Challenges in Securing Railway Signalling

CyberSecurity4Rail Conference 2017

DB Netz AG | Christian Schlehuber | I.NPS 5 | Brüssel | 2017-10-04

Agenda

1. Introduction
2. New Features – New Threats
3. Domain-specific challenges
4. Security for Safety & Lessons learned
5. Conclusion

Introduction
Railway (in Germany)

Biggest business premises in Germany – **with public access**

- **5,700** Stations (in Germany) as gate to railway transportation
- **33,500** km rail network
- **48,800** heated railway switches (of 70,000 total)

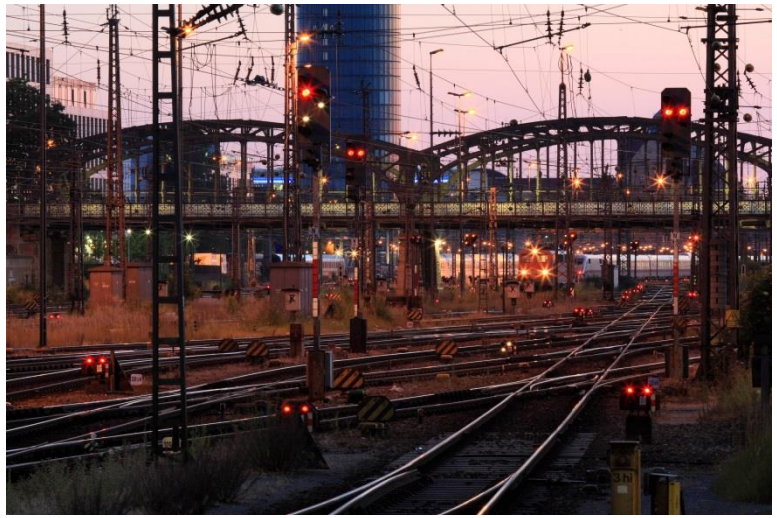
- Approx. **3,300** interlockings
  - **1,323** electronic interlockings (ESTW)

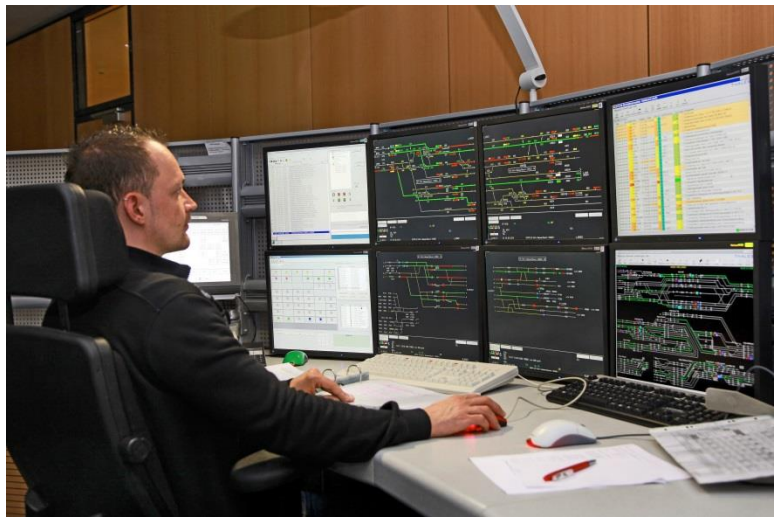
Main Objective: Safe railway operation

Strong regulations of technical installations (according Safety)

- EN 50126 (Reliability, Availability, Maintainability, Safety – RAMS)
- EN 50128 (Software for safety systems)
- EN 50159 (Communication)
- Etc.

➔ National Safety Authority has to grant **admission for every interlocking**



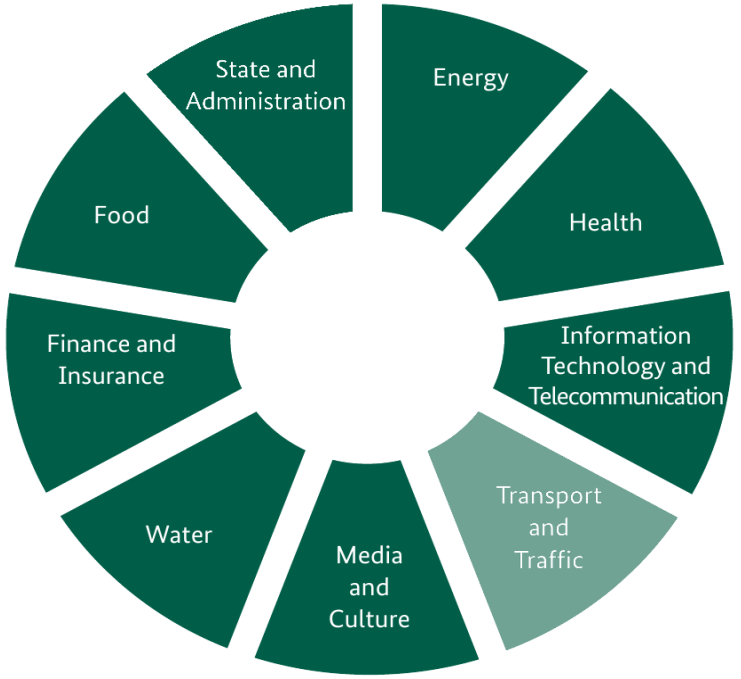


Motivation

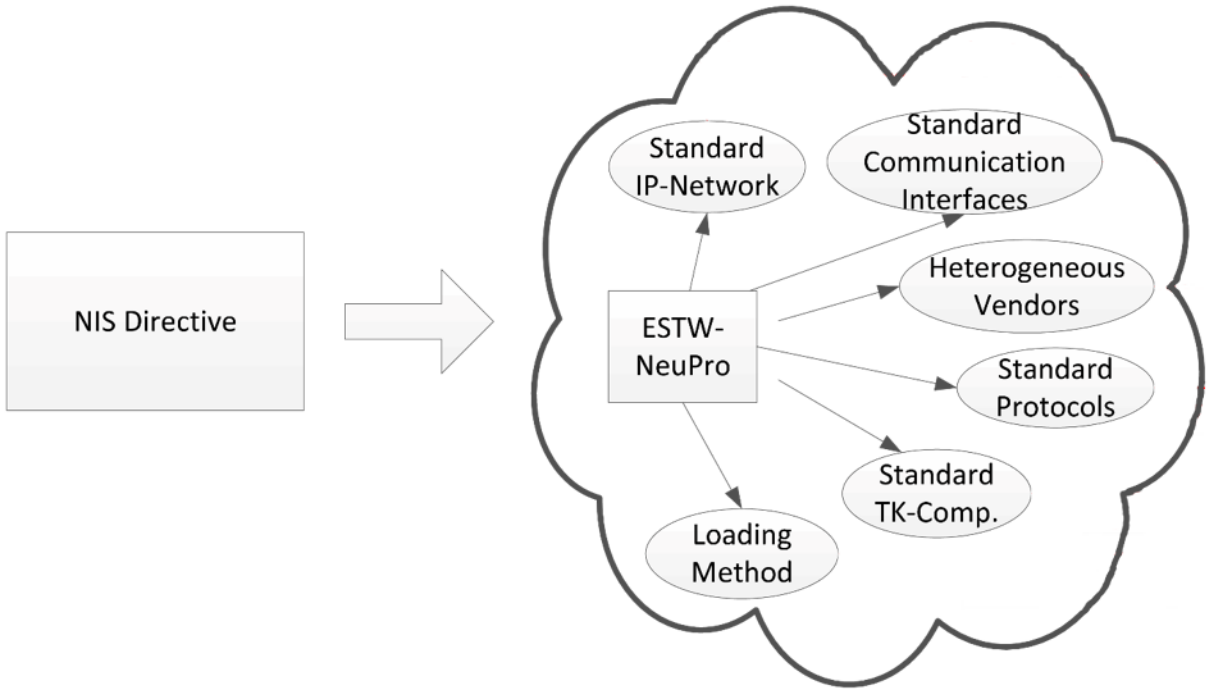
- Railway transport significantly contributes to our society's mobility and economy

- Railway is considered as Critical Infrastructure in many countries (including Germany) and the European Union
  - In Germany TEN-T Corridors categorized as critical

- Failures would result in disruption of public safety and security as well as supply shortages

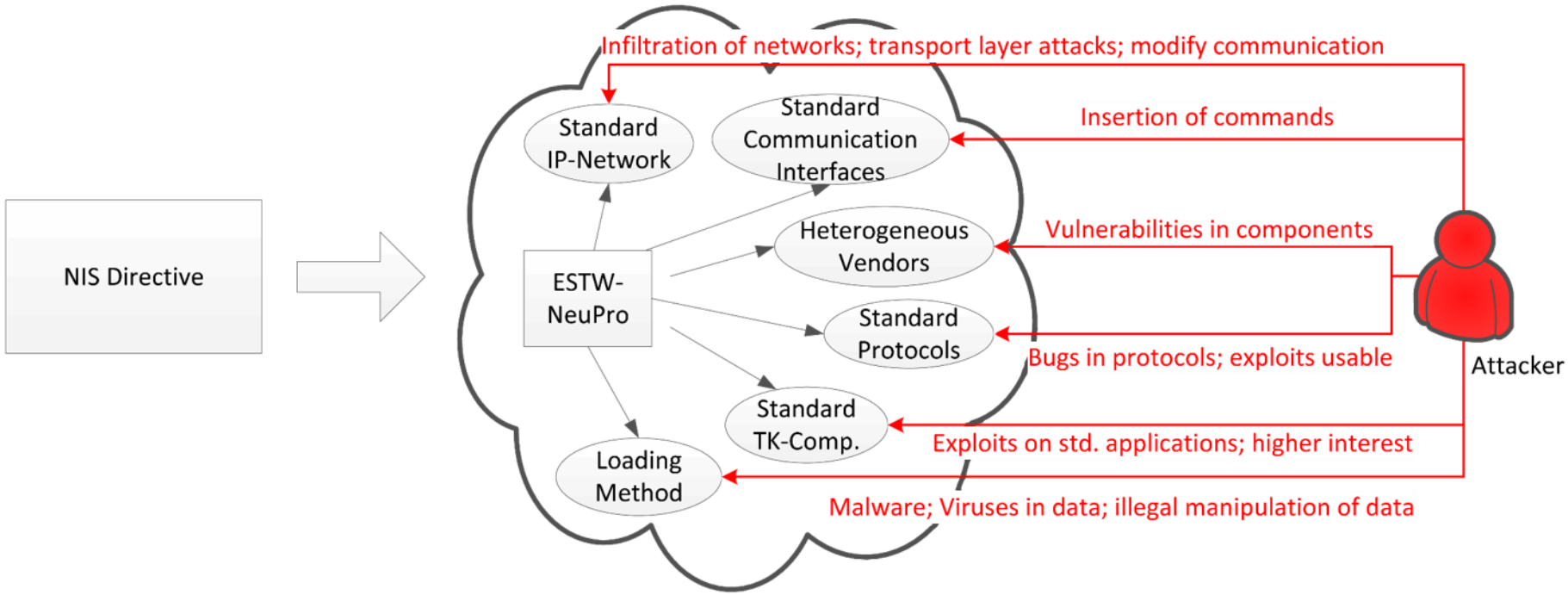


New Features



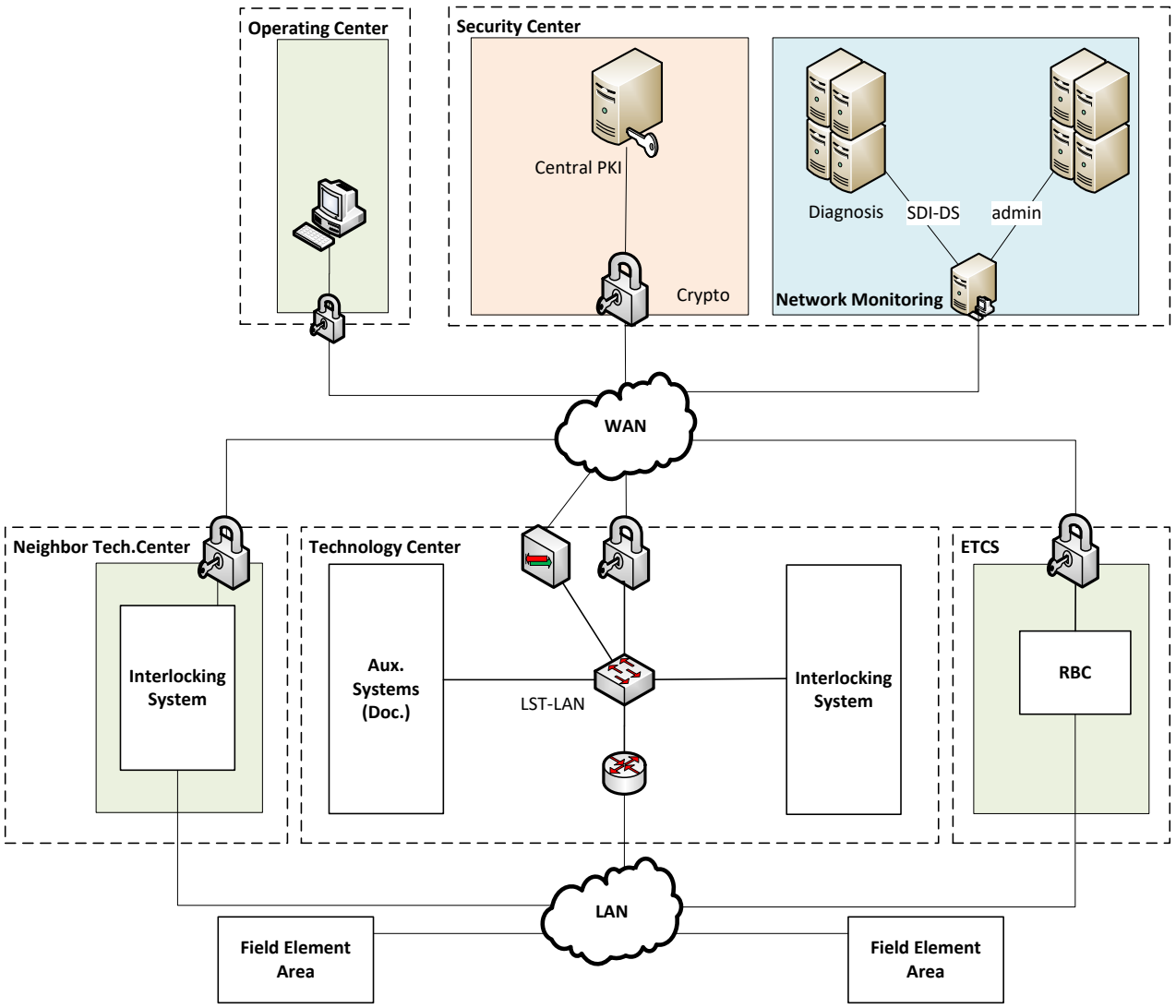
ESTW-NeuPro (DSTW) ➔ euLynX

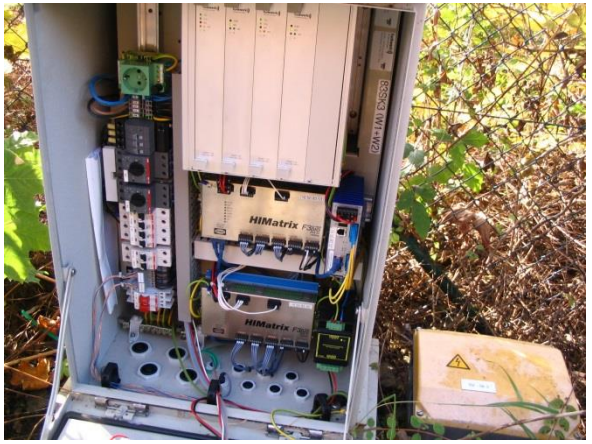
New Threats



ESTW-NeuPro (DSTW) ➔ euLynX

Current Architecture Design





Domain Specific Requirements

Eisenbahn-Bundesamt

Homologation (admission) through National Safety Authority

Takes months or years

Freedom of interference (between security and safety)

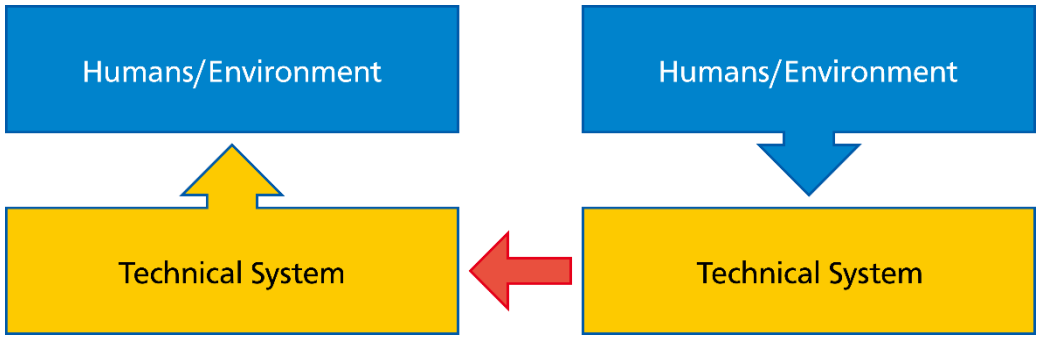
Loss of admission o/w

§

Laws and Regulations

- Directive on Network and Information Security (NIS)
- German IT Security Act

Domain Specific Requirements – Standards



Source: IEC Draft Guide 120 Edition 1

Safety

EN 50126

EN 50128

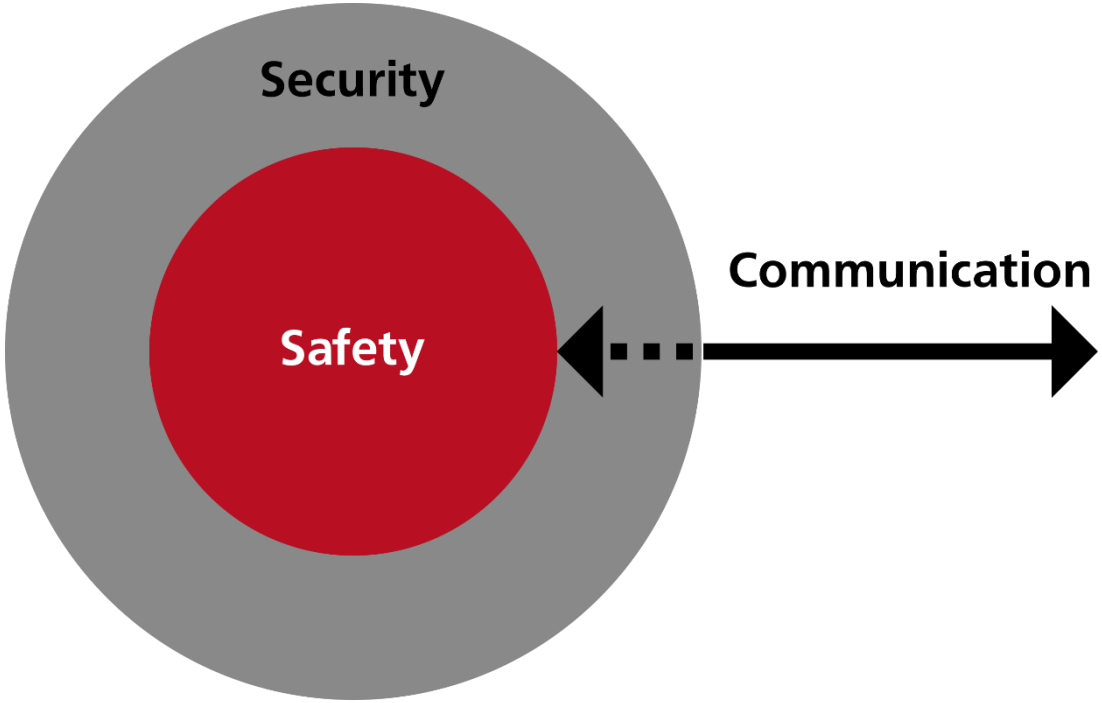
EN 50129

EN 50159

Security

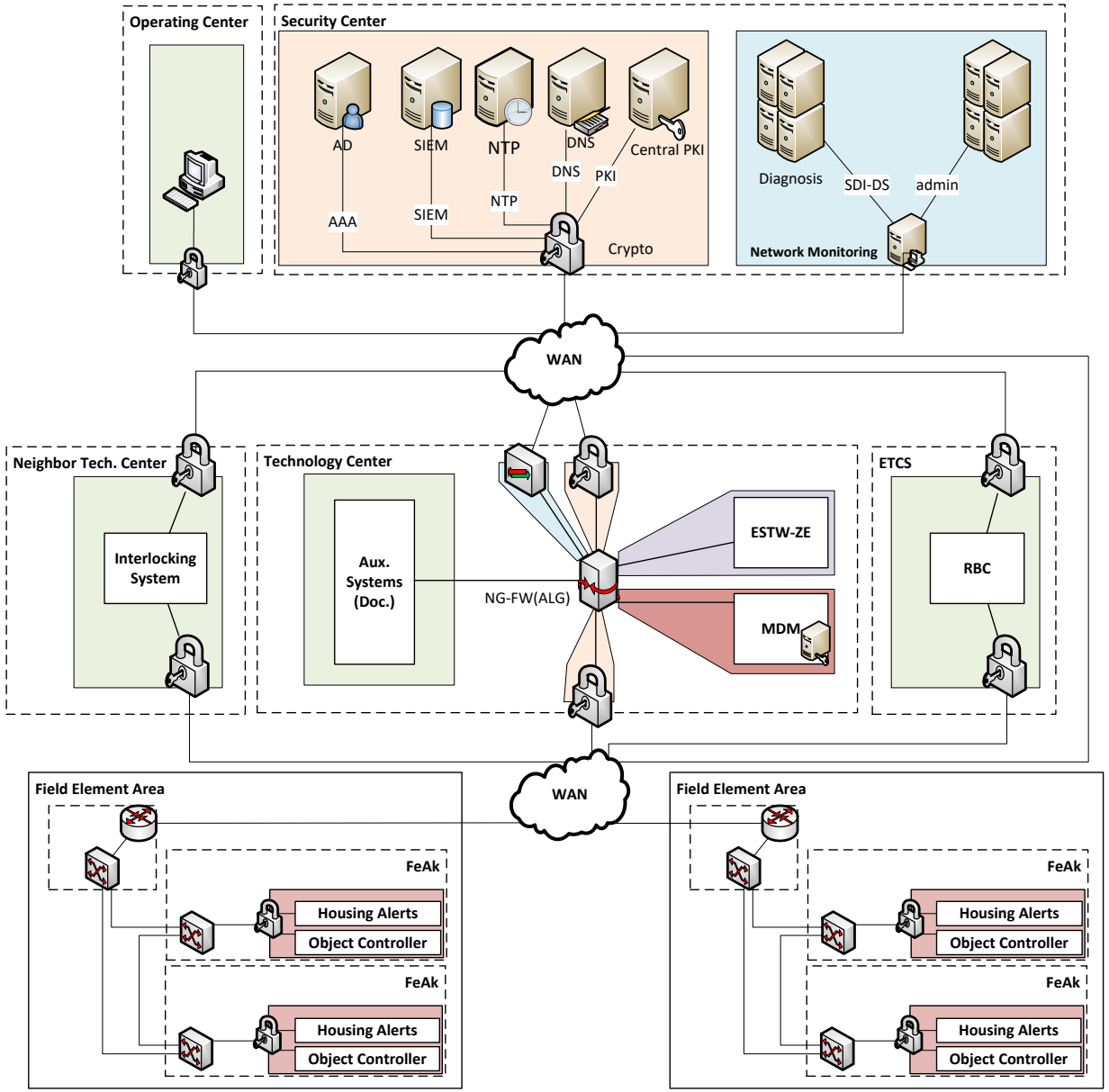
IEC 62443

Security for Safety – Shell Concept



Required Security Applications

Security-Applied Design



(Remaining) Challenges

- Vulnerability Analysis and recommendations
  - Is knowledge about the systems available?
  - Can the Recommendations be implemented?

- Preventive Vulnerability Scanning
  - Is my system capable of a scan?

- Penetration Testing
  - May the test result in outages?

- Staff Training and Awareness
  - Is our staff capable to understand cyber security?

- Forensic Analysis
  - Analysis vs. Fast Recovery

Lessons Learned:
Shell is not the end of the road

- Safety and Security Departments worked parallel with minimum interaction

➔ Safety and Security performed own analyses, estimated impacts and derived requirements

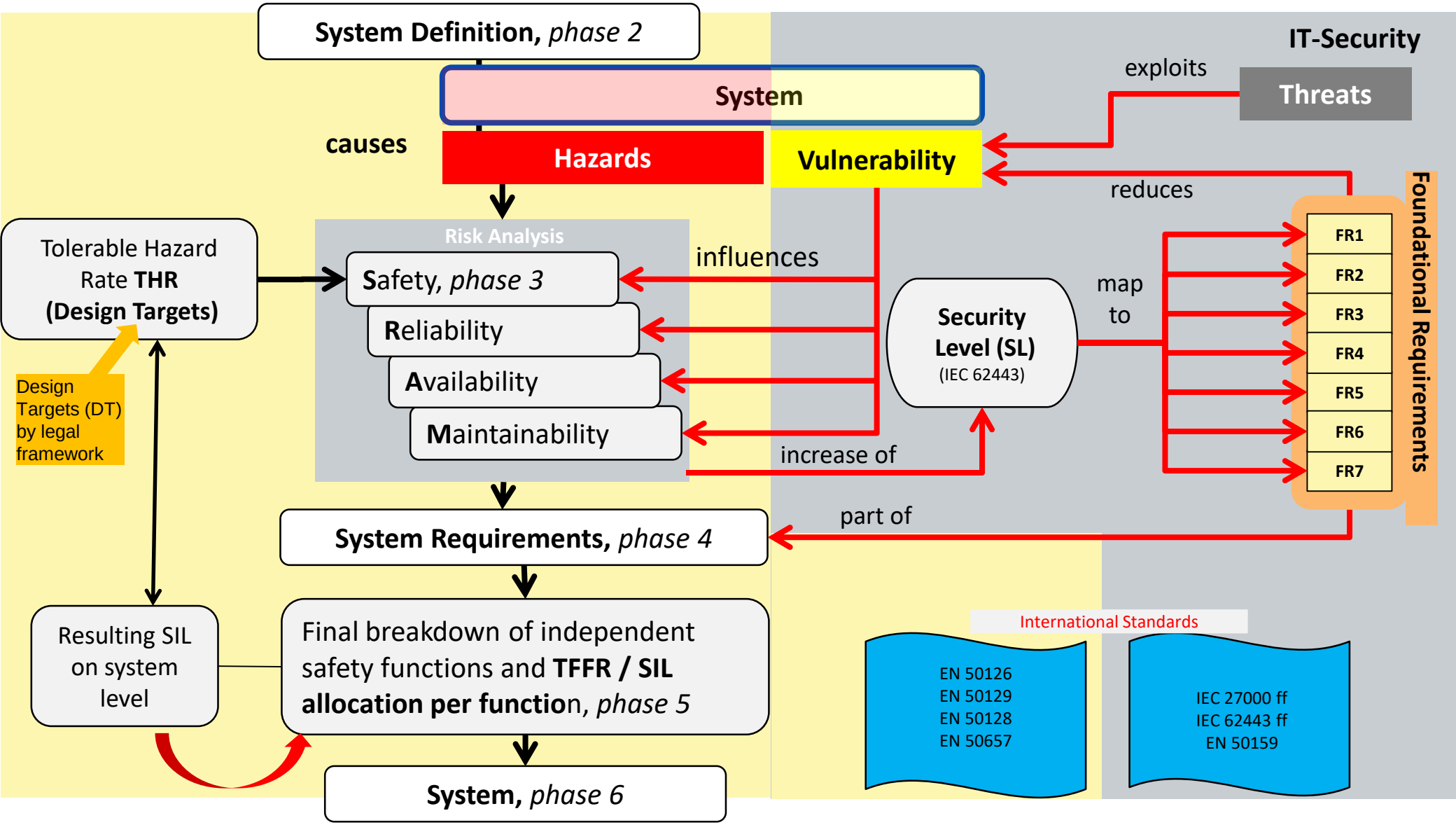
➔ The result works, but it was discovered, that duplicate work was done

Current ongoing investigations on how much the new Security process can be integrated in our well-established Safety process

- Vulnerability vs. Hazard

- Safety Requirements vs. Security Requirements

Lessons Learned



Thank you for your attention

http://fahrweg.dbnetze.com