ER JU - System Pillar Cyber Security

Overview, Organization, Activities, Outlook

Status as of November 3rd, 2023

Agenda

1. Who we are – System Pillar – Cyber Security
2. How we work – input and output of the group
3. How we align – drafts availability and commenting periods

1. System Pillar – Cyber Security domain

System Pillar Cyber Security Mission

Mitigate security risks by defining the requirements for Rail Cyber Security in the scope of the System Pillar to support interoperability across Europe, to reduce lifecycle cost and support a unified market for components for railway system.

Note: measure: reducing/minimizing country specific requirements
Cost reduction compared to not standard-based approach

1. Who we are
System Pillar – Cyber Security

Industry

Cyber Security Expert	Company
Markus Wischy (LEAD)	UNIFE/SMO
Daniel Gutierrez	UNIFE/CAF
Dario Principe	UNIFE/Hitachi
Dimitrios Sisiaridis	UNIFE/Alstom
David Goltzsche	UNIFE/SMO
Martin Weller	UNIFE/Thales

Mirror group: UNISIG CyberWG

Operators

Cyber Security Expert	Company
Kurt Kayser (LEAD)	DB
Richard Poschinger/ Helmut Klarer	ÖBB
Max Schubert	EUG
Ulrich Meier	SBB
Nicolas Poyet	SNCF
Erwin Kooi	NS
Stefano Cortellessa	RFI

Mirror group: EUG Security Expert Group

ER JU System Pillar – Cyber Security

2.1 How we work
Output / deliveries of Cyber Security group

Strategy

- focus on main specification first (Year 1 and 2)

Planned deliveries

Draft specification for Innovation Pillar and other SP domains (12/23)

- Secure component spec
- Shared security services spec
- Secure Process requirements

TSI input / final specification (12/24)

- Secure component spec
- Shared security services spec
- Secure communication spec
- Secure Process requirements

2.2 Input/Output of System Pillar – Cyber Security

X2RAIL 1
X2RAIL 3
X2RAIL 5

Cyber Security deliverables

EUROPEAN UNION AGENCY FOR RAILWAYS
U-N-I-S-I-G

UNISIG subset 146 & 147
TSI CCS 2023

EULYNX

Baseline 4 R2 – Detailed security requirements

ERTMS USERS GROUP

ESCG
Security Measures

OCORA

enisa

42 input documents

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 (12/24)
Secure component spec (12/24)
Secure communication spec (12/24
Secure Process requiremnets (12/24)

Draft security specifications (12/23)

Future ERA TSI CCS / System Pillar Spec

Innovation Pillar
Selected demonstrator projects

ER JU System Pillar – Cyber Security

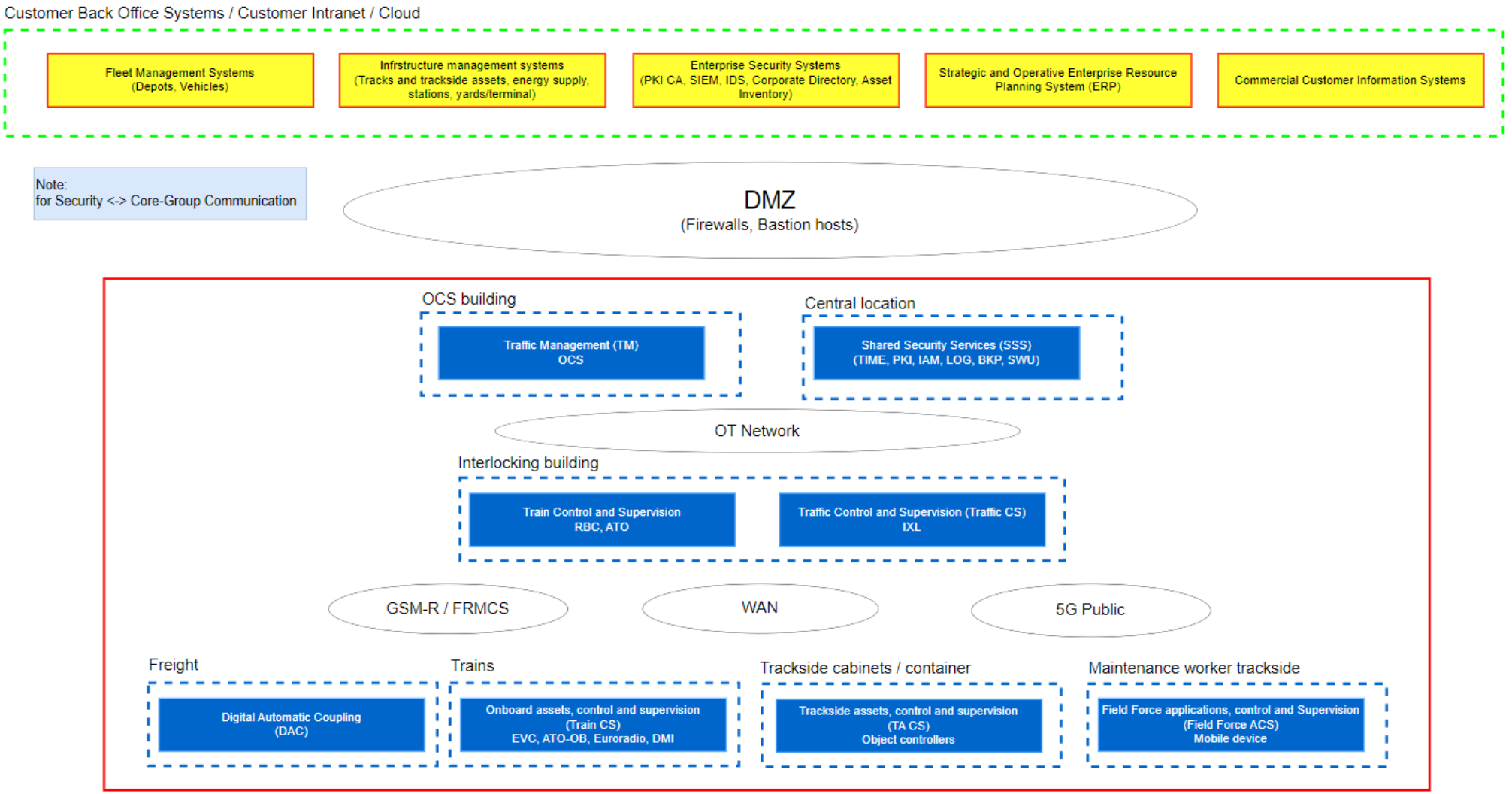
2.3 Cyber Security group Milestones 2023/24

- **Finalize as-is analysis**
  - document existing work (12/2022) **- done**
  - finalize reviews + recommendation of reuse of existing work (10/2023) – **done**
- **Support / contribute to other domains (ongoing)**
  - interconnect, find out what's the target - ongoing
  - define what input should be given - ongoing
  - provide input to groups (depends on domain) - ongoing
- **First drafts of specifications (12/2023)**
  - Draft specifications for (selected) innovation pillar demonstrators and other SP domains
- **Start risk analysis process (Q1/2024)**
- **Final specifications / input for TSI CCS update (~12/2024)**

2.4 Strategy of security group for spec development

- Timeline: for future TSI CCS update: tentative 2025, likely effective for new projects: 2027/2028
- The security specs should be stable for some time (therefore tendency for a more complete set of requirements)
- Analysis of all IEC 62443-4-2 requirements (incl. SL-4) for
  - Easy implementation (e.g. open source component available, …)
  - Cost of implementation
  - Cost of operation
- Statement for requirements not accepted for specification (with rationale why not applicable)
- Ideally, the generic security architecture, generic risk assessment and security specs create a one-stop shop / aligned package ready reusable for rail automation projects
- However, the security specs should be also fit for alternative (project specific) risk assessments.
  - For such cases, we have a clear rationale, why certain requirements are not applicable for rail automation systems/products (e.g. due to implementation issues, cost issues,…), so the TSI is still sufficient
- 100% compliance with legal technical requirements (NIS-2, CSA, CRA,…) and EN 50701 / IEC 63452
- The component security specs should also be proposed (together with IEC 62443-6-2) as cyber security certification scheme to ENISA (fulfilling the CSA requirements for critical infrastructure products)

2.5 Scope of ER JU System Pillar – Cyber Security

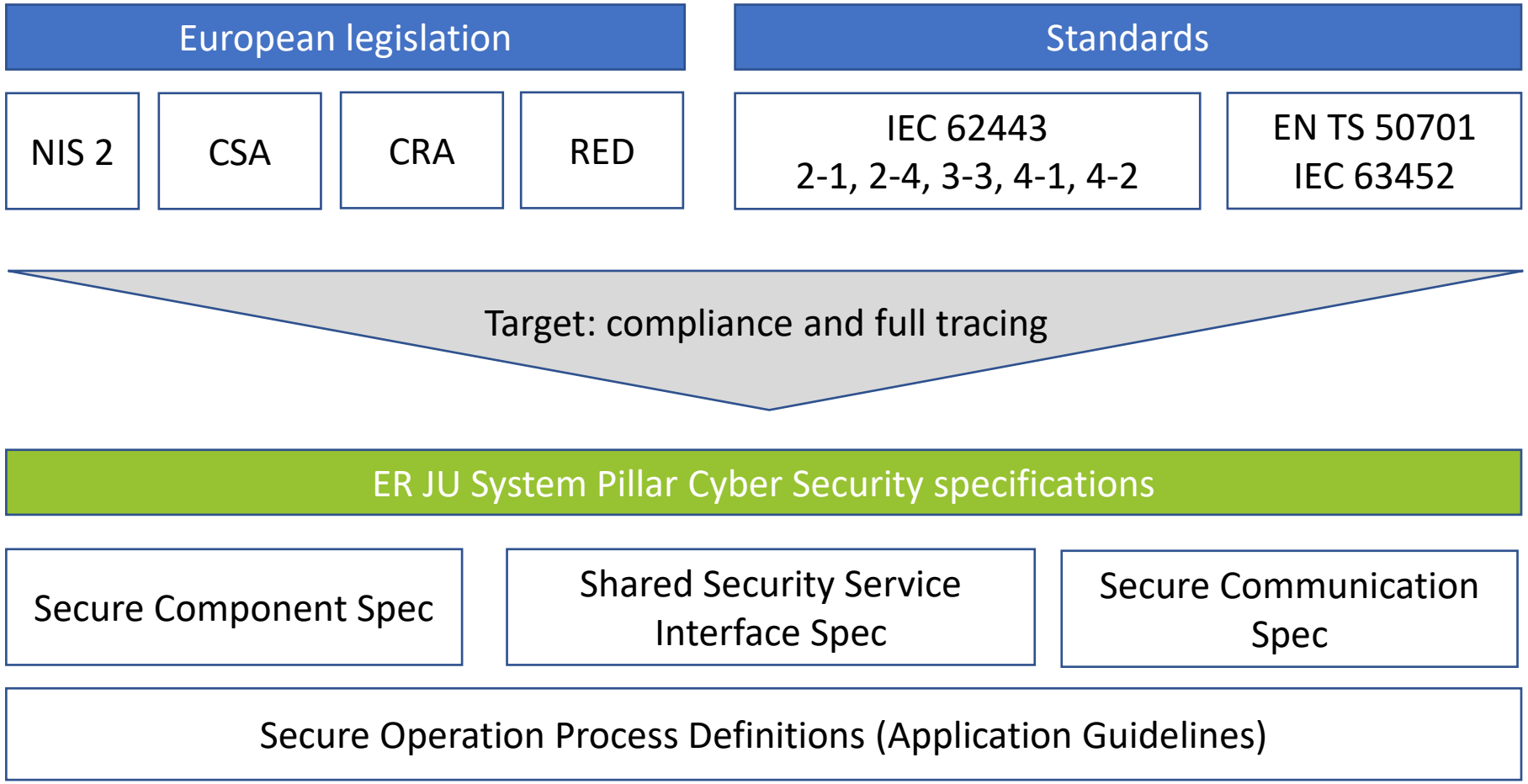


ER JU System Pillar – Cyber Security

2.6 Output of Cyber Security group

- **Secure component specification**
  - new doc based on EULYNX BL4 R2 Eu.Doc 114, UNISIG subset 146 & 147, X2Rail-3 docs,...)
- **Shared Security services specification**
  - new doc based on EULYNX BL4 R2 Eu.Doc 117, UNISIG subset 146, X2Rail-3/5 docs,...)
- **Secure communication specification**
  - update of UNISIG subset 146, EULYNX 114, 115 ...)
- **Application guideline / security operation process definitions**
  - as TSI Application Guideline, based on EULYNX BL4 R2 Eu.Doc 114, X2Rail-3/5 best practices,...)

2.7 Requirements flow



2.8 Document structure for standardization

ERA TSI CCS 2023	Update of ERA TSI CCS 2023		CSA Protection Profile
Subset-146 4.0 End-to-End Security Layer	Subset-146 5.0 End-to-End Security Layer	update with Secure Communication Spec	Secure Component Spec Protection Profile
Subset-147 1.0 Ethernet Consist Network	Subset-147 2.0 Ethernet Consist Network	update with Shared Sec Serv IFSpec	Evaluation method IEC 62443-6-2
Subset-137 4.0 Online ETCS Key Mngt.	Subset-137 5.0 Online ETCS Key Mngt.	Start deprecation?	
Subset-114 4.0 Offline ETCS Key Mngt.	New Subset-1xx Shared Security Service Interface Spec		
	New application guideline Secure Operation Process Definitions		

3. Outlook 2024

- **First drafts of specifications (12/2023)**
  - Draft specifications for innovation pillar, other SP domains, ERA, ENISA, UNISIG,...
- **Comment period (Jan-Mar 2024)**
  - Provide comments to draft specifications
- **Specification work (07/2024)**
  - Complete open points, work on finalization of specs, answer and include comments
- **Comment period for final draft (Aug – Sep 2024)**
  - Provide comments to final draft specifications
- **Finalization work (Sep – Dec 2024)**
  - Answer and include comments
- **Public version of final specifications / input for TSI CCS update (12/2024 - 01/2025)**

Thank you!

Questions?

Contact: markus.wischy@siemens.com
kurt.kayser-extern@deutschebahn.com