Der Mythos vom geschlossenen Netz
IT-Sicherheit für Leit- und Sicherungstechnik
1. Introduction
2. Closed and open Networks
3. New Features - New Threats
4. Security for Safety
5. Security Operations
6. Remaining Challenges / Outlook
Introduction
Railway / current challenges

Biggest business premises in Germany - with public access
• 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)
➤ Security is an upcoming challenge

Evolution of transport
• Autonomous driving and platooning
• Flexible travel concepts (Uber, etc.)
➤ Railways also have to evolve to keep track!

Source: DB-Mediathek
New Legislation – IT-SiG / NIS

Railway is part of our everyday life

- 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

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

Source: Bundesamt für Sicherheit in der Informationstechnologie
Network Categories

B.1 Categories of transmission systems

Subclause 6.3 identifies three categories of transmission system:

- Category 1 – Closed transmission systems, where all essential properties of the system are under the control of the safety-related system designer, and a simplified set of safety requirements can be defined;
- Category 2 – Open transmission systems where, although the transmission is not fully under the control of the safety-related system designer, the risk of malicious attack can be considered negligible;
- Category 3 – Open transmission systems where there is opportunity for malicious attack, and cryptographic defence measures are required.

Table B.2 – Threat/Category relationship

<table>
<thead>
<tr>
<th>Category</th>
<th>Repetition</th>
<th>Deletion</th>
<th>Insertion</th>
<th>Re-sequence</th>
<th>Corruption</th>
<th>Delay</th>
<th>Masquerade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cat. 1</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Cat. 2</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>+</td>
<td>++</td>
<td>++</td>
<td>-</td>
</tr>
<tr>
<td>Cat. 3</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

Key
- Threat can be neglected.
+ Threat exists, but rare; weak countermeasures sufficient.
++ Threat exists; strong countermeasures required.

Source: Excerpts from EN 50159
Network Categories (what to do)

Gleiche IBs:
- Security Gateways (SG)

Untersch. IBs:
- Security Translator (ST)

Quelle der Grafik: SIEMENS
Agenda

1. Introduction
2. Closed and open Networks
3. New Features - New Threats
4. Security for Safety
5. Security Operations
6. Remaining Challenges / Outlook
Interlocking Architecture ESTW (since 1988/1999)
Evolution of Signalling Networks - SCI-XX

- Introduce modularization
- Break monolithic structure
- Prevent vendor lock-in
- Facilitate COTS products
- Reduce cost

Standard Communication Interfaces (SCI-XX) are key for enabling modularization and break up of monolithic structures
New Features

ESTW-NeuPro (DSTW) ➔ euLynX
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

Strong requirements for low latency for networks

- Only 50ms for complete communication
- < 5 ms for security operations

Loss of availability
# Agenda

1. Introduction
2. Closed and open Networks
3. New Features - New Threats
4. Security for Safety
5. Security Operations
6. Remaining Challenges / Outlook
Current Architecture Design
Security for Safety:
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
Security for Safety: Merits of the Security Shell

**Safety**
- Maintain safety functionality
- Change in long intervals (decades)
- Distinguish safety incidents

**Security**
- Uncouple from safety homologation
- Change in short intervals (days)
- Distinguish security incidents
- Catch security attacks

**Interface**
KPI/QoS: latency, bandwidth
## Agenda

1. Introduction
2. Closed and open Networks
3. New Features - New Threats
4. Security for Safety
5. Security Operations
6. Remaining Challenges / Outlook
Security Controls vs. Reality
Excursus: What about USB sticks?

USB RUBBER DUCKY

$44.99

The USB Rubber Ducky is a key as a generic flash drive. Computers, keyboards, and monitors can be used to drop reverse shell payloads, craft attacks against users, and many other automated penetration tester and systems.

Since 2010 the USB Rubber Ducky has been used by hobbyists, penetration testers, and hackers as the first IT automation dev-board. It has since grown into the Keystroke Injection Attack Platform, which captured the imagination of hardware language, formidable hardware experts, and enthusiasts alike.
Security Operations

Security Applications (in focus)

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

Safety
Security Operations
Overview and important roles

Important roles:

- Monitoring
- Security Incident Response
- Patch-&Vulnerability Management
- Security Intelligence & Threat Forecast
- Vulnerability Scans
- Consulting

Figure 8-2  A Sample SOC Organization Structure
Security for Safety: (Remaining) Challenges

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

• Preventive Vulnerability Scanning / Penetration Testing
  • Is my system capable of a scan?
  • May the test result in outages?

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

• Forensic Analysis
  • Analysis vs. Fast Recovery

→ Topics currently addressed in research projects
# Agenda

1. Introduction
2. Closed and open Networks
3. New Features - New Threats
4. Security for Safety
5. Security Operations
6. Remaining Challenges / Outlook
Outlook: Securing Legacy Systems

- **Operation Area**
  - Documentation
  - Loupe
  - Area-View
  - Area-View

- **ESTW-Z (TSO)**
  - EKIR
  - I/O and Display System
  - Workstation
  - Security-Gateway

- **ESTW-A (Track Field)**
  - Area Controller 1
    - Point
    - Axle Counter
  - Area Controller 2
    - Signal
    - Track Circuit

- Railway Operation Center

---

DB Netz AG | Christian Schlehuber | I.NVI 1(S) | 2019-03-18
Outlook: An integrated platform for Safety and Security

- Integration on a single hardware platform
  - Specialized redundant hardware as a base with security anchor
  - SIL 4 operating system that provides virtualization and a Separation Kernel
- Separated Compartments provide isolation
  - Safety-Functions: provide “normal” functionality of signaling component
  - Safety-Functions: provides encryption, filtering, malware detection, etc.
- Virtualization enables seamless operation while updating
Conclusion

- Security is becoming more and more important for Railway Systems
- Safety and Security have different mindsets
- A “Security for Safety Shell” may be a solution
  - It separates security from safety
  - It is a compromise between safety’s durability and security’s flexibility
  - It enables adaption of necessary security measures without interfering with the homologation
- Security Operations and raising awareness are major points
- Networks are a starting point for increasing the security of a system
- Virtualization may be the technology to solve several issues
Thank you for your attention

M.Sc. Christian Schlehuber
Lead of CyberSecurity R&D / Expert CyberSecurity

DB Netz AG
I.NVI 1(S) - IT-Security Management
Weilburger Str. 22
60326 Frankfurt am Main

christian.schlehuber@deutschebahn.com
www.deutschebahn.com

http://fahrweg.dbnetze.com