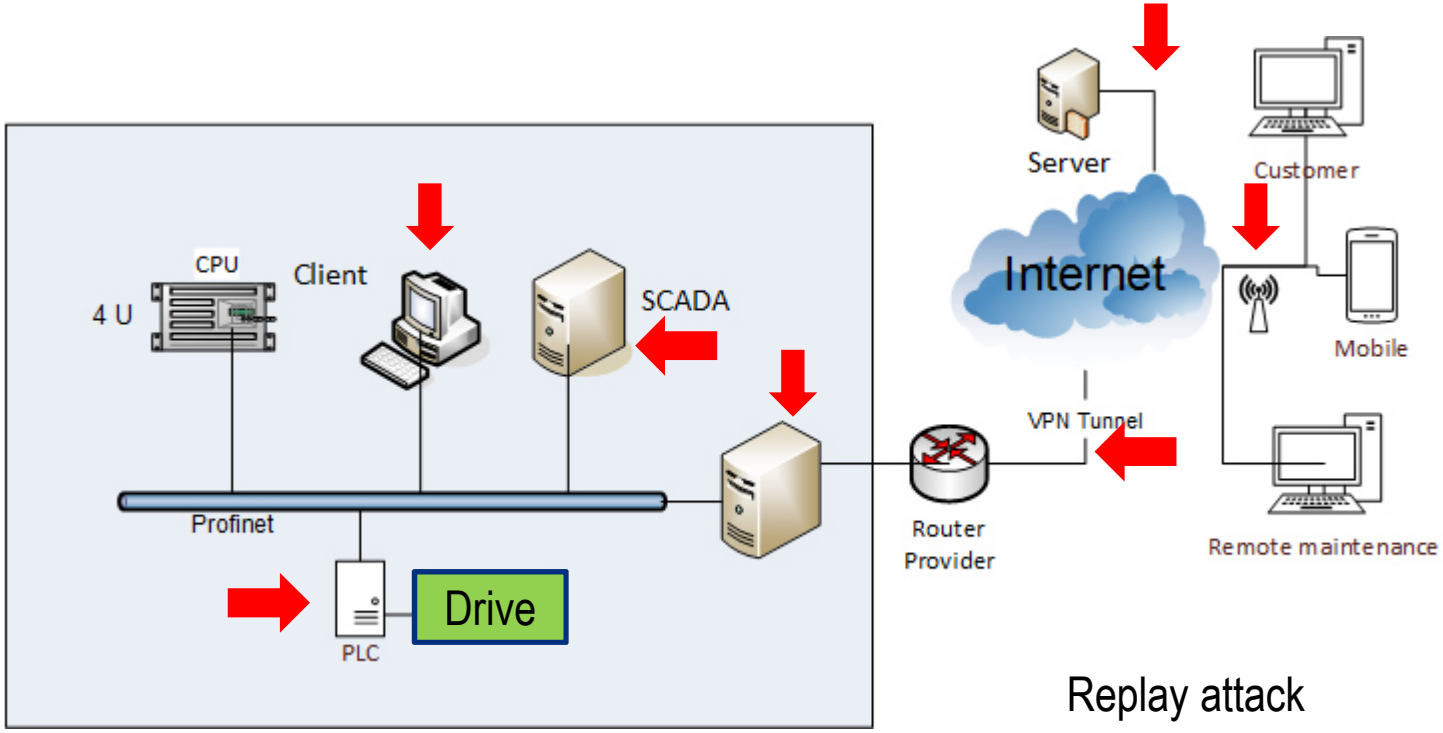
- **Safety** *Freedom from unacceptable risk. (siehe IEC 61508)*

has to be considered.

Control system for ropeways (simplified)



Threats to the control system infrastructure of ropeways



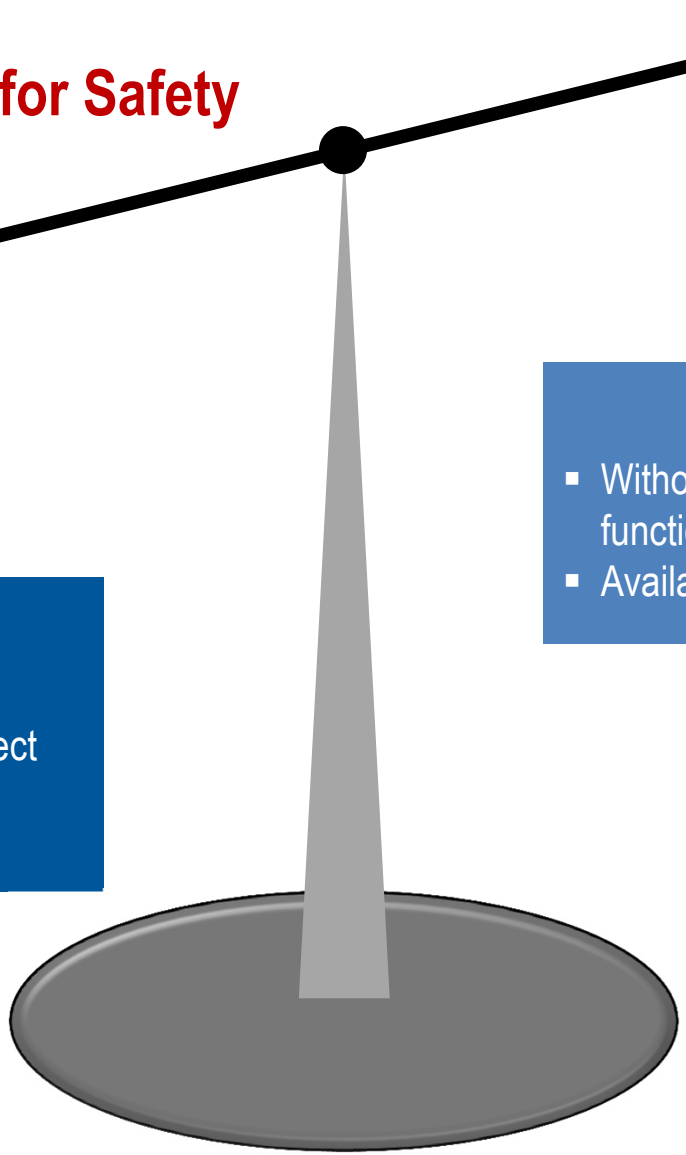
Replay attack
Malware like virus, trojans
Denial-of-Service
Manipulation …….

Possible impacts of threats

- Denial-of-Service: no remote maintenance
  => long interruption for service
- Manipulated SCADA: change of parameters and settings of control system
  => no normal operation
  => system may be stopped
- Encryption of data
  => attempted extortions
- Manipulated control
  => system may be stopped
  => safety might be manipulated

Mandatory rules for control systems

Safety first, Security for Safety



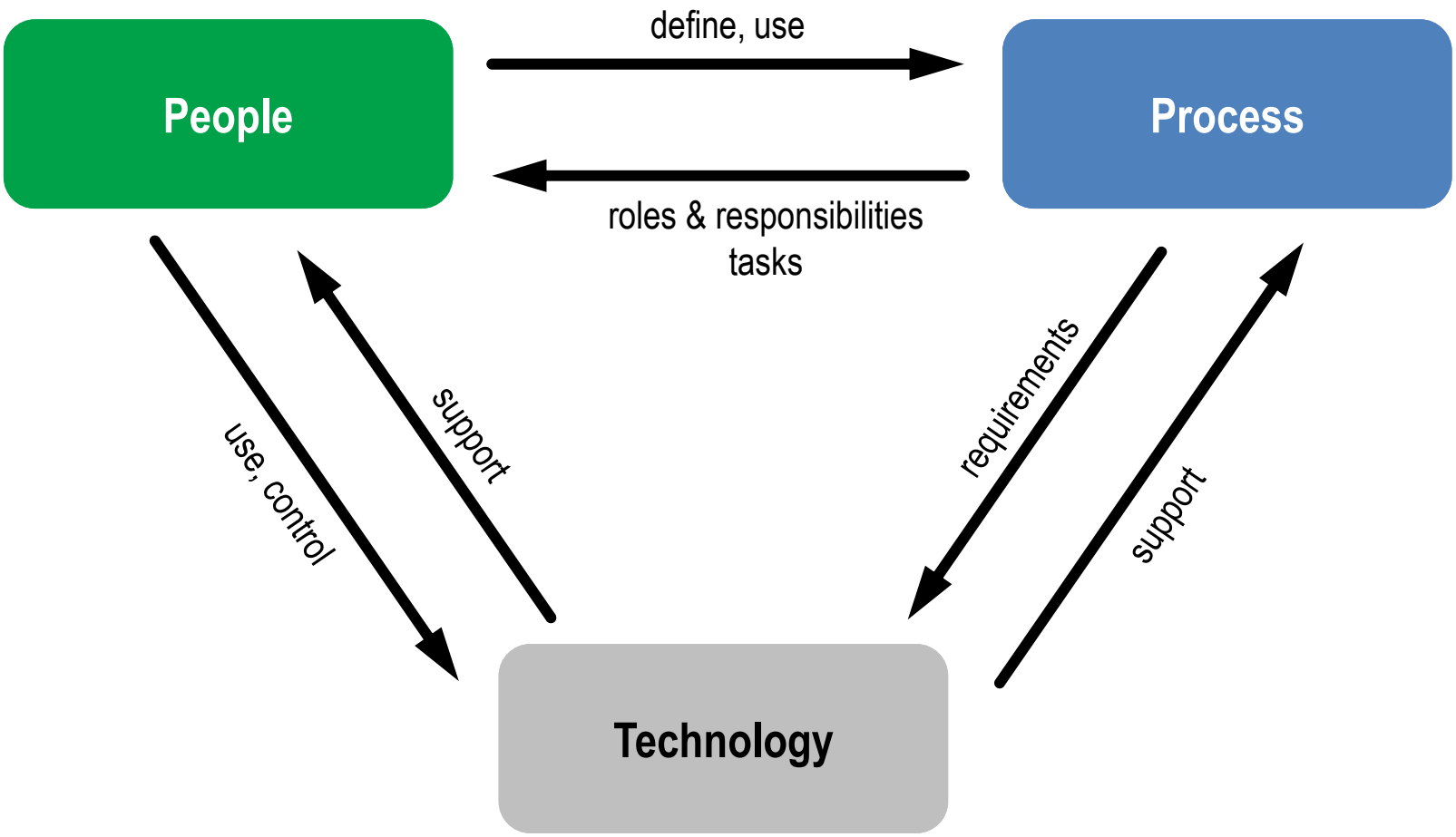
SAFETY

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

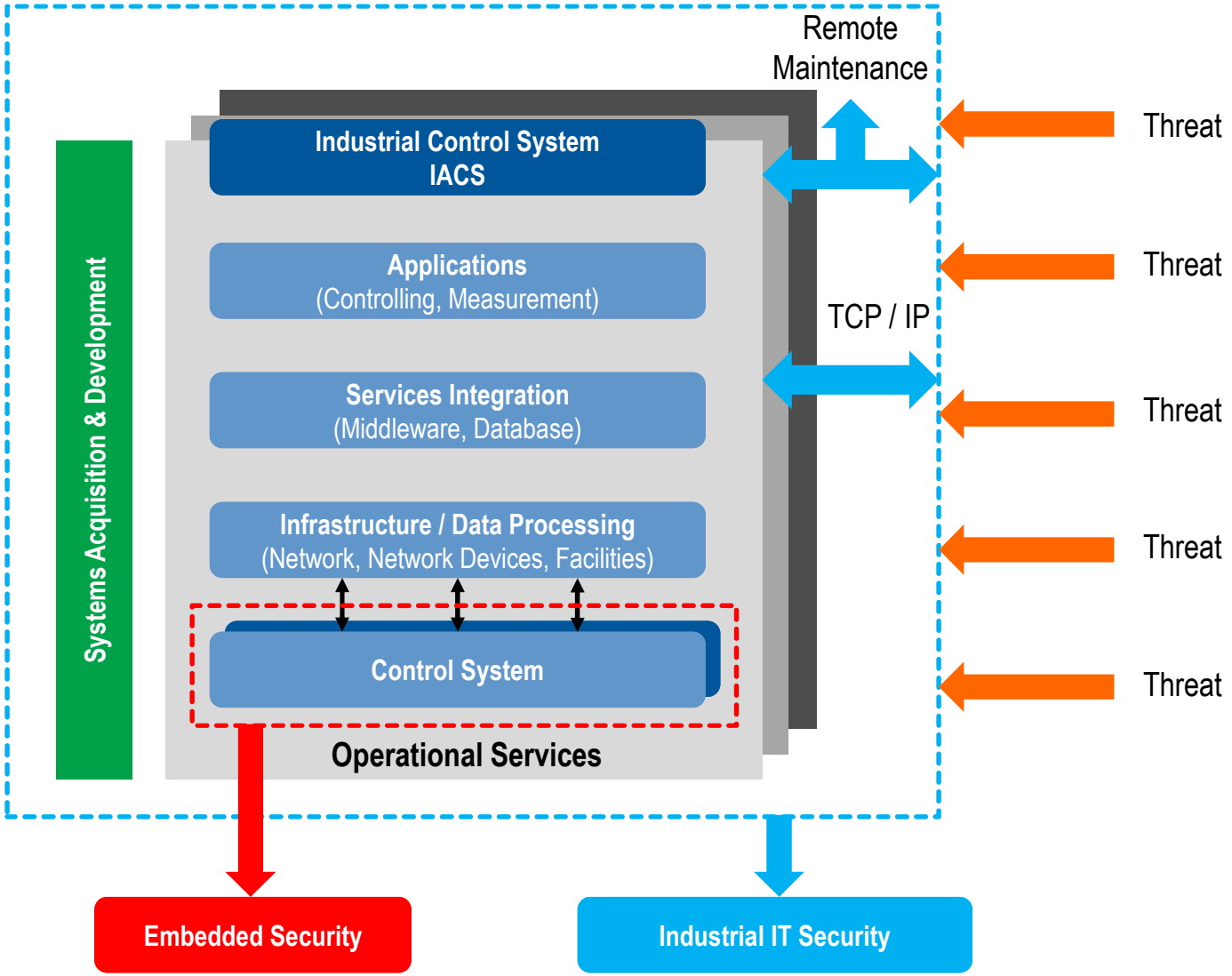
SECURITY

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

People, Process, Technology

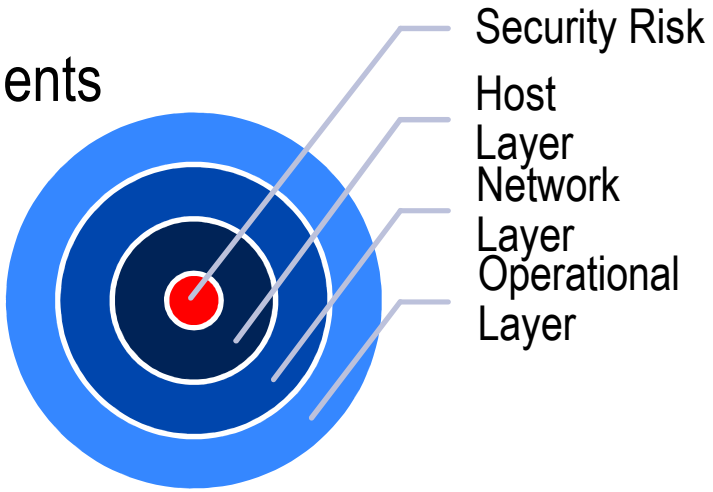


Holistic approach



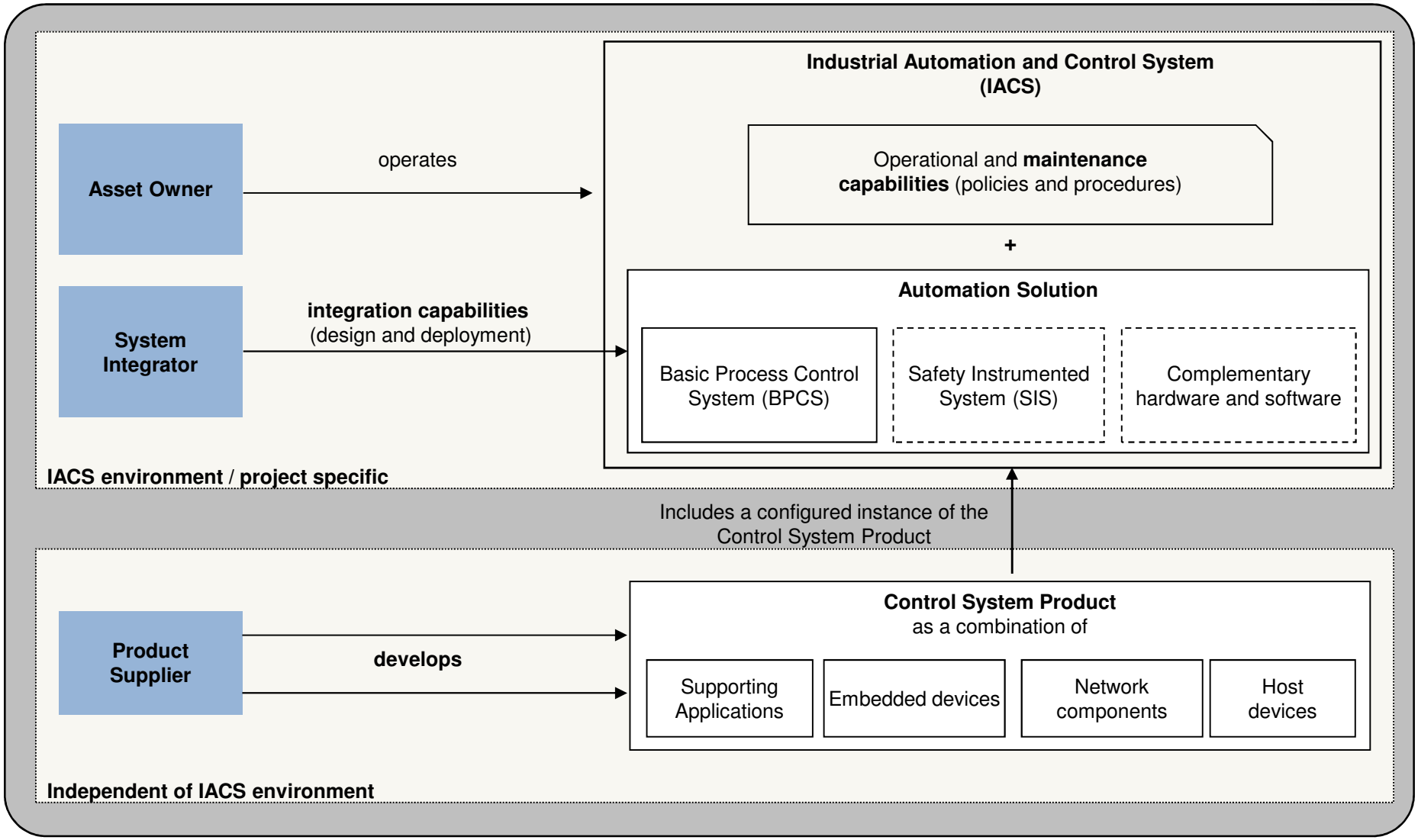
Defense-in-depth strategy

- 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



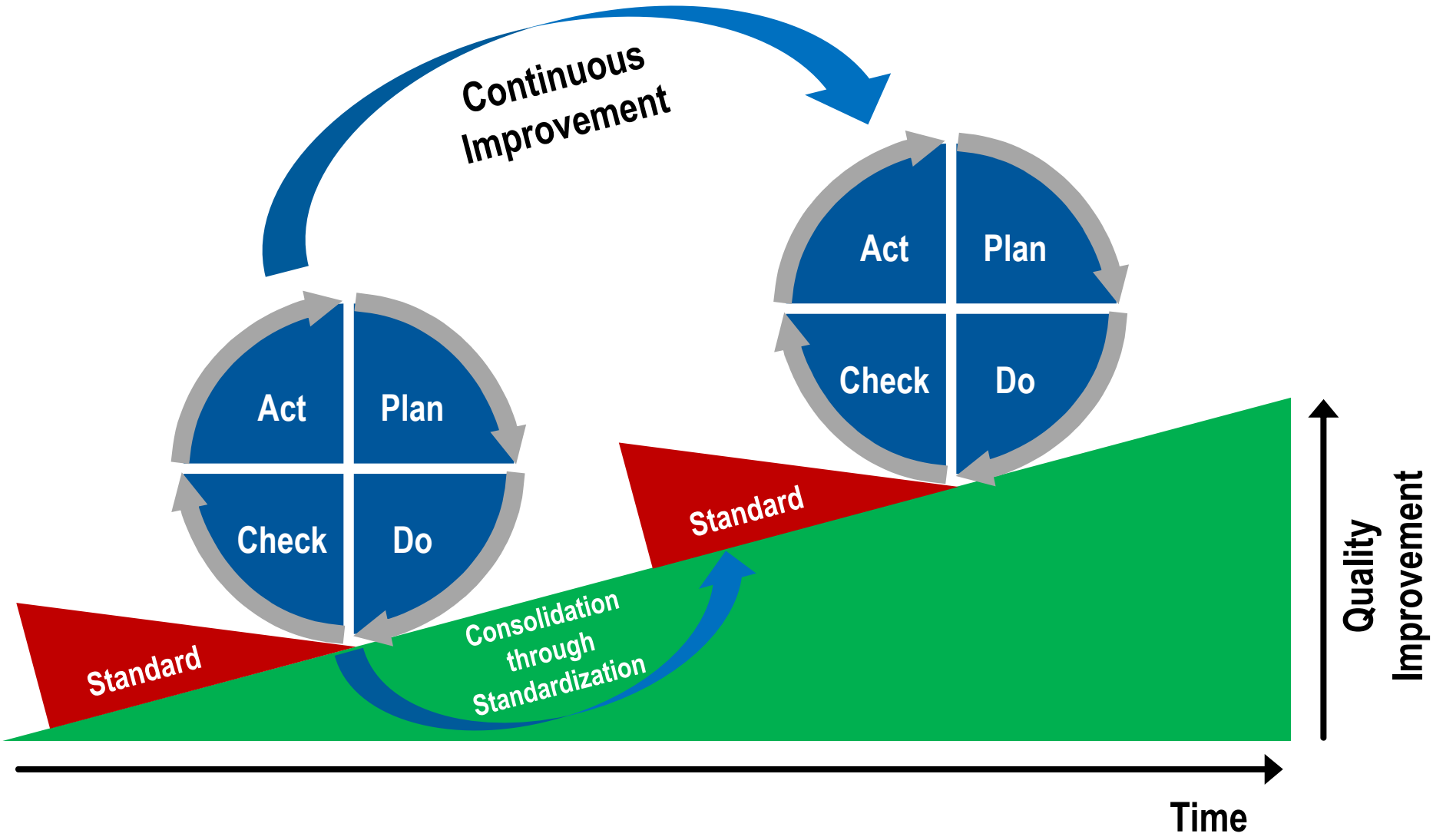
cf. Homeland Security (2009) Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies figure 5

Must be considered: Roles



Source: IEC 62443 standard

Continuous Improvement: Security is a process



Contact

Frank Seyfried
frank.seyfried@tuev-sued.de
Phone: +49 89 5791-2430
Fax: +49 89 5791-2470

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

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

TÜV SÜD
Westendstr. 199
80686 Munich
Germany

www.tuev-sued.com