ÖBB INFRA

Protecting Railway Systems against Cyber Attacks

Christian Sagmeister


Agenda

- **Automatic Train Operation**
- **Cyber Security**
- **Security in Operational Management**
- **Future Challenges**

Automatic Train Operation

Grades of Automation	
GOA 1	Driver takes control of train (start, stop, doors opening and closing)
GOA 2	Half automatic railway traffic. Driver takes only control of doors closing and opening
GOA 3	Train accompanied by personnel, driverless train operation
GOA 4	Unattended train operation / manless train operation MTO), no personnel on the train

Automatic Train Operation

Efficient improvements

- Reducing costs
- Increasing operational availability
- More performance on track

Hazard

- No train driver
  → no local fallback in case of critial incidents

Automatic Train Operation (ATO)

Automatic Train Operation – Impacts

Business and Customers

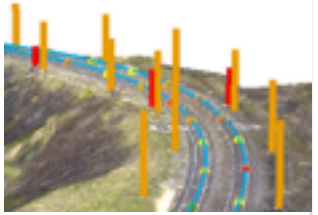
- Punctuality
- Energy efficiency
- CO2 emissions

Operational Management

- Operational security
- Higher precision of train operation
- Avoidance of unscheduled stops

Technical Development

- Automatisation of train operation (e.g. conflict management)
- Sensors on the vehicles
- Passenger information system



Agenda

- Automatic Train Operation
- Cyber Security
- Security in Operational Management
- Future Challenges

Major Cyber Security Challenges for ATO

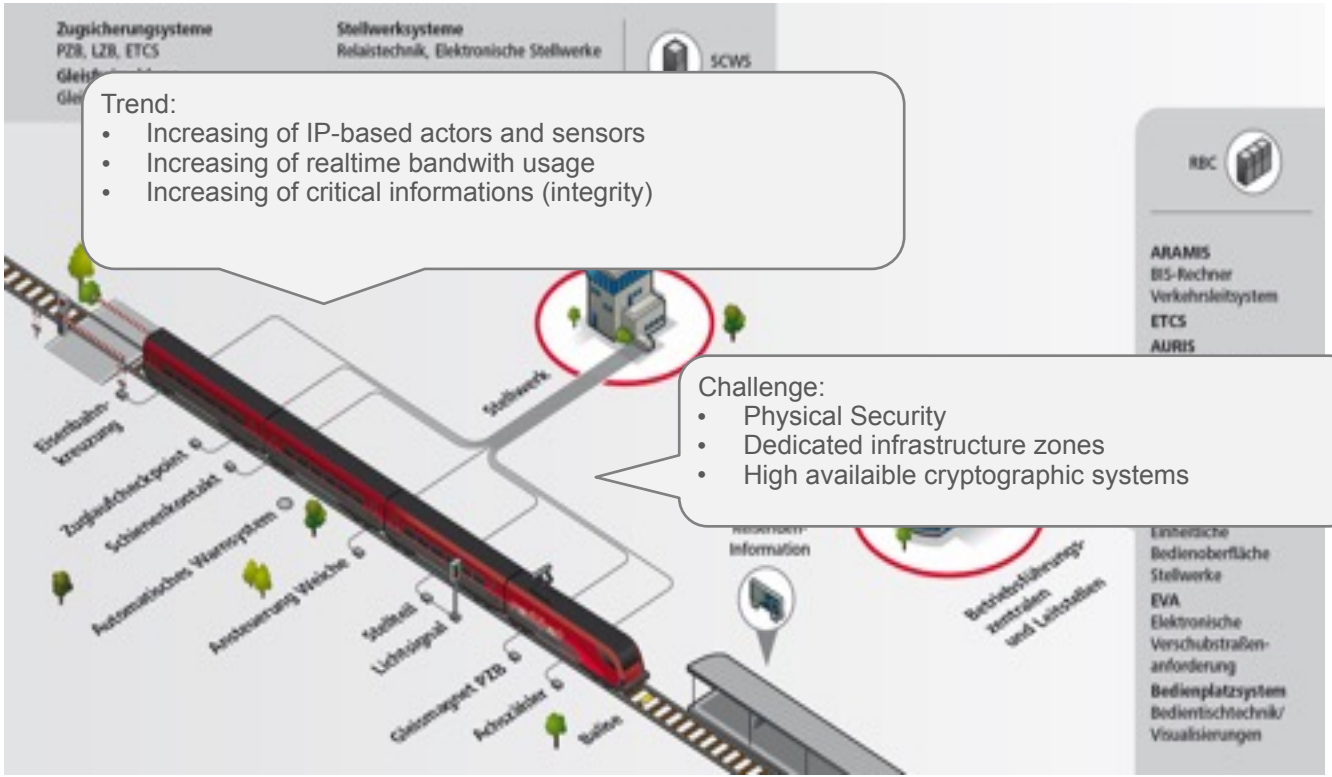
Operational / Daily Business

- Delays
- Constructions
- Environmental damages

Security & Safety

- Security exceptions triggerd by operational units
- Java Versions (ETCS Key Management System)
- GPS and GSMR-Jammer
- Fast Malware releases & legacy on train systems

Complex system landscape



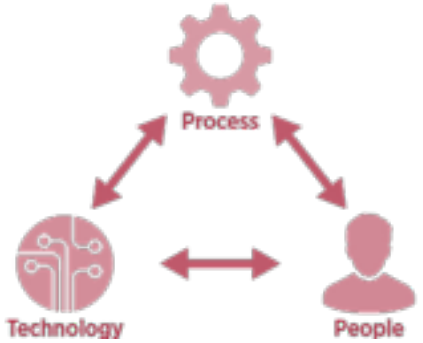
Agenda

- Automatic Train Operation
- Cyber Security
- Security in Operational Management
- Future Challenges

Cyber Security – centralized management

Network segmentation

- Protocol change on segment entry
- Port access control
- Identity management & strong authentication



SIEM

- Central logging & alarming
- Linking user & assetinformation
- Baselining & anomaly detection
- Threat intelligence

Cyber Security – operational risks

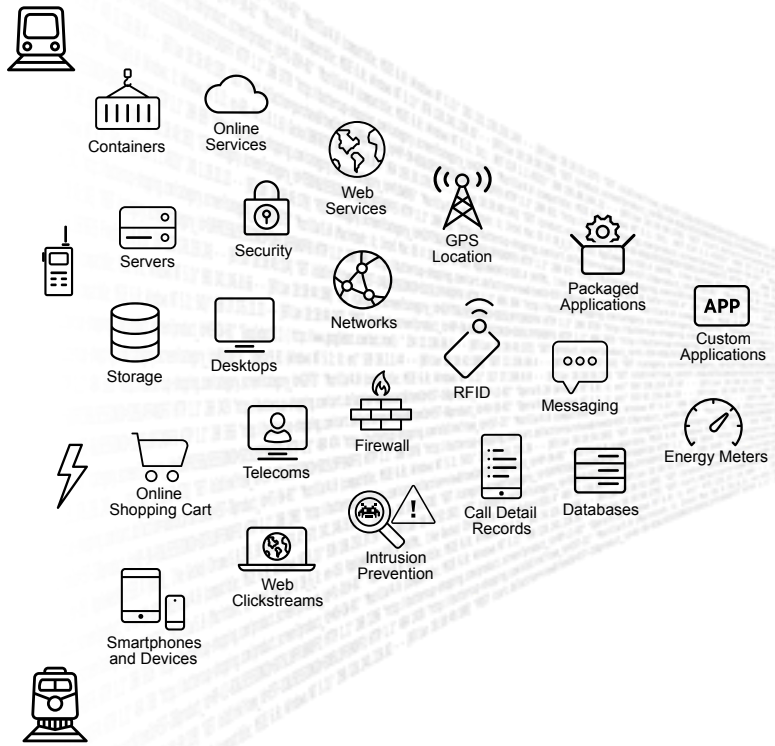
Failure Potential

- Network enviroment stretched and need for high interconnectivity between segments
- Increasing complexity for troubleshooting
- Legacy systems & time pressure at implemention time lead to unwanted exceptions

Hazards of Cyber Attacks

- Industrial spionage
- Denial of service / blackmail
- Political motivation

Future Challenges



Education

- New skills in railway sector needed
- Awareness trainings

Emergency Measures

- Emergency plans / Training
- Backup and redundancy tests

Train Operation & Cyber Defense

Organisation

- Strict guidelines for operational procdures and implemenations
- Risk managament
- Vulnerabilty assessment / pentesting

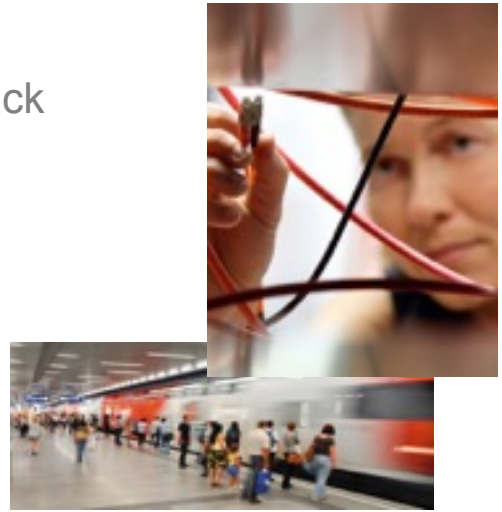
Agenda

- Automatic Train Operation
- Cyber Security
- Security in Operational Management
- Future Challenges

Hazards of Cyber Attacks

Non legacy and IoT

- Patch cycle too short for systems on track
- Incompatible device-mix
- Many „intelligent“ devices



Interfaces

- Intrusion by onboard-Wireless
- Secure System Interface need

Emergency tasks

- How to clean a moving System in case of an incident?
- How to connect remote by an “stolen” Interface?

Thank you for your attention!