Eisenbahn-Bundesamt

Cybersecurity aspects in German Railway Sector

Safety & IT Security in the German Railway Sector Protecting Germany’s most critical transportation

Dr. Frank WERNER
IT Security Taskforce
German Federal Railway Authority (EBA)

5th ENISA-ERA Conference on Cybersecurity in Railways

Overview

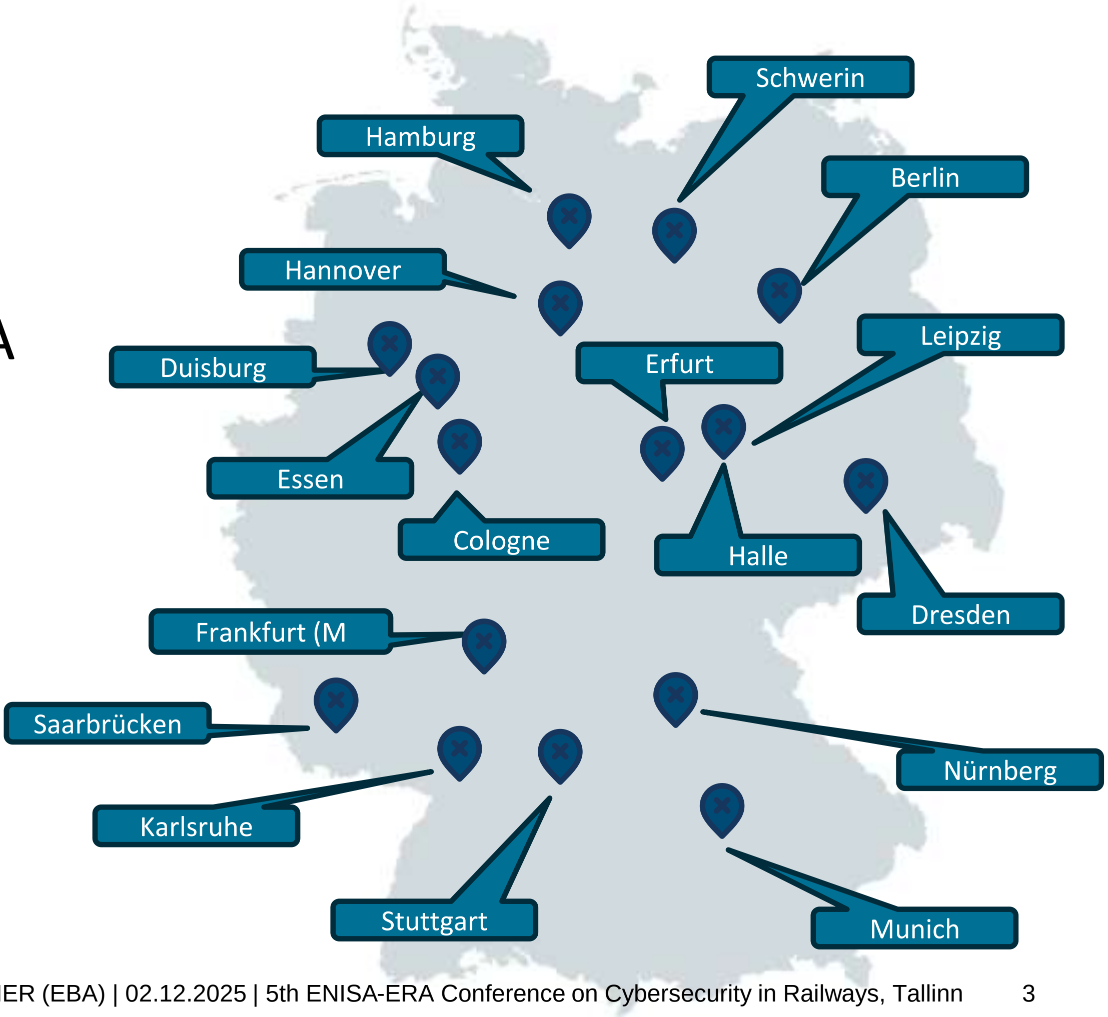
1. IT Security Taskforce at German Federal Railway Authority
2. German Railway Landscape
3. Project I: oKMC - Online Key Management Center
4. Project II: „EDIS“ – A New Dispatch and Scheduling System

Eisenbahn-Bundesamt

IT Security Taskforce @EBA

Who we are..

… a team of security experts responsible for supervising the German railway infrastructure.



Our Duties (excerpt)

- Railway IP network (**sbbIP**), etc.
- **Digital Interlocking System** (DSTW)
- Digital Rail Germany (DSD)
- **IT Security Components**
- NOC and SOC of DB InfraGo Track
- Participation in **railway vehicle approvals**
- **Innovative railway projects** (e.g., driverless operation, oKMC, security software/network, etc.)
- German Centre for **Railway Research**
- Policy work, own and impactful laws, **regulations**, **standards** (several standardization bodies)
- **Recognition and supervision of testing bodies**
- Participation in **safety approvals** and **approve security experts**
- **International cooperation** (ERA, ENISA, EU Commission, supervisory authorities in Europe)
- **Regular Exchange** with the BSI and other NSAs, i.e., BAV (Switzerland), EPSF (France), NSA Rail Belgium, SJT (Norway), Tarficom (Finland)

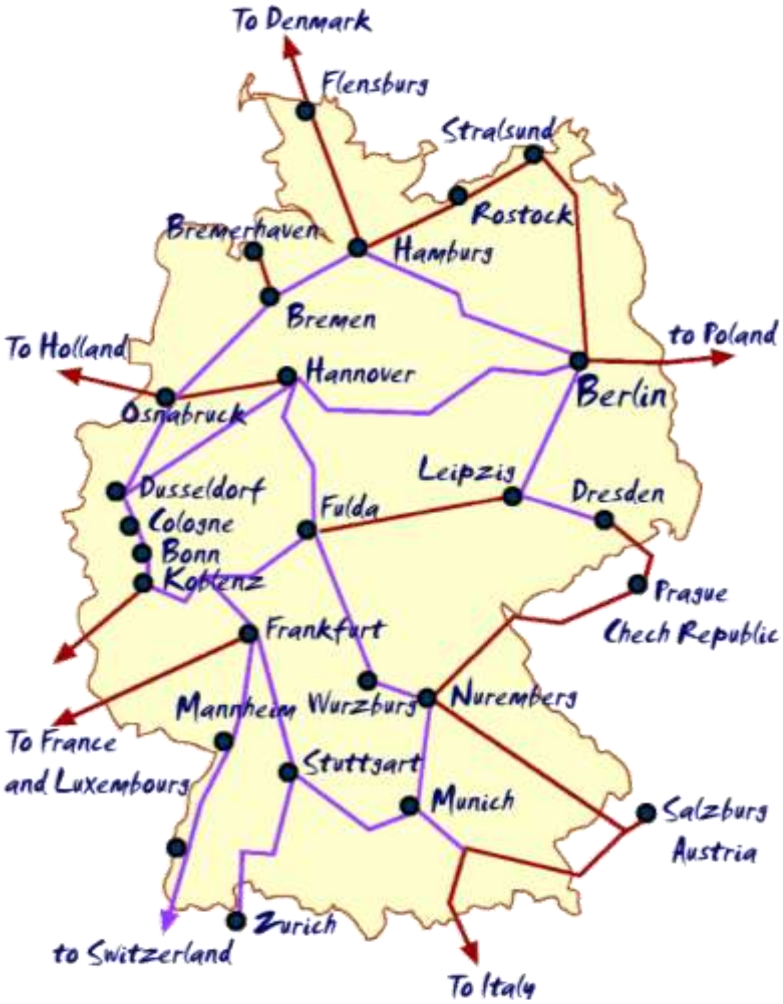
The German Railway Network

Facts

- >36.000 km of rail network (2 429M passengers, 179,8M t goods)
- Railways essential for Germany's transport network and energy transition (CO_2 reduction)
- Links to many European countries

Security

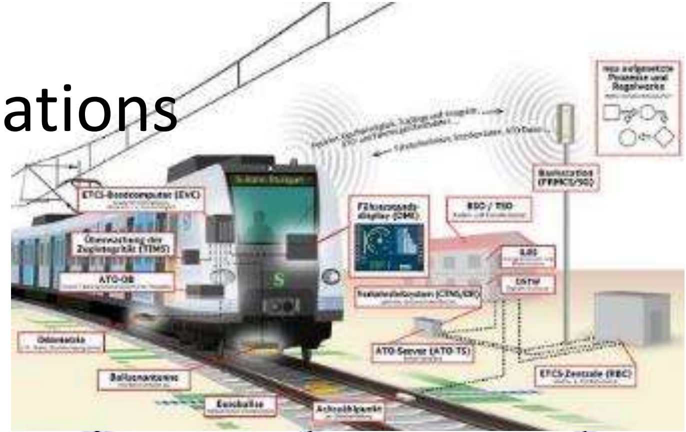
- Increasing digitalization introduces new risks and threats
- Integrated view of safety and cybersecurity is essential
- To ensure safety, risks must remain at an acceptable level

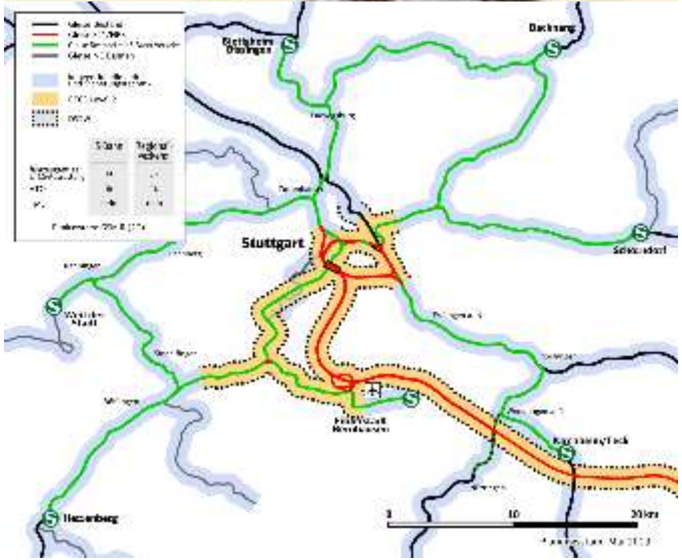


Source: German Rail Map: Train Routes in Germany. Photo: James Martin

Examples of Highly Networked Applications in Railway (excerpt)

- Digital Rail Germany (DSD)
- Digital Node Stuttgart (DKS)
- Digital Interlocking System Mertingen-Meitingen (in operation)
- bbIP and sbbIP
- Distributed Power System (DPS) for freight driving in Sandwich position
- and more..





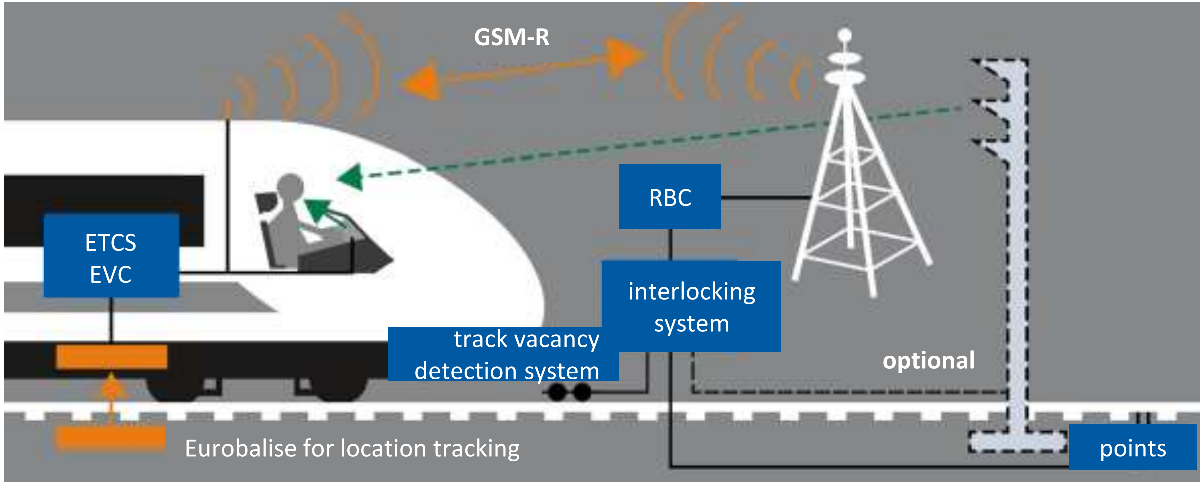
Project: oKMC

Introduction Online Key Management Centre (oKMC) for ETCS

Online Key Management Centre

Purpose of the oKMC

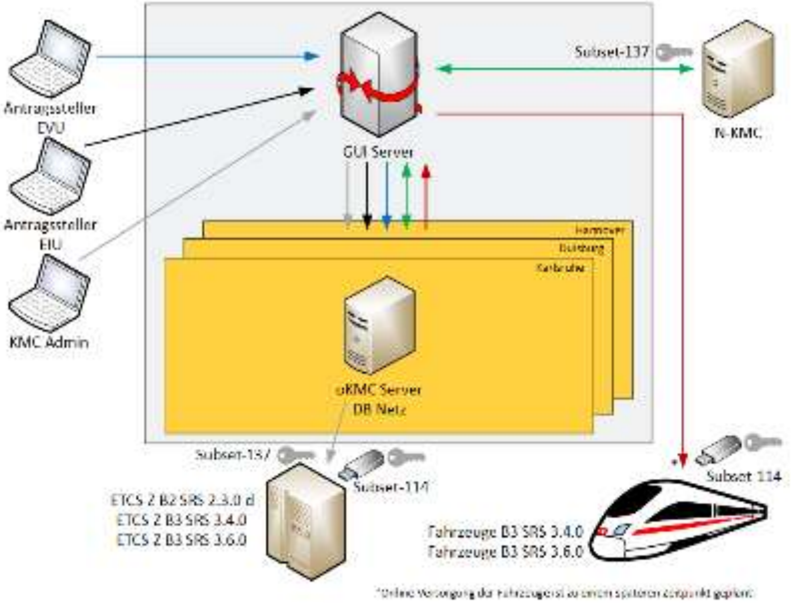
- Securing the connection: vehicle with cryptographic keys ←→ETCS control centre
- Automation of key distribution and reduction of key management processing times
- Replacement of the offline KMC



IT Security Concerns: oKMC

- **3 geo-redundant locations** (in Karlsruhe, Duisburg, and Hanover) with server/VMs connected via **VPN**
- **HW security module** (HSM) for encrypting ETCS keys and storing encryption keys
- **firewall** connects the VPN to the cloud, where the oKMC user interface is located
- oKMC realizes more **secure handling** than KMC

→ Network security: network disruption
→ System redundancy in case of failure
→ System security



Project: Introducing „EDIS“ – A New Dispatch and Scheduling System

A New Dispatch & Scheduling System – “EDIS”

EDIS – A New Dispatch and Scheduling System*)

- Real-time overview of operation states (delay, rail allocation)
- bundling of all relevant timetable and infrastructure information
- Uniform operating standard in all DB InfraGO operations centres
- Basis for implementing the EU standard TAF/TAP-TSI for digital train identification (cross-border rail transport and Europe-wide train scheduling)

Foto: DB InfraGO AG/Tanja Spang

*) Source: EDIS-Deine Bahn, Bahn Verlag GmbH, 10/2025, p. 20 f

IT Security Concerns: EDIS

- **Integration** of external systems must be ensured via VPN
- **Authentication** of users with identify and access management
- Central network coupling-node without network **redundancy**
- **Access restrictions** to the facilities
- **Redundancy** of IT services/network sufficient?

  Availability: systems properly distributed over AZs ensure critical services remain active?

  → 99,9% availability (approx. 9h downtime p.a.)

Definition of 18 topic-specific focus areas

Penetration test

Networks

Asset management

Attack detection

Application security

Redundancy

Miscellaneous

Basic operations

Roles & rights

EAS (input/output system, clients in the field)

System hardening & cryptography

Vulnerability scan

Identity & access management

Virus protection

Logging

IT emergency

Test & release

Eisenbahn-Bundesamt

Questions & Answers

Dr. Frank WERNER

German Federal Railway Authority

IT Security Taskforce

Web www.eba.bund.de

E-mail WernerF@eba.bund.de