Challenges in Securing Railway Signalling

CyberSecurity4Rail Conference 2017
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

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

Humans/Environment

Technical System

Source: IEC Draft Guide 120 Edition 1
Security for Safety – Shell Concept
Required Security Applications

- Authentication and key exchange
- Secure asset and configuration management
- Reaction to critical events
- Data logging and aggregation
- Physical access detection
- Data filtering

Safety
Security-Applied Design

Operating Center

Security Center

ETW-ZE
MDM
Technology Center

ETCS

WAN

Central PKI

SIEM

AD

AAA

Network Monitoring

Diagnosis

SDI-DS

admin

WAN

Aux. Systems (Doc.)

System

Network Monitoring

Crypto

DB
NETZE

Neighbor Tech. Center

Technology Center

Interlocking System

Field Element Area

Field Element Area

Housing Alerts

Object Controller

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

System Definition, *phase 2*

- **Hazard Definition**
  - **Tolerable Hazard Rate (THR)**
    - Design Targets (DT) by legal framework
  - System
    - **Risk Analysis**
      - Safety, *phase 3*
        - **Reliability**
        - **Availability**
        - **Maintainability**
    - **Vulnerability**
  - **IT-Security**
    - Threats
      - Exploits
      - Reduces
      - Maps to
        - **Foundational Requirements**
          - FR1
          - FR2
          - FR3
          - FR4
          - FR5
          - FR6
          - FR7
      - Increase of
        - Part of
  - **International Standards**
    - EN 50126
    - EN 50129
    - EN 50128
    - EN 50657
    - IEC 27000 ff
    - IEC 62443 ff
    - EN 50159

**System Requirements, *phase 4***

**Final breakdown of independent safety functions and TFFR / SIL allocation per function, *phase 5***

**System, *phase 6***

DB Netz AG | Christian Schlehuber | I.NPS 5 | 2017-10-04
Thank you for your attention