

# Functional Safety and Cybersecurity:

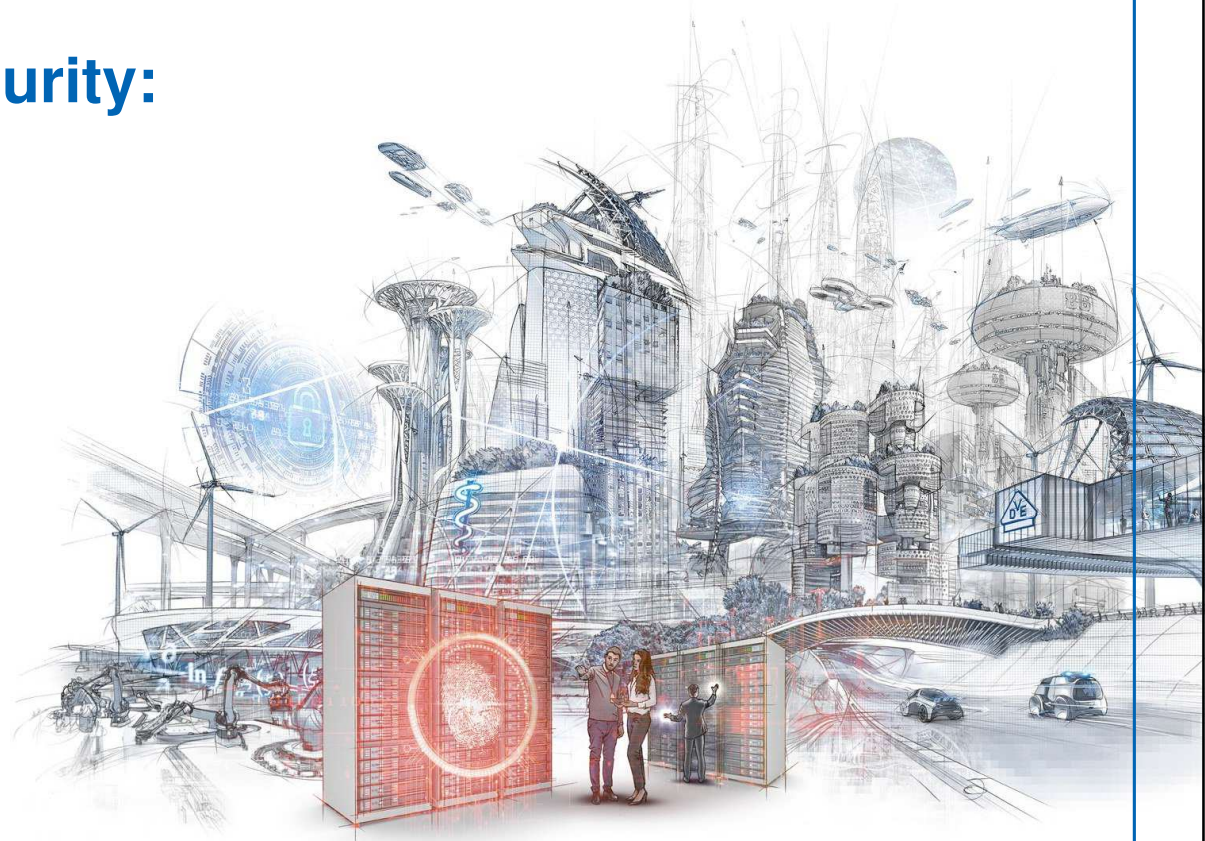
*Dependencies*

*Standards*

*Pragmatic approaches*

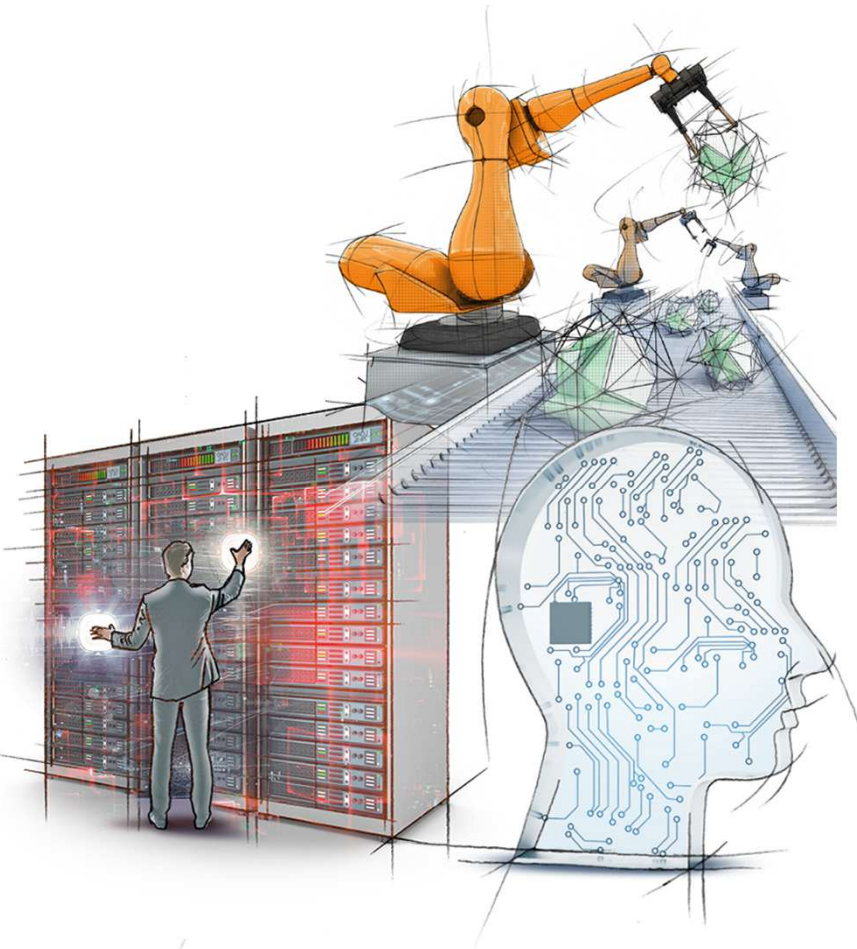
Florian Spittler

September 25<sup>th</sup> 2023, Pune



**DKE**

# DKE is the trusted platform for:



- standardization,
- cooperation
- and the interaction of experts

## in the areas of:

- electrical engineering
- Electronics
- information technologies

German member in IEC, CENELEC and ETSI

# Short introduction



Find me  
on LinkedIn:



## Member of the DKE Executive Board, since 2019

- Leading the division External Relation & Support
- Analyzation of political and business environment; development of standardization strategies
- Responsible for bi- and multilateral international cooperation
- Representation of German interests IEC, CENELEC and ETSI

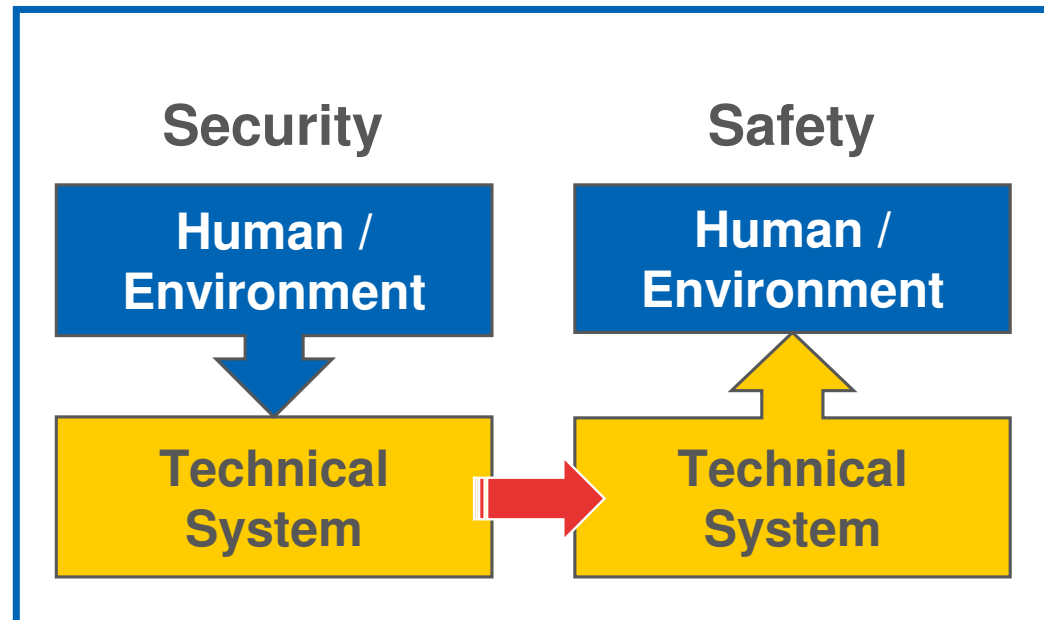
## Industry Experience

- Former Director of Sales and Marketing, Test Manager and Test Engineer in the Automotive Industry for safety critical products

## Education

- Diploma (Master equivalent) in Electrical Engineering, Electronics and Information Science of Friedrich-Alexander University Erlangen-Nürnberg, Germany
- EMBA of Quantic School of Business and Technology, Washington DC, USA
- Program for Executive Development (PED), Diploma of IMD, Lausanne, Switzerland

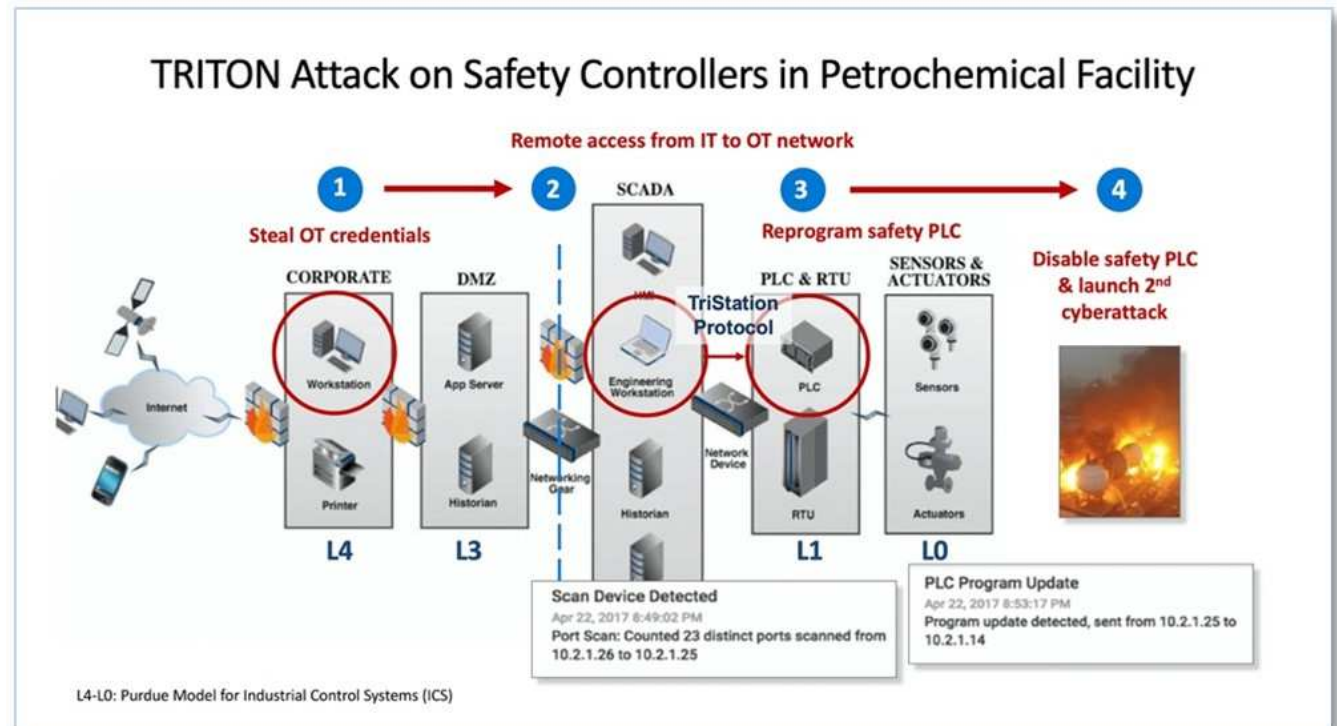
# What is Security and what is Safety?



# Attack-Framework TRITON

Discovered 2017

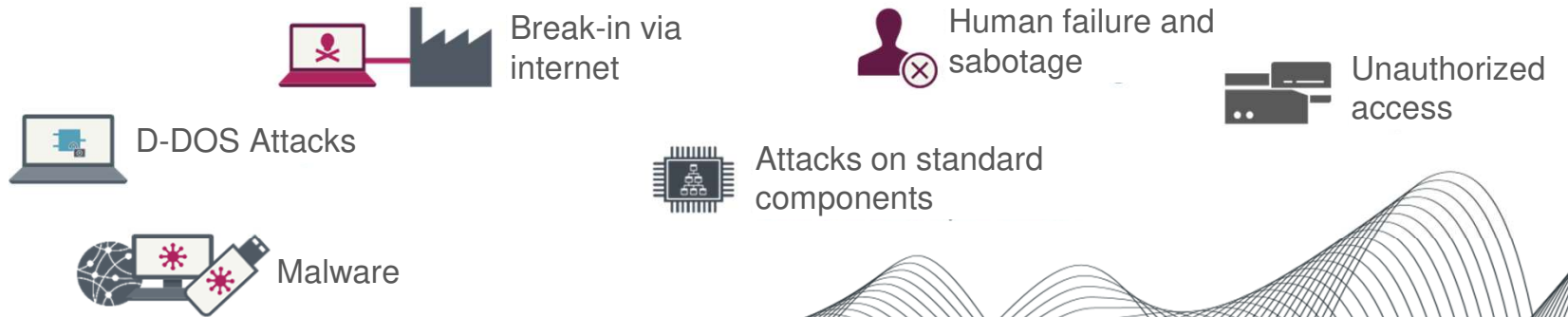
- First public incident of an attack against a SIS (Safety Instrumented System)
- Software to intrude an ICS network (Industrial Control Systems) and manipulate safety products
- Intention: cause physical damage
- Target: Triconex products of Schneider Electric



# Cybersecurity needs continuous processes due to the changing threat environment



## Changing threat environment\*



## Changing infrastructure



# Information Technology (IT) & Operational Technology (OT)



## IT – Management of information

- web/app/data/email server, management systems
- Primary security objective: **confidentiality**
- e.g., ISO/IEC 27000 series

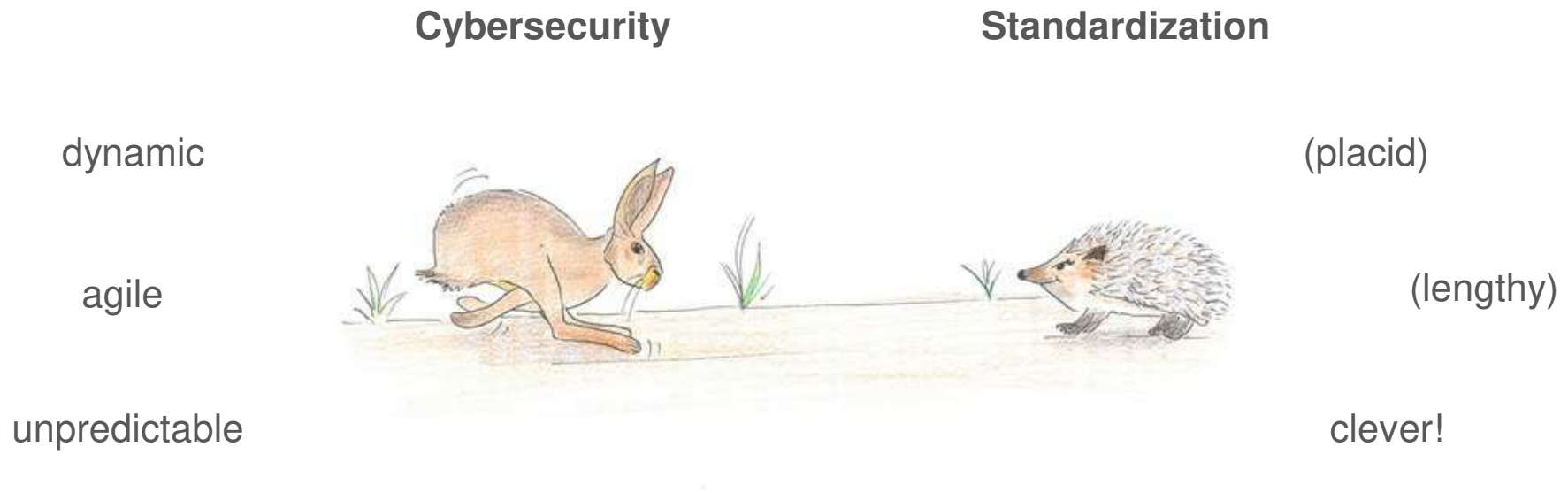


## OT – Management of physical processes

- Industrial Controls (PLC, DCS, SCADA & I/O), sensors, embedded systems, ...
- Primary security objectives: **availability & integrity**
- e.g., IEC 62443 series

# Why cybersecurity in standardization?

*What is the goal?*



Goal of the hedgehog: Not be as fast as the rabbit, but cleverer!



**Goal of standardization: No 100% specification but develop guidelines and assistances!**

Quelle: [https://www.ndr.de/fernsehen/service/leichte\\_sprache/haseundigel118\\_v-contentgross.jpg](https://www.ndr.de/fernsehen/service/leichte_sprache/haseundigel118_v-contentgross.jpg) © Universität Hildesheim





# To reduce complexity: use standardization!

„The product/system is secure!“

- ...can never be shown due to unpredictability (environment changes almost daily)
  - ...is not a useful goal (deterrent)
- **complex!!**

„We have done everything reasonable to make the product/system secure.“

- ...can be shown
- ...can be documented and certified!

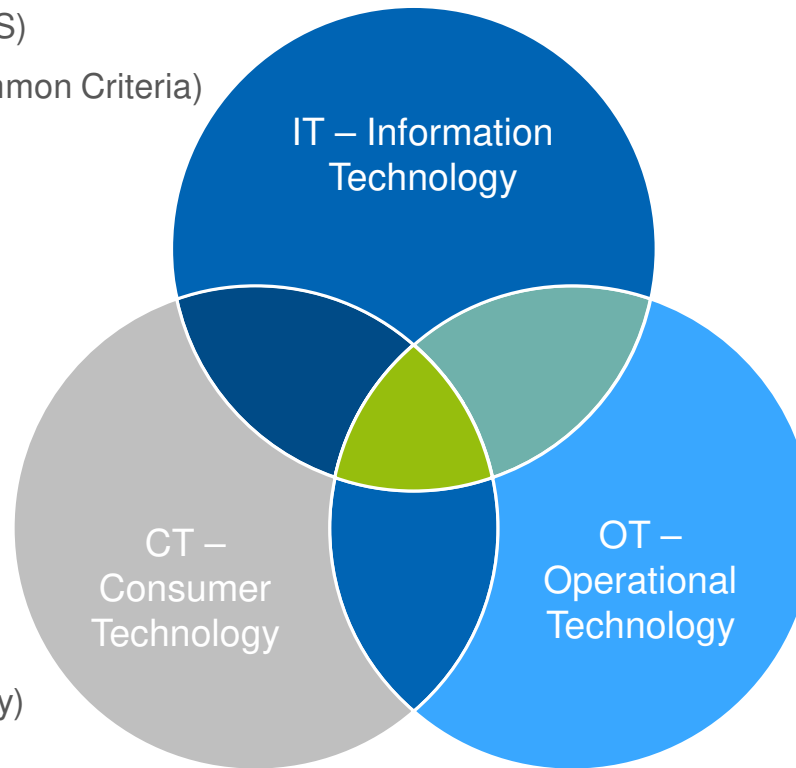
↓  
**Improvement due to use of norms and standards!!!**



# Information Technology (IT) & Operational Technology (OT)

*IT/OT/CT Standardization landscape*

- ISO/IEC 27000 series (ISMS)
- ISO/IEC 15408 series (Common Criteria)



- ETSI EN 303 645 (IoT-Security)

- IEC 62443 series (Industrial Automation)
- IEC 62351 series (Smart Grid Communication)
- IEC 63096 (Nuclear Power Plants)
- IEC 80001 series (Medical Devices)
- IEC 63110 series (Charging Infrastructure)
- ...

# Sectors for Operational Technology



Energy Supply



Process Industry



Automotive Industry



Renewable Energy



Shipbuilding



Railway Industry



Water Industry



Machine Building Industry



Industrial Electronics



Building Automation

# Examples for the interaction between standards for functional safety and OT security

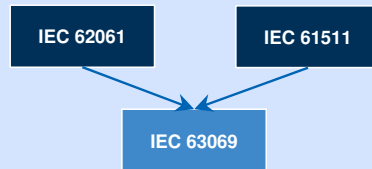
IEC 62443

„Horizontal“ series for OT security

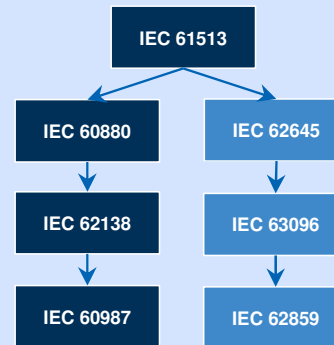
IEC 61508

„Horizontal“ series for functional safety

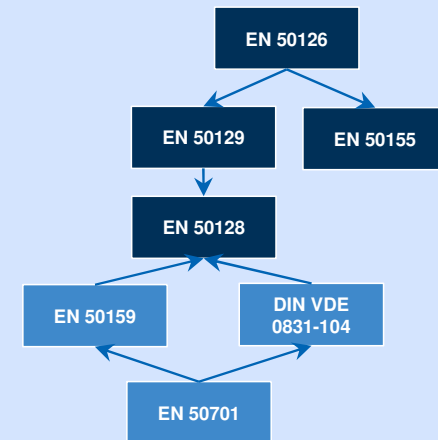
## Process industry



## Nuclear energy

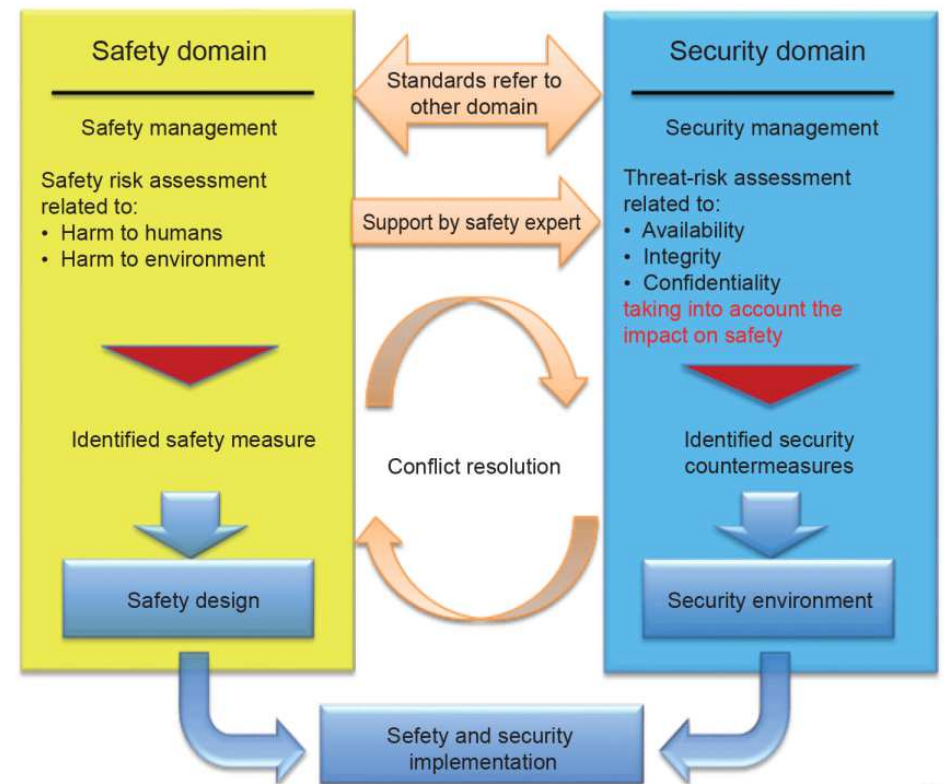


## Railway



# IEC TR 63069 – Industrial-process measurement, control and automation – Framework for functional safety and security

- Information and guidelines for a common application of IEC 61508 (Safety) and IEC 62443 (Security)
  - Guiding principle 1: protection of safety implementations
  - Guiding principle 2: protection of security implementations
  - Guiding principle 3: compatibility of implementations
- Product lifecycle should cover both safety and security measures:
  - Concept and development
  - Production, use and maintenance
  - Support und End-of-life
- IEC TR 63069 helps with the understanding of safety and security, but it is no magical bullet for the application



IEC

**DKE**

# Thank you for your attention!

We are building the e-dialistic future.  
Please join us.

## Your contact:

Florian Spittler  
Head of External Relations & Support  
Member of the DKE Executive Board  
Phone +49 69 6308-380  
[florian.spittler@vde.com](mailto:florian.spittler@vde.com)



# DKE