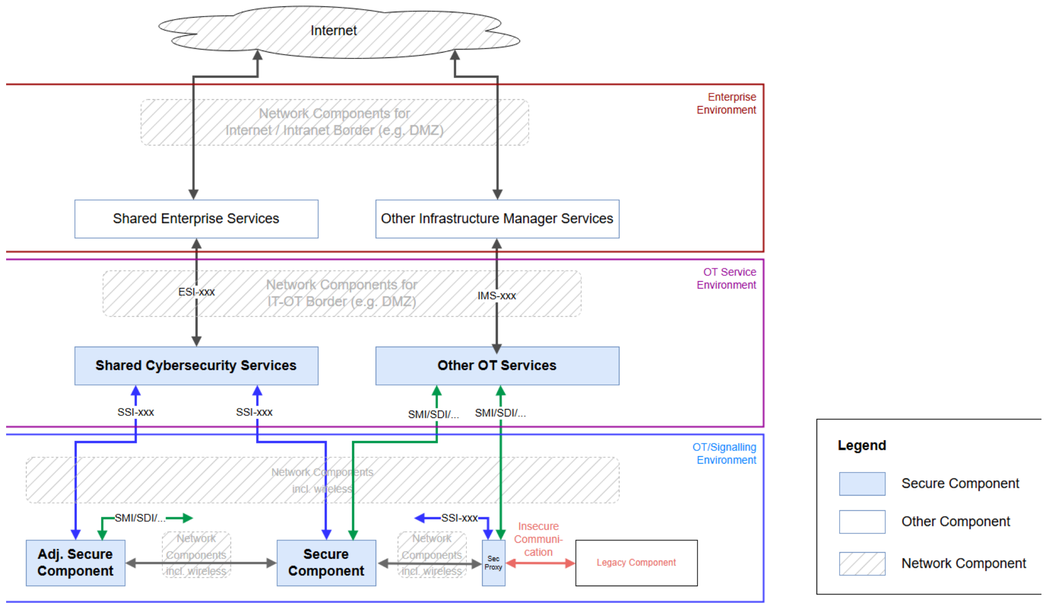
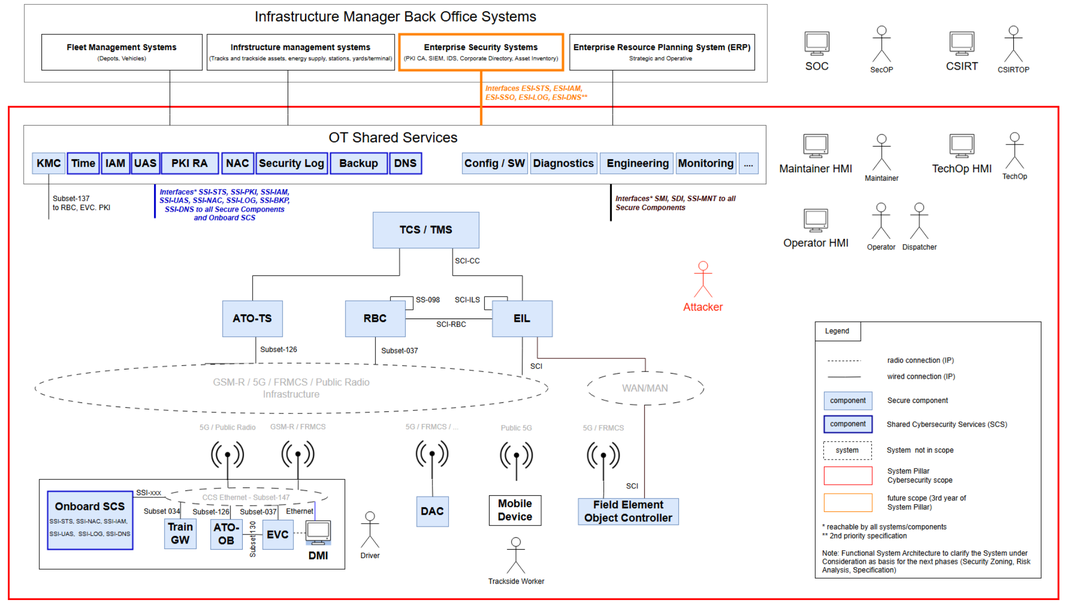
Cybersecurity

The Cybersecurity team is responsible of defining central cybersecurity requirements. This includes aspects as generic security architecture, threat and risk assessment, security requirements for system under consideration, definition of interfaces to Shared Cybersecurity Services, compliance to standards and legal obligations, and secure program requirements.

Security – System Under consideration (generic architecture)



Cyber Security Architecture for the System Pillar scope



The Cybersecurity Team focuses to support the **“Harmonized European Rail Operation”** migration plateau with

- Security gap analysis and security support for all System Pillar Domains, ERA TSIs and other rail-specific topics
- Defining migration concepts (esp. for ERA TSI CCS) and aligning security certification processes with existing certification processes.
- Maintaining the System Pillar Cybersecurity specification

Cybersecurity

Oliver Knapp *(DB)* **– Railway Lead**
Markus Wischy *(Siemens)* **– Supplier Lead**

Lead STIP Deliverables

- **STIP_75: Shared Security Services Specification -** 2024
- **STIP_76: Secure Communication Specification -** 2024
- **STIP_77: Secure Program Req. -** 2024
- **STIP_78: Secure Component Specification** - 2024

Deliverables Request for Service (SC2.4)

D01	**Shared Security Services Specification -** Q3 2025
D02	**Secure Communication Specification** – Q3 2025
D03	**Secure Program Req.** – Q3 2025
D04	**Secure Component Specification** – Q3 2025
D05	**Other TSI** – Q3 2025
D06	**Cooperation with System Pillar Domains and Innovation Pillar** – Continuous

Latest Achievements, Challenges and Design Decisions *(to be filled periodically by the domain)*

- **Latest Achievements:**
  - **Publication of SP Cybersecurity Specification:** specification is available on EU Rail System Pillar Website: https://rail-research.europa.eu/horizontal-tasks/ (Section Security)
  - **Intensified communication with various stakeholders in regards to cyber security:** DAC (SP Task 4), FRMCS (UIC), Transversal, SP Architecture Group

- **Domain Current challenges:**
  - **Integration of Cyber Security in other TSIs**: Setup of communication for work estimation and planning still ongoing. Alignment with ERA on prioritization

Expected outcomes for sector review in the next 3 months

Finish of security gap analysis for all TSIs

- finalize security gap analysis for all eight TSIs

Accompanying communication for the document release

- Plan for dissemination of specification publication on conferences and publications