ERJU System Pillar
Cyber Security Domain

ERA ENISA Conference 2024, Lille
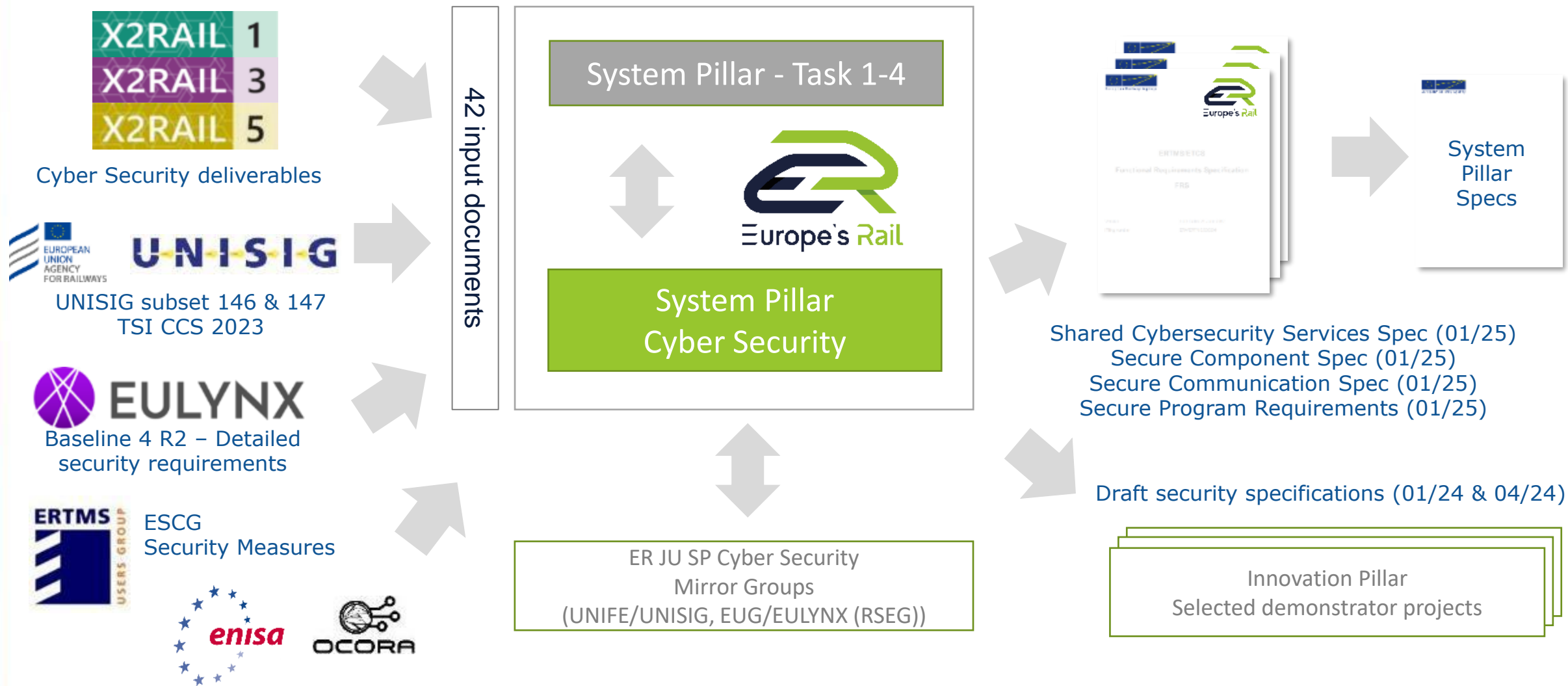
PART 1

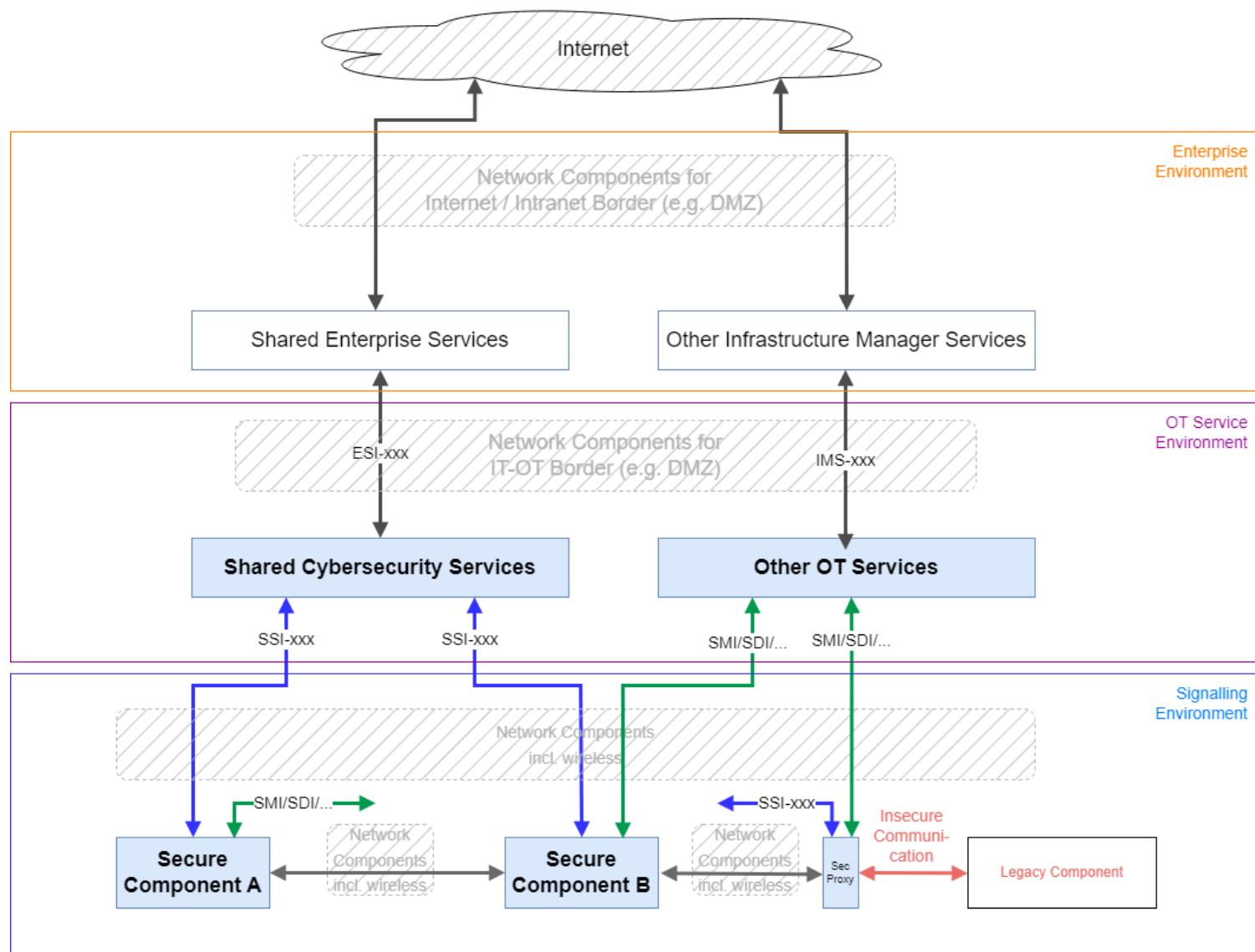# WORKFLOW
CYBER SECURITY ARCHITECTURE
TAXONOMY
# SPECIFICATION DETAILS

Workflow of System Pillar – Cyber Security

X2RAIL 1
X2RAIL 3
X2RAIL 5

Cyber Security deliverables

UNISIG subset 146 & 147
TSI CCS 2023

EULYNX

Baseline 4 R2 – Detailed
security requirements

ERTMS
ESCG
Security Measures

enisa   OCORA

42 input documents

System Pillar - Task 1-4

Europe's Rail

System Pillar
Cyber Security

ER JU SP Cyber Security
Mirror Groups
(UNIFE/UNISIG, EUG/EULYNX (RSEG))

System
Pillar
Specs

Shared Cybersecurity Services Spec (01/25)
Secure Component Spec (01/25)
Secure Communication Spec (01/25)
Secure Program Requirements (01/25)

Draft security specifications (01/24 & 04/24)

Innovation Pillar
Selected demonstrator projects

Generic Cyber Security Architecture

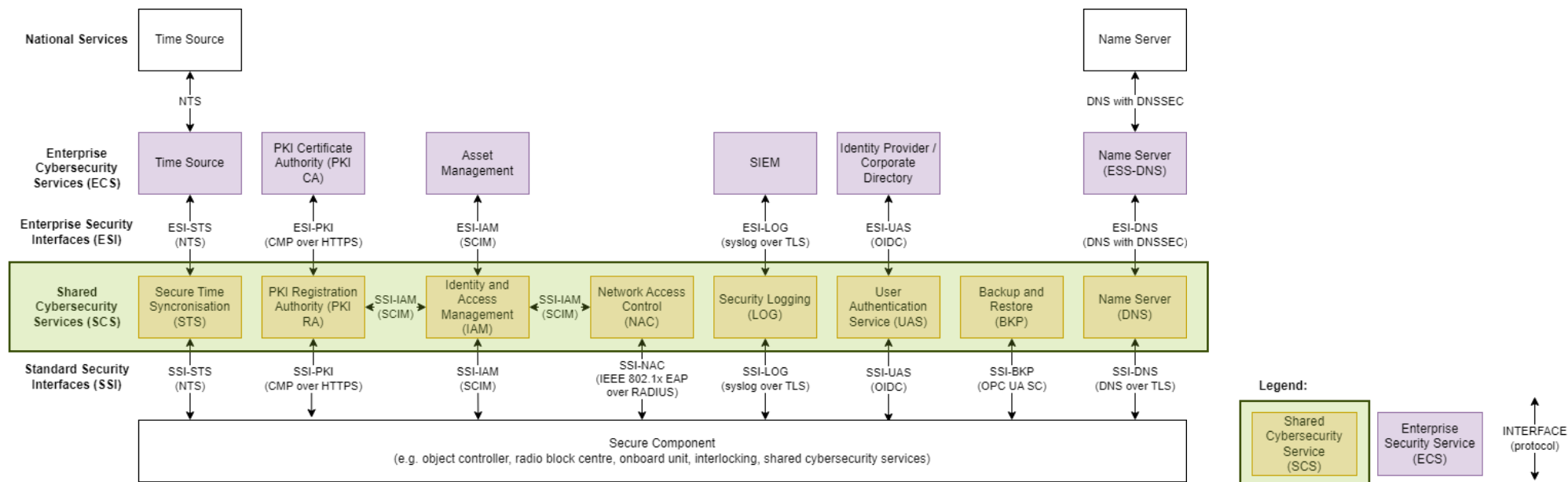# Cyber Security Architecture (System Pillar scope)
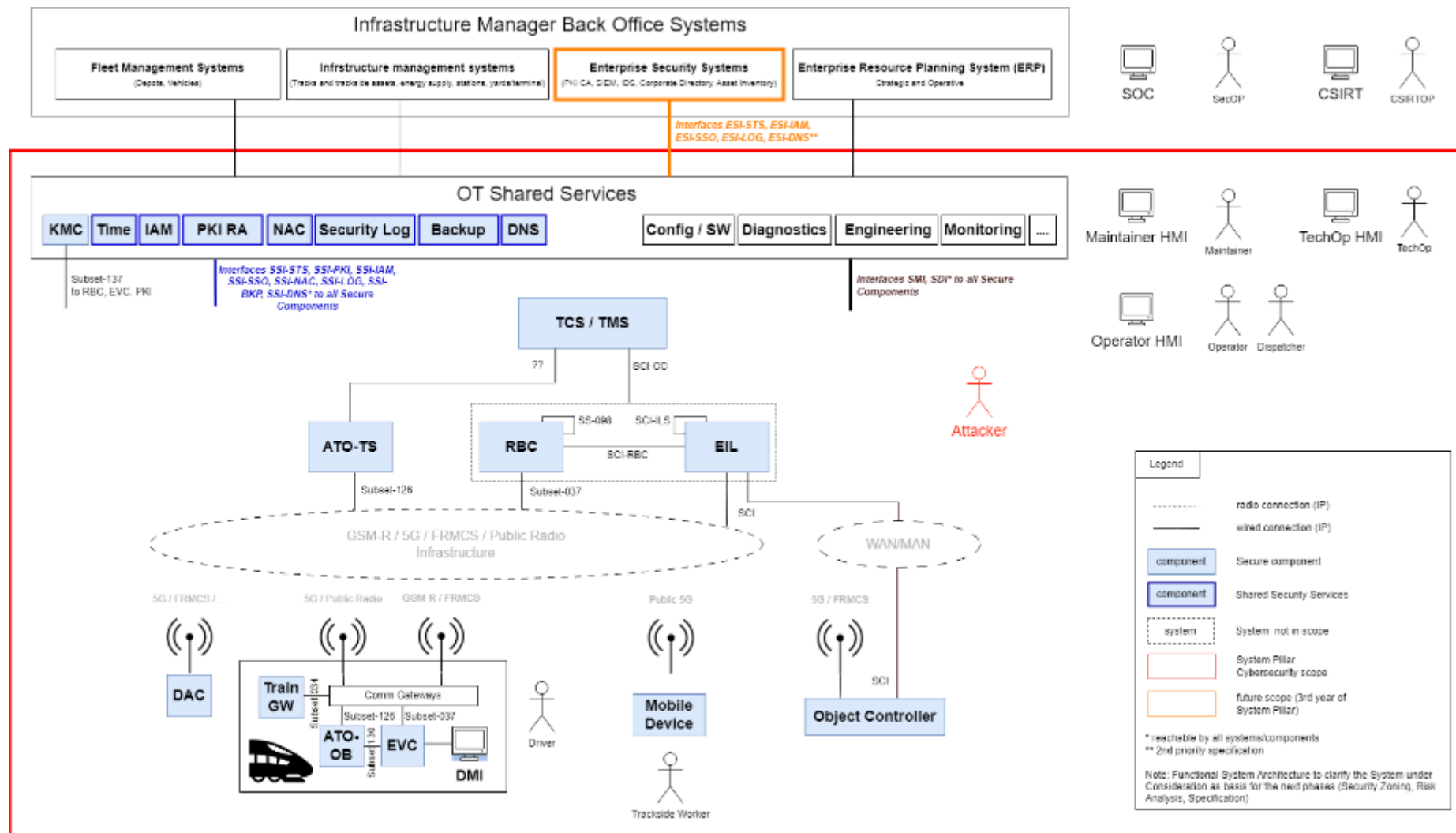
System Pillar Cybersecurity Specifications
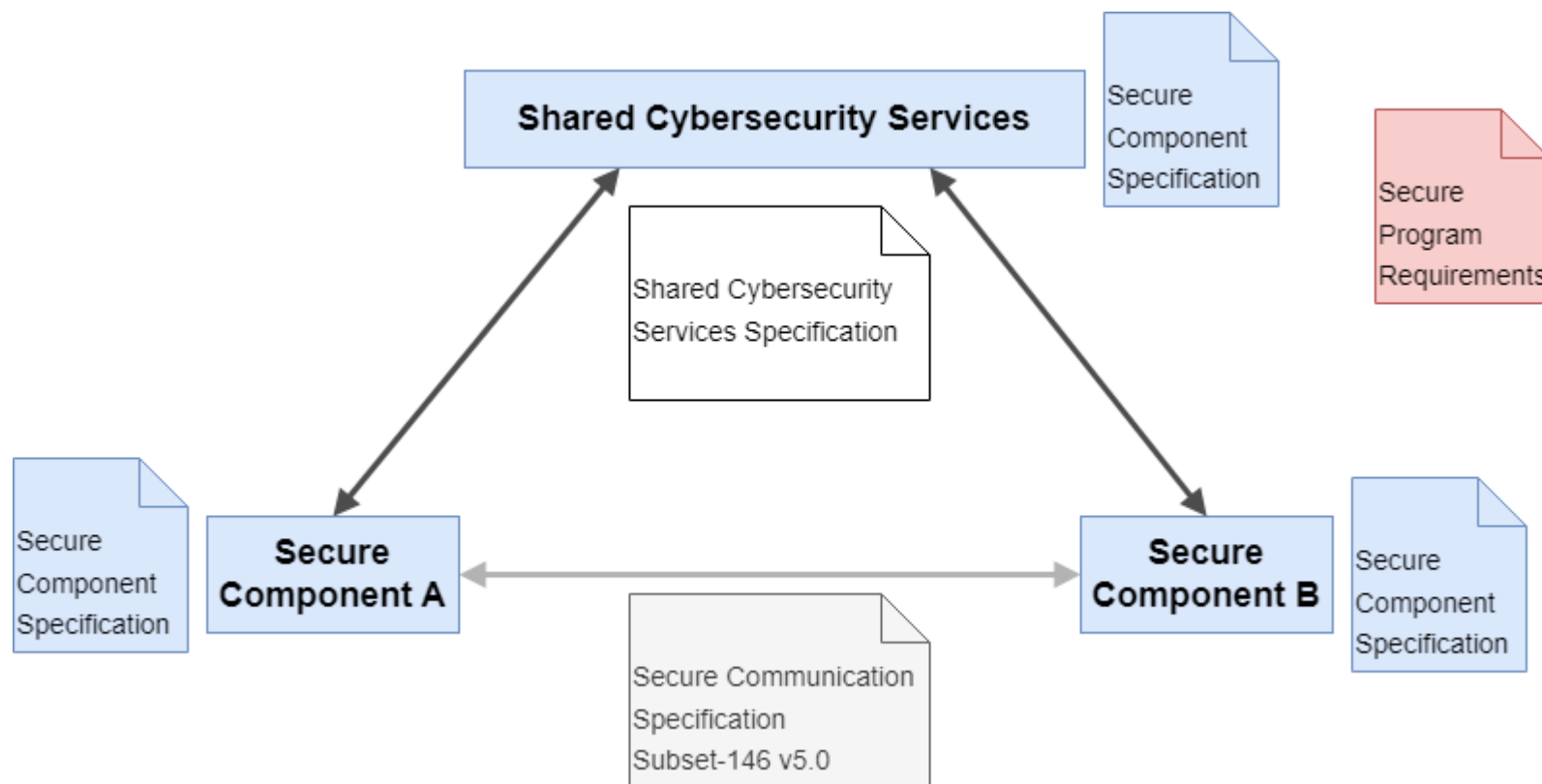
Overview of Key Terms and security specifications (from Taxonomy)

Shared Cybersecurity Services

Schematic of Shared Cybersecurity Services with Interfaces

Definition of 8 services & interfaces

1. **STS**: Secure Time Synchronisation
2. **PKI**: Public Key Infrastructure
3. **IAM**: Identity and Access Management
4. **NAC**: Network Access Control

5. **LOG**: Security Logging
6. **UAS:** User Authentication Service
7. **BKP**: Backup and Restore
8. **DNS**: Domain Name System

PART 2

EUROPEAN SECURITY COMPLIANCE TIMELINE OUTLOOK

European Security Compliance

European legislation	Standards

NIS 2	CSA	CRA	RED	ISO 27001	IEC 62443 2-1, 2-4, 3-3, 4-1, 4-2	CLC/TS 50701 IEC 63452

Target: compliance and full tracing

ER JU System Pillar Cyber Security specifications

Secure Component Spec	Shared Cybersecurity Service Spec	Secure Communication Spec

Security Program Requirements (Application Guidelines)
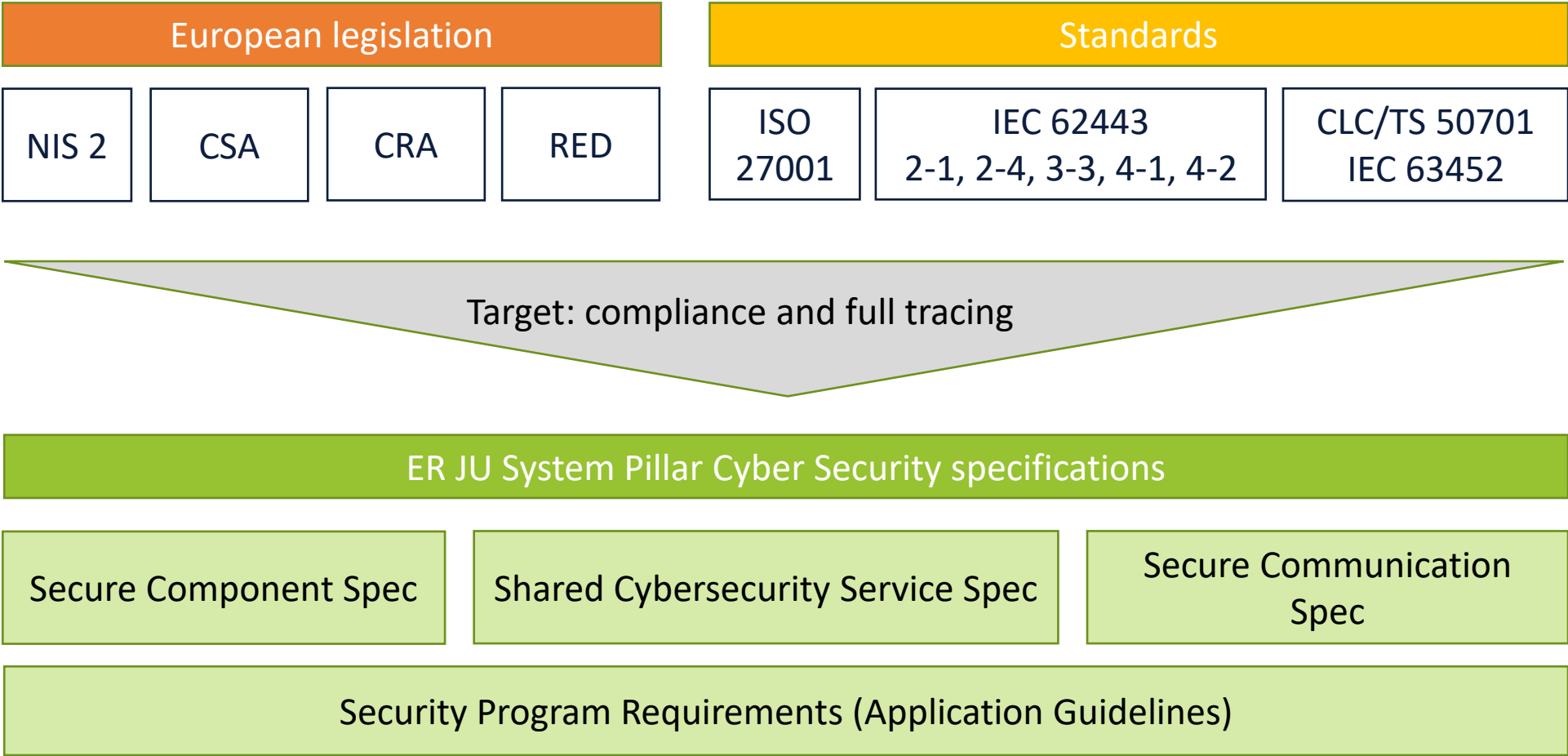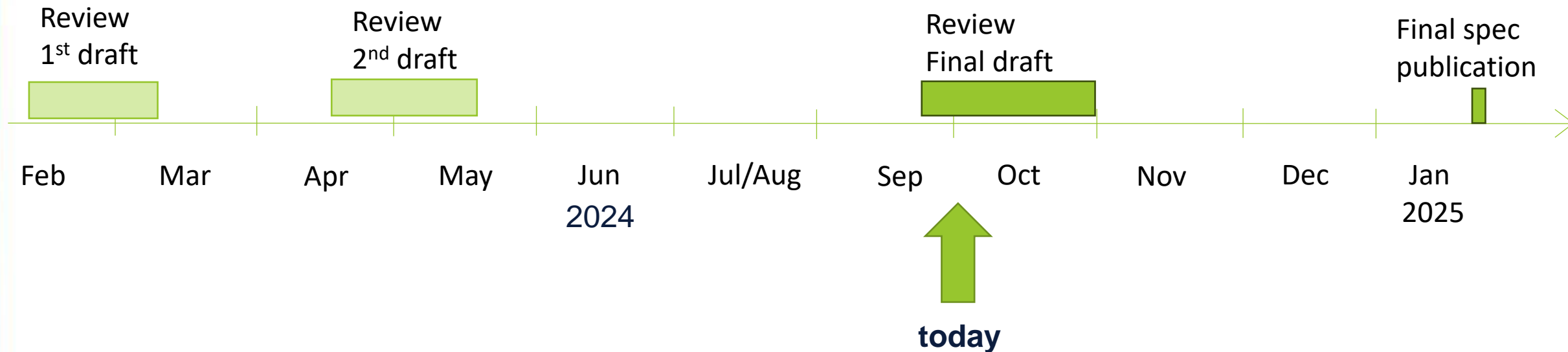
Timeline review System Pillar Cyber Security Specs

Upcoming review (final draft):

- Final draft comment submission: Oct 31st 2024
  Specs and review sheet available at:
  https://rail-research.europa.eu/wp-content/uploads/2023/10/ERJU_SP_CyberSecurity_Review3_Files.zip

- Public Q&A every Friday 8.30am – 9.00 am, from Oct 18th to Nov 1st

3rd. Draft of Cybersecurity Specs

Review 1st draft		Review 2nd draft				Review Final draft				Final spec publication
Feb	Mar	Apr	May	Jun	Jul/Aug	Sep	Oct	Nov	Dec	Jan

2024

today

2025

# Outlook: security gap analysis and CRs for all TSIs

ERA request Q1 2024

- Conduct **gap analysis** on all TSIs and **create CRs to close the gaps**.
  - CCS TSI, TELEM TSI (former TAF/TAP), OPE TSI, LOC&PAS TSI, WAG TSI, INF TSI, ENE TSI, RINF, ERATV/EVR

System Pillar response

- Current focus is System Pillar scope (CCS, IXL, object controllers, TMS, DAC)
- Review and comments **done for Telematics TSI**
- **Start gap analysis** from Q1 2025 onwards
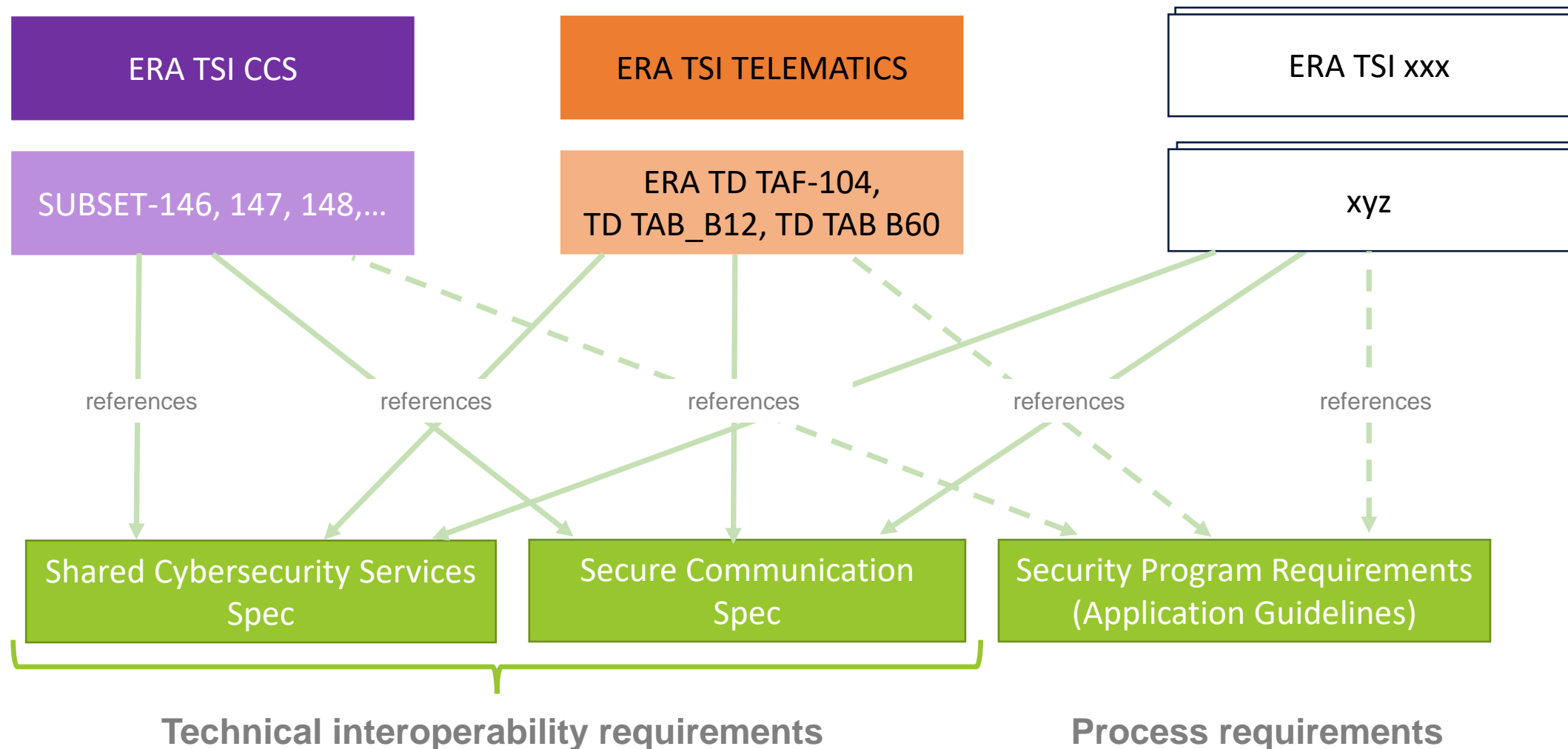
Outlook 2025 and beyond: planned additional topics

IEC TC9 PT 63452

- Liaison with IEC TC9 PT 63452

- Alignment of the specifications (system pillar specification as a **reference system** for IEC PT 63452)

IEC 63452	System Pillar Cybersecurity deliveries
SO-02-01: Railway system model	Generic Security Architecture
SO-03-01: Railway zone model	Zone Model
SO-04-01: Specification of shared security services	Shared Cybersecurity Services Specification
ZR-01,02,03,04: Zoning and risk assessment	Generic threat and risk analysis
ZR-04-11: Cybersecurity requirements specification	Secure Component Spec (outline as of Annex G.4) Secure Communication Spec Security Program Requirements (ApplGuide)
(correct references as of 22/08/2024)	

Innovation Pillar FP2 R2DATO Amendment

- **Setup** of **Shared Cybersecurity Services** for Innovation Pillar projects (planned amendment)

- Cooperation with demonstrator projects (alignment, security training,…)

Review of other security related specification

- Support of MORANE 2 demonstrator with shared cybersecurity services

- Review of FRMCS v3 specs

Thank you

cybersecurity.review@ertms.be

www.rail-research.europa.eu