Status & Results
X2Rail-1, X2Rail-3, X2Rail-5

Markus A. Wischy

2nd ERA-ENISA Conference on Cybersecurity in Railways
December 1st 2022

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No: 826141

Cybersecurity in S2R – IP2 TD2.11 timeline

X2R3 WP8 Cyber Security:

X2R3 WP8 & WP 9 Cyber Security

X2R5 WP 11 Cyber Security

TD2.11 Participants

Key stakeholders of EU rail automation:
railway operators, solution providers & research organizations

Main results of X2Rail-1 (2015-2018)

- **Selection of the Security-by-Design Standard**

  IEC 62443-4-1 – Secure product development requirements and **IEC 62443-4-2** – Technical security requirements for IACS components are proposed as the standard framework for the "Secure-by-design" standard in the railway domain"

- **Application of the risk assessment to the railway signalling system**

  The Target Security Level (SL-T) evaluation resulted on SL-T vectors with SL3 on all (13) but two zones

Results of X2Rail-3 / WP8

1. Definition of a **generic cybersecurity architecture** and the security environment for next generation rail automation products (shared security services)

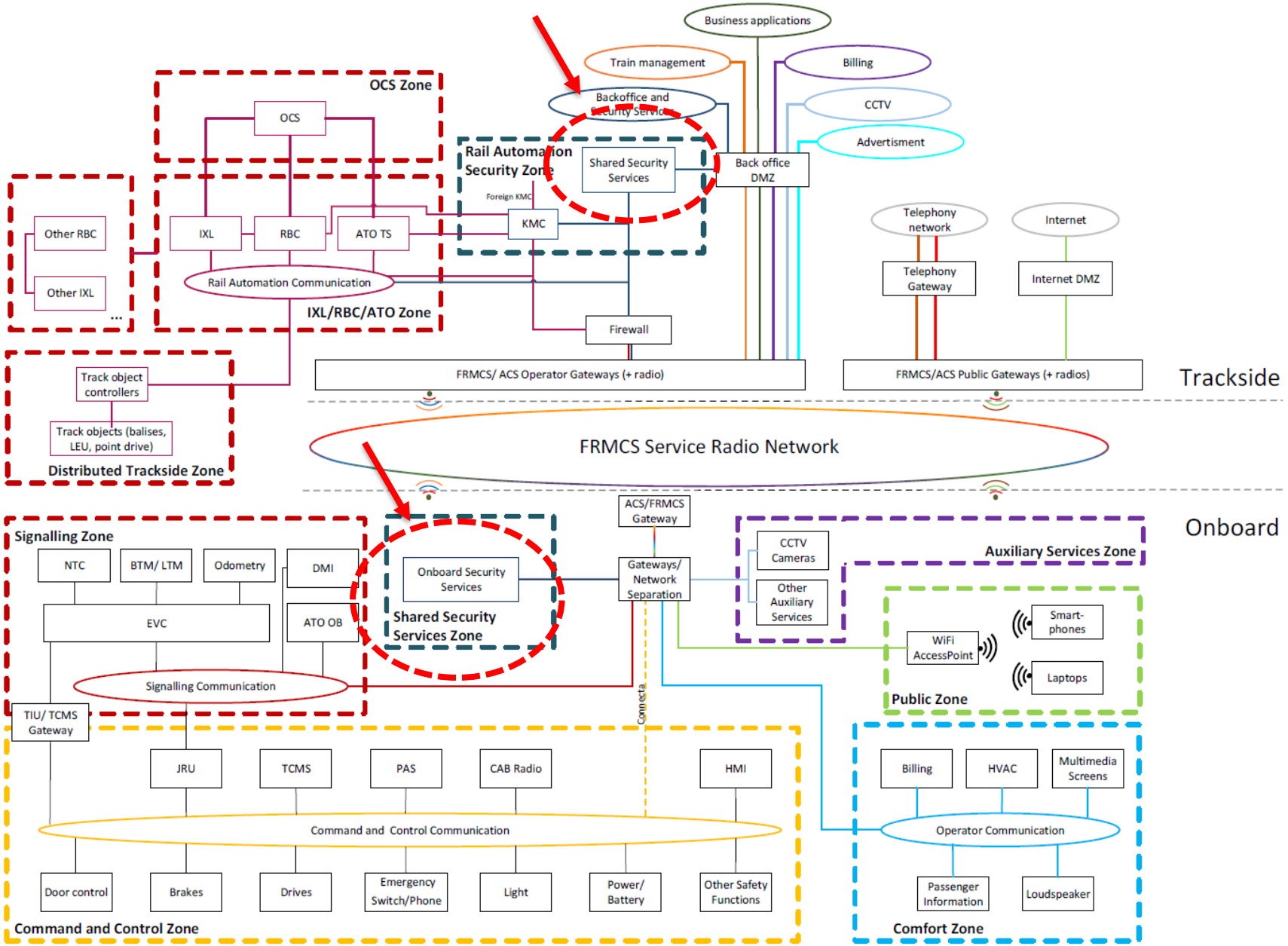
2. Investigation and **selection of protocols** to shared security services for interoperability

3. Define **protection profiles** for trackside, on-board and ACS components based on selected protocols for shared security services

4. Update of **risk assesment method** (optimisation over X2Rail-1), reports on IoT security, security for legacy systems and securing resilient architectures

Generic cybersecurity architecture

- For next generation products and new rail automation systems
- Incorporating FRMCS, ATO and CONNECTA (TCMS) topics (ERA CCS TSI revisions)
- Definition of shared security services



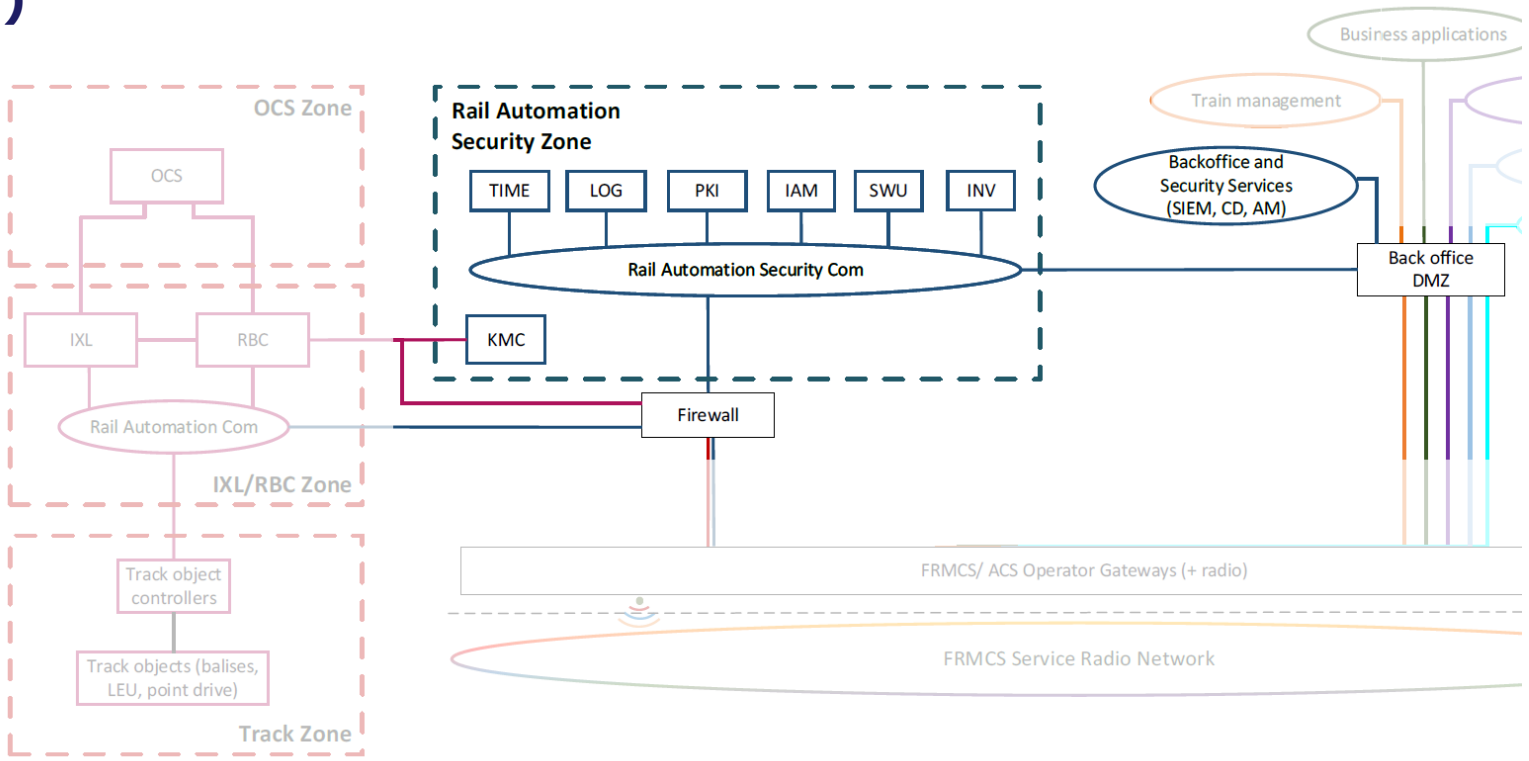
Security Environment for EU-Interoperability

Mandatory services

- System-wide time service **(TIME)**
- Central Logging **(LOG)**
- Security Incident and Event Management **(SIEM)**
- Intrusion Detection / cont. monitoring **(IDS)**
- Identity and Access Management **(IAM)**
- Backup **(BKP)**
- Asset Inventory **(INV)**

Highly recommended services

- Public key management **(PKI)**
- Central Software Update **(SWU)**



Protection profiles

Release of protection profiles

- Trackside components
- On-board components
- Radio (ACS) components

Horizon 2020 European Union Funding for Research & Innovation

X2Rail-3

Project Title:	Advanced Signalling, Automation and Communication System (IP2 and IP5) – Prototyping the future by means of capacity increase, autonomy and flexible communication
Starting date:	01/12/2018
Duration in months:	36
Call (part) identifier:	H2020-S2RJU-CFM-IP2-01-2018
Grant agreement no:	826141

Deliverable D8.2-3b

Protection Profile - Trackside components

Due date of deliverable	Month 24
Actual submission date	02-12-2020
Organization name of lead contractor for this deliverable	SMO
Dissemination level	PU
Revision	Final release

https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-3

Results of X2Rail-3 / WP9

- D8.1: Simplified Risk Assessment
- D9.1: Product & System security verification best practices
- D9.2: Supply-chain security approach for railways
- D9.3: Security evaluation of X2Rail demonstrators (ATO, CONNECTA, VCTS, ACS, SWOC) & Holistic Approach – (consortium internal)
- D9.4: Railway CSIRT feasibility study

X2Rail-5 Cybersecurity

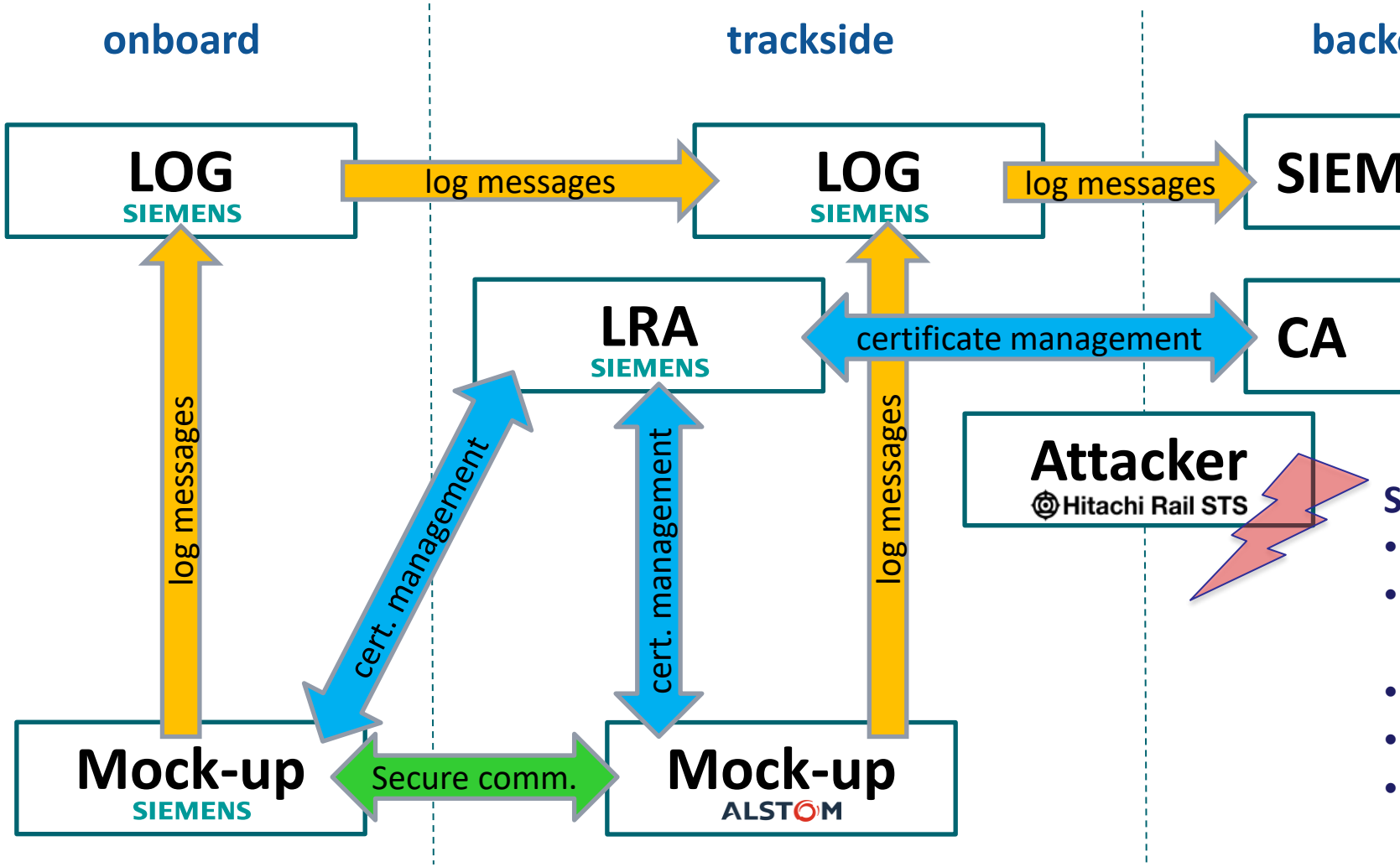
Project duration X2Rail-5 WP 11 Cybersecurity

- Oct 2021 – May 2023

Planned X2Rail-5 WP 11 Cybersecurity publications

- D11.1: Cybersecurity assessments of other X2Rail demonstrators
- D11.2: Integrated technical demonstrator report
- D11.3: CSIRT/ISAC prototype verification, validation and test (internal)
- D11.4: Summary statement from the perspective of an operator(s)
- D11.5: Recommendations on railway systems' cyber resilience

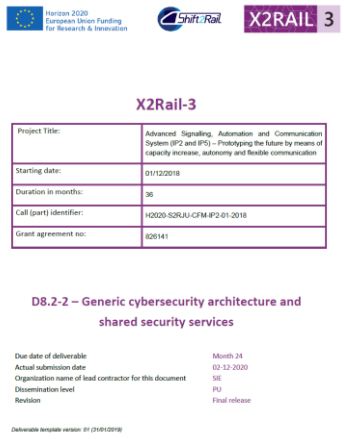
D11.2: Security Demonstrator Overview (ERA TSI CCS 2022 scope)



Shared Security Services

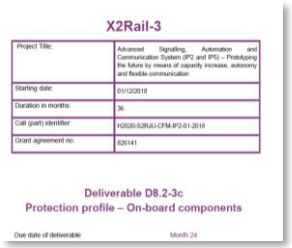
- LOG: Central Logging Service
- SIEM: Security Incident and Event Management
- CA: Certificate Authority
- LRA: Local Registration Authority
- TIME: System-wide time service (not shown)

Successful dissemination

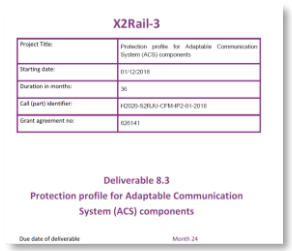


Cybersecurity architecture and shared security services

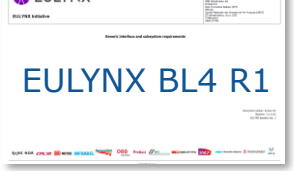
PP Trackside



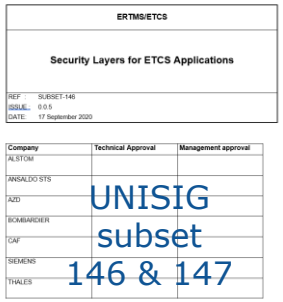
PP Onboard

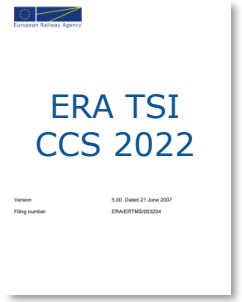


PP ACS



UNISIG





ER JU - System Pillar
Cyber Security

Overview

Europe's Rail – System Pillar overview

- **Started 10/2022, planned until 2028**
- **Four tasks (railway system, CCS, TMS, DAC/FDTO), >12 tasks, appr. 200 experts**
- **Innovation pillar: 28 projects**

- **Cyber Security Domain members:**
  - **Rail operators: DB, ÖBB, EUG (SBB, Trafikverket), SNCF, RFI, NS**
  - **Rail industry: UNIFE (Siemens Mobility, Alstom, AZD, CAF, Hitachi, Mermec, Thales)**

Security activities for System Pillar task 1, 2, 3 and 4

- **Conduct as-is analysis** (review existing cyber security specifications: X2Rail, UNISIG, EULYNX…)
- **Contribute to CCS concept of operation** (security operation processes (2-1, 2-4), people training and capacity building)
- **Contribute to migration concept** (technical and process migration steps related to security)
- **Contribute target system architecture**
  - add security to functional, logical and physical target architecture
  - create security risk analysis on reference architecture using TS 50701 (reuse existing risk analysis)
  - add zone & conduits to architecture and define IEC 62443-3-3 security levels for each zone
  - define IEC 62443-4-2 component level requirements
- **Create technical security TSIs**
  - CCS secure product specification / protection profile (4-1, 4-2)
  - Shared security infrastructure specification
  - Secure communication interface specifications

Input / Output of System Pillar – Cyber Security

X2RAIL 1
X2RAIL 3
X2RAIL 5

Cyber Security deliverables

EUROPEAN UNION AGENCY FOR RAILWAYS
UNISIG

UNISIG subset 146 & 147
TSI CCS 2022

EULYNX

Baseline 4 R1 – Detailed security requirements

ertms
OCORA
FRMCS
Future Railway Mobile Communication System

System Pillar - Task 1-4

Europe's Rail

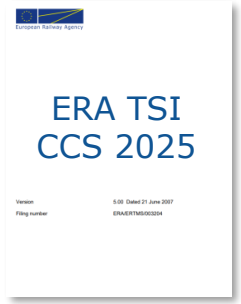
System Pillar
Cyber Security

ER JU SP Cyber Security
Mirror Groups (UNISIG, EUG,…)

Shared security services spec
CCS component security spec
Secure communication spec

Draft security specifications (12/23)

Innovation Pillar
Selected demonstrator project



ER JU System Pillar – Cyber Security

Inputs for Cyber Security activities

Deliverables from different Security Specification Groups will be used and integrated in the target specification.

These inputs are coming from:

- **X2Rail-1, 3 and 5:** Generic cybersecurity architecture for rail domain (based on IEC 62443-3-3), protection profiles for trackside (based on IEC 62443-4-2), onboard and radio components, guidelines for various security processes, several risk assessments
- **UNISIG CyberWG:** Subset 137 (Online Key Management), Subset 146 (End-to-End Secure Communication), Subset 147 (One-common bus lower layers)
- **EULYNX Security cluster:** Detailed specification (Phase 5) for security for EULYNX 4 R1 (aligned with X2Rail and UNISIG), risk assessments on IXL domain
- **ERTMS Security Core Group:** Requirements for Existing and Future System for ERTMS.
- **OCORA:** Requirements for CCS onboard on logical architecture level
- Input from other organizations on different levels from CONNECTA, ER-ISAC and FRMCS

Cyber Security Milestones 2023/24

- **Finalize as-is analysis**
  - document existing work (12/2022)
  - finalize reviews + recommendation of reuse of existing work (04/2023)
- **Support / contribute to other domains**
  - interconnect, find out what's the target (12/2022)
  - define what input should be given (03/2023)
  - provide input to groups (depends on domain)
- **Start risk analysis process (01/2023)**
- **First draft of specifications**
  - shared security services / security management (06/2023)
  - innovation pillar (~12/2023)
- **Final input for TSI 2025 (~12/2024)**

More informartion

https://rail-research.europa.eu/about-europes-rail/