CENELEC prTS 50701
(Railway applications – CyberSecurity)

ENISA-ERA Conference: Cybersecurity in Railways

16th of March 2021

CEN CENELEC

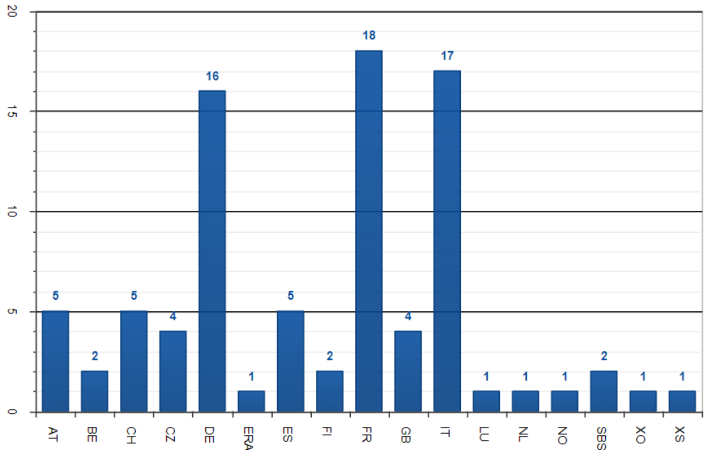
Railway CyberSecurity challenges

- Railway-specific challenges need to be addressed
  - Attackers have fairly easy physical access
  - The train is only one part of an diverse cross-border eco-system
  - There are safety-critical and non safety-critical systems in the environment
- Commercially viable methods for operators, manufacturers and vendors are needed
- → Synchronization points between stakeholders as well as safety and security required

CENELEC TC 9X/WG 26

WG 26

- Working Group on “Railway Applications – Cybersecurity”
- Covers Signaling, Rolling Stock, Fixed Installation
- ~90 experts (20-30 experts participating to F2F meetings)
- Experts from 13 countries (+ SBS, ERA and ENISA as observer)



Goal

- **Establish a TS for handling CyberSecurity in an unified way for the whole railway sector**
- **Based on already existing Industrial CyberSecurity security standards (e.g. IEC 62443)**

Timeline

- July 2017: Creation of TC9X – WG 26 to produce a Technical specification (TS 50701)
- June 2019: First enquiry on prTS 50701 draft
- Dec 2020: Final version submitted to NC vote
- In European Voting process since 8th of January 2021

Next steps

- End of Voting: 2nd of April 2021
- TS expected to be available in Summer 2021

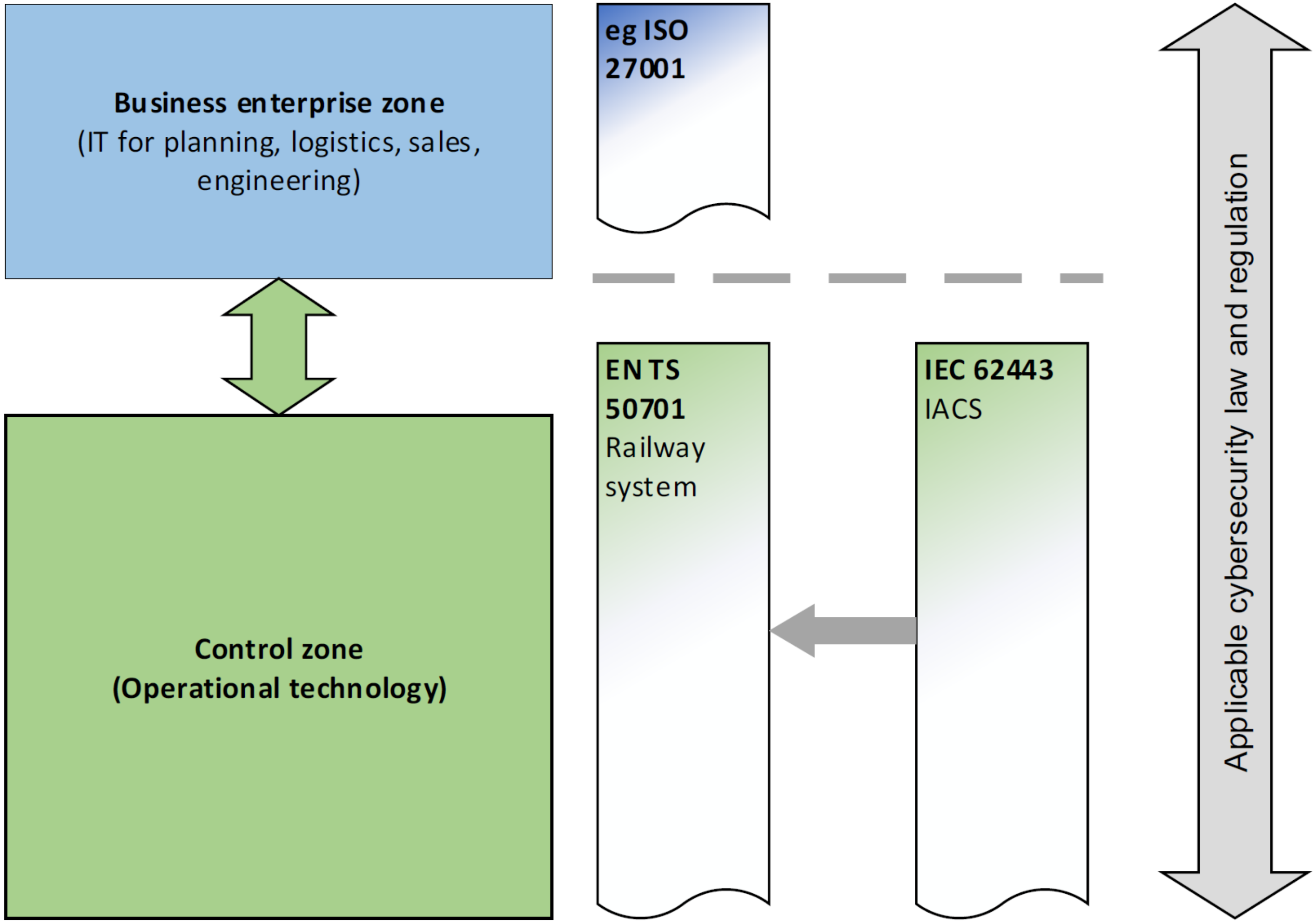
prTS 50701 overview

- The TS is an innovative standard that takes inspiration from different sources ...
  - IEC 62443 (SL vector, Risk assessment, list of requirements)
  - EN 50126 (life-cycle, threat log, cybersecurity case, SecRACs)
  - CSM-RA (risk acceptance principles)

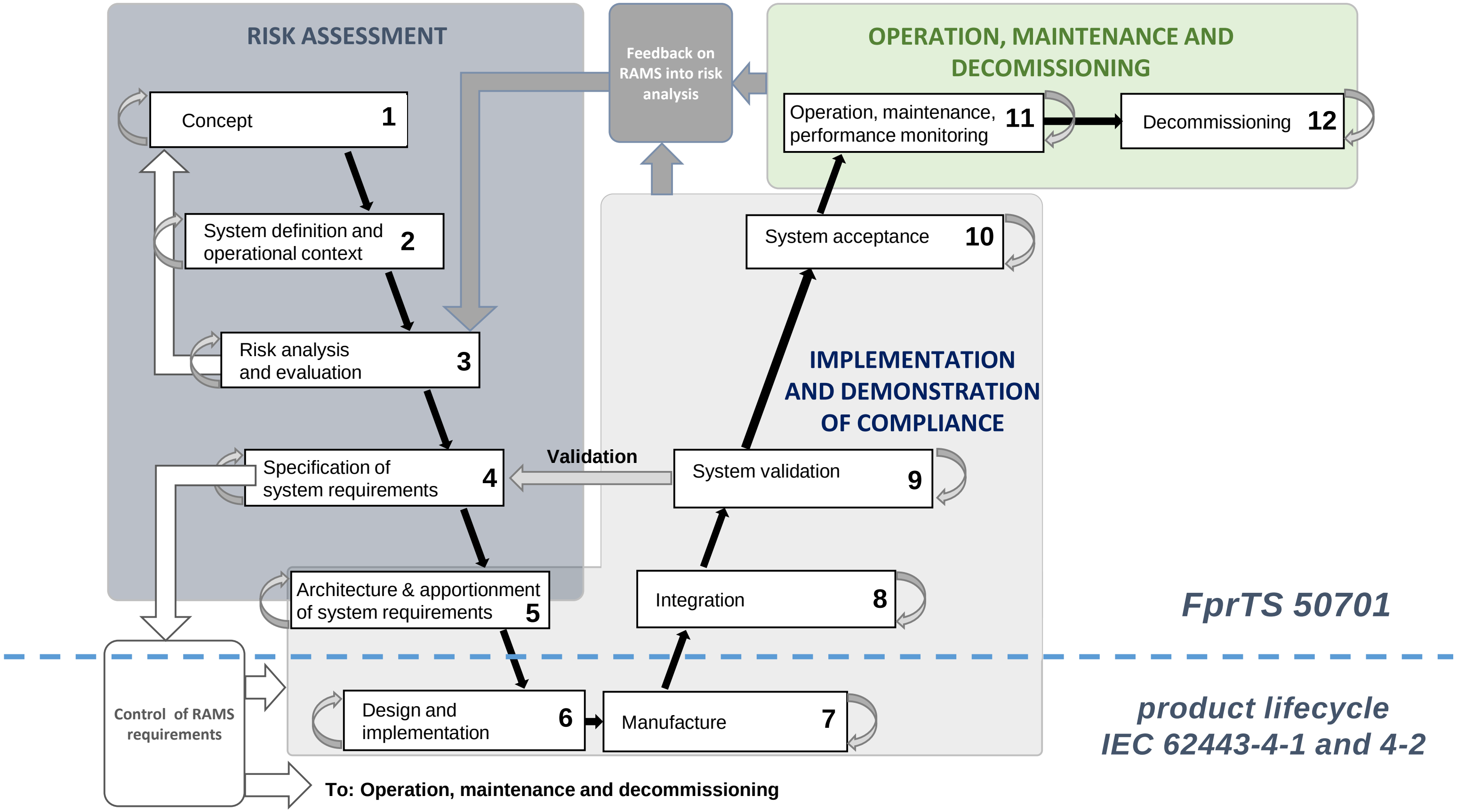
- ... adapted to railway context
  - Railway architecture model & zoning example
  - Railway notes for Security Requirements
  - Cybersecurity Design principles
  - Cybersecurity & Safety interface
  - Handling Legacy System
  - Risk acceptance methods

- In 3 years the TS shall be re-examined and possibly transformed into an EN
  - The success of this upgrade will depend on its capability to intercept the needs of the users
  - One key element is the availability of a simple and easy-to-implement process

prTS 50701 overview - Scope - IT/OT


Business enterprise zone
(IT for planning, logistics, sales, engineering)
eg ISO 27001
Control zone (Operational technology)
EN TS 50701 Railway system
IEC 62443 IACS
Applicable cybersecurity law and regulation

prTS 50701 overview - Scope vs EN50126

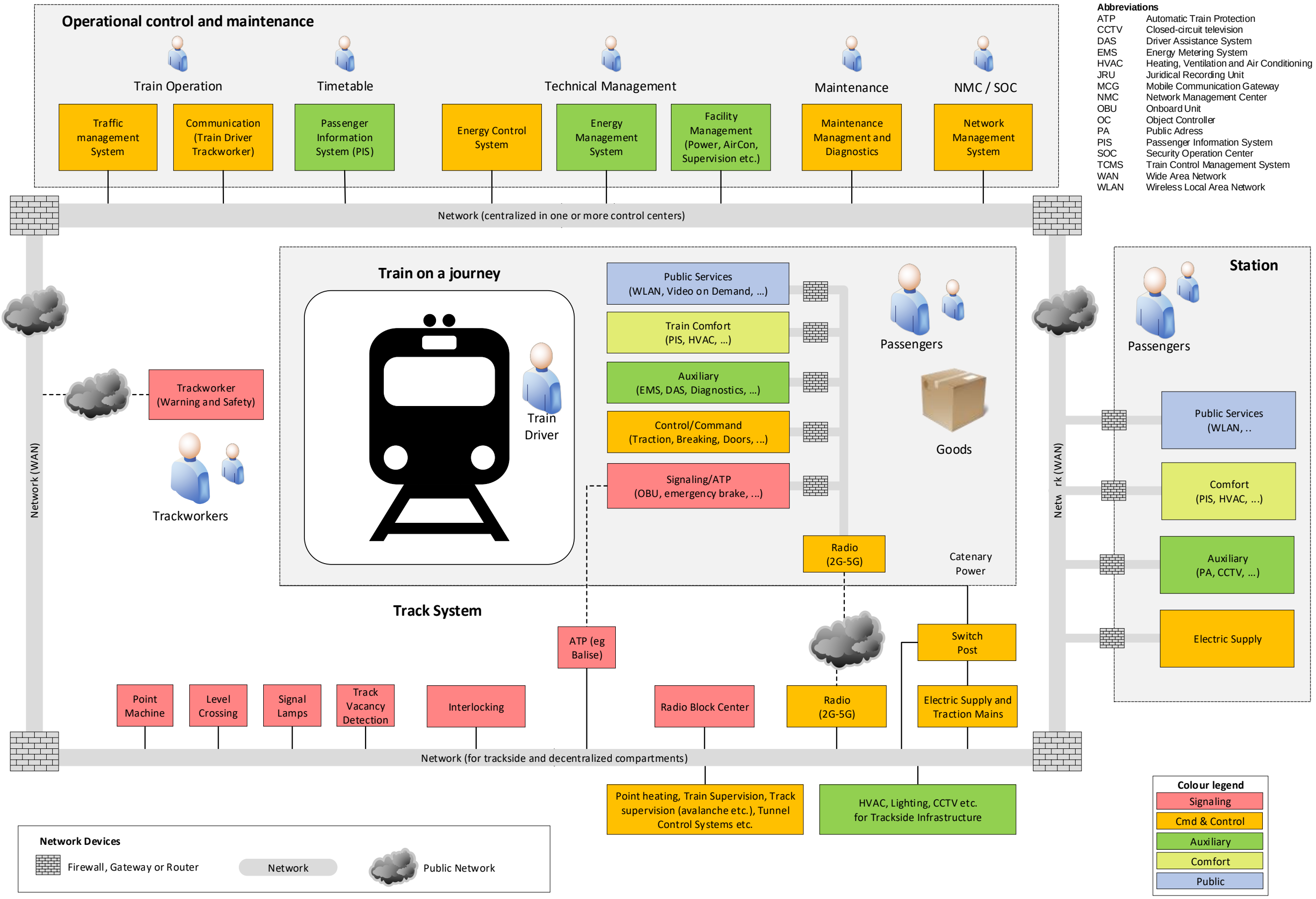

RISK ASSESSMENT
Feedback on RAMS into risk analysis
OPERATION, MAINTENANCE AND DECOMISSIONING
Concept 1
System definition and operational context 2
Risk analysis and evaluation 3
Specification of system requirements 4
Architecture & apportionment of system requirements 5
Design and implementation 6
Manufacture 7
Integration 8
System validation 9
System acceptance 10
Operation, maintenance, performance monitoring 11
Decommissioning 12
Validation
IMPLEMENTATION AND DEMONSTRATION OF COMPLIANCE
Control of RAMS requirements
To: Operation, maintenance and decommissioning

FprTS 50701

product lifecycle
IEC 62443-4-1 and 4-2

EN 50126-1:2017 - Figure 7 — The V-cycle representation

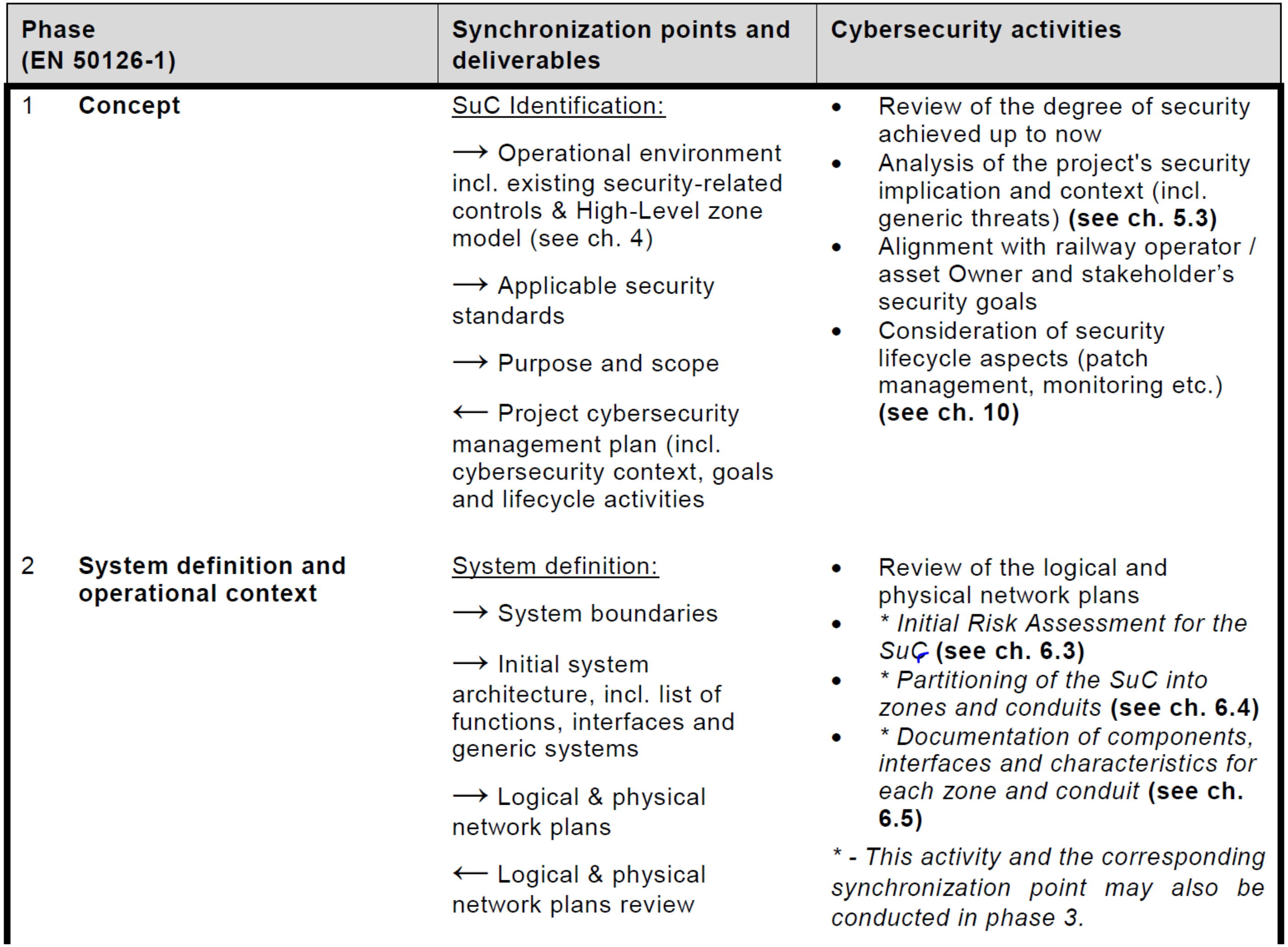
prTS 50701 overview – Reference Arch.


Operational control and maintenance
Train Operation
Timetable
Technical Management
Maintenance
NMC / SOC
Traffic management System
Communication (Train Driver Trackworker)
Passenger Information System (PIS)
Energy Control System
Energy Management System
Facility Management (Power, AirCon, Supervision etc.)
Maintenance Managment and Diagnostics
Network Management System
Network (centralized in one or more control centers)
Network (WAN)
Train on a journey
Train Driver
Public Services (WLAN, Video on Demand, ...)
Train Comfort (PIS, HVAC, ...)
Auxiliary (EMS, DAS, Diagnostics, ...)
Control/Command (Traction, Breaking, Doors, ...)
Signaling/ATP (OBU, emergency brake, ...)
Passengers
Goods
Radio (2G-5G)
Catenary Power
Trackworker (Warning and Safety)
Trackworkers
Station
Passengers
Public Services (WLAN, ..
Comfort (PIS, HVAC, ...)
Auxiliary (PA, CCTV, ...)
Electric Supply
Netw rk (WAN)
Track System
ATP (eg Balise)
Switch Post
Point Machine
Level Crossing
Signal Lamps
Track Vacancy Detection
Interlocking
Radio Block Center
Radio (2G-5G)
Electric Supply and Traction Mains
Network (for trackside and decentralized compartments)
Point heating, Train Supervision, Track supervision (avalanche etc.), Tunnel Control Systems etc.
HVAC, Lighting, CCTV etc. for Trackside Infrastructure
Network Devices
Firewall, Gateway or Router
Network
Public Network
Colour legend
Signaling
Cmd & Control
Auxiliary
Comfort
Public

Abbreviations

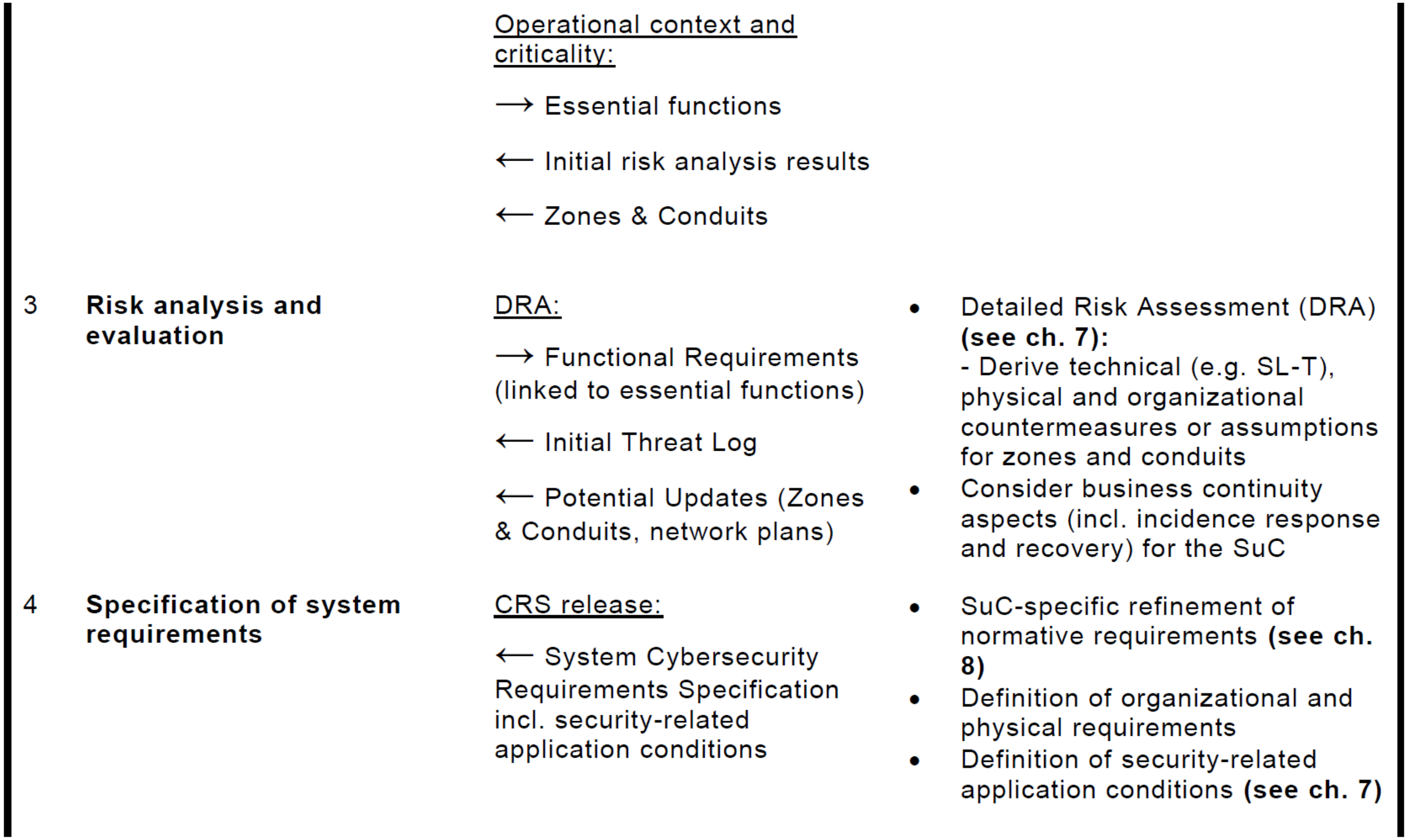
ATP	Automatic Train Protection
CCTV	Closed-circuit television
DAS	Driver Assistance System
EMS	Energy Metering System
HVAC	Heating, Ventilation and Air Conditioning
JRU	Juridical Recording Unit
MCG	Mobile Communication Gateway
NMC	Network Management Center
OBU	Onboard Unit
OC	Object Controller
PA	Public Adress
PIS	Passenger Information System
SOC	Security Operation Center
TCMS	Train Control Management System
WAN	Wide Area Network
WLAN	Wireless Local Area Network

prTS 50701 overview – Lifecycle



Phase (EN 50126-1)	Synchronization points and deliverables	Cybersecurity activities
1 **Concept**	SuC Identification: ⟶ Operational environment incl. existing security-related controls & High-Level zone model (see ch. 4) ⟶ Applicable security standards ⟶ Purpose and scope ⟵ Project cybersecurity management plan (incl. cybersecurity context, goals and lifecycle activities	• Review of the degree of security achieved up to now • Analysis of the project's security implication and context (incl. generic threats) **(see ch. 5.3)** • Alignment with railway operator / asset Owner and stakeholder's security goals • Consideration of security lifecycle aspects (patch management, monitoring etc.) **(see ch. 10)**
2 **System definition and operational context**	System definition: ⟶ System boundaries ⟶ Initial system architecture, incl. list of functions, interfaces and generic systems ⟶ Logical & physical network plans ⟵ Logical & physical network plans review	• Review of the logical and physical network plans • ** Initial Risk Assessment for the SuC* **(see ch. 6.3)** • ** Partitioning of the SuC into zones and conduits* **(see ch. 6.4)** • ** Documentation of components, interfaces and characteristics for each zone and conduit* **(see ch. 6.5)** ** - This activity and the corresponding synchronization point may also be conducted in phase 3.*

prTS 50701 overview – Lifecycle

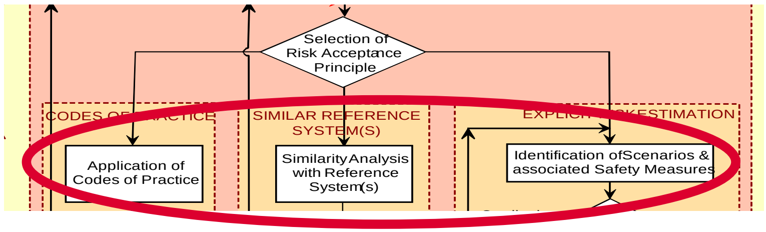


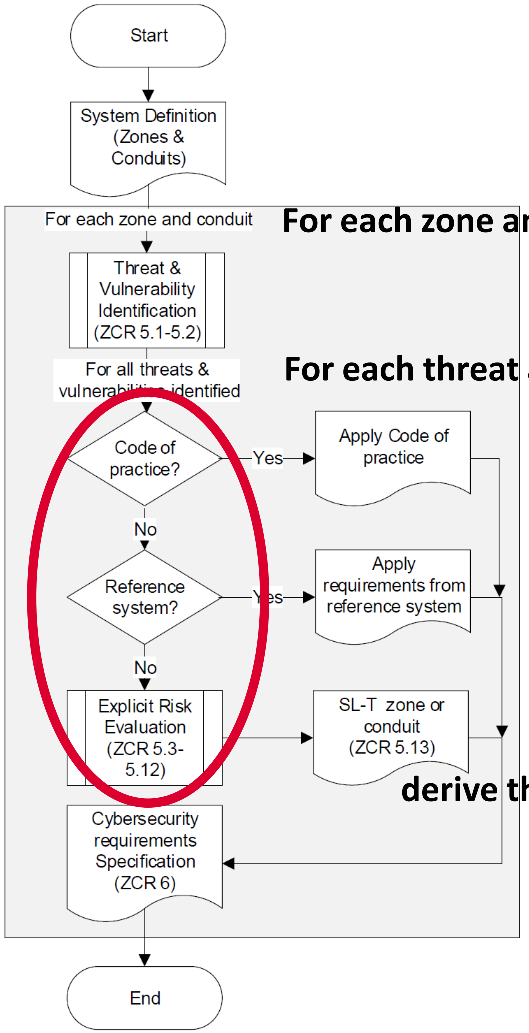
		Operational context and criticality: ⟶ Essential functions ⟵ Initial risk analysis results ⟵ Zones & Conduits	
3	**Risk analysis and evaluation**	DRA: ⟶ Functional Requirements (linked to essential functions) ⟵ Initial Threat Log ⟵ Potential Updates (Zones & Conduits, network plans)	• Detailed Risk Assessment (DRA) **(see ch. 7):** - Derive technical (e.g. SL-T), physical and organizational countermeasures or assumptions for zones and conduits • Consider business continuity aspects (incl. incidence response and recovery) for the SuC
4	**Specification of system requirements**	CRS release: ⟵ System Cybersecurity Requirements Specification incl. security-related application conditions	• SuC-specific refinement of normative requirements **(see ch. 8)** • Definition of organizational and physical requirements • Definition of security-related application conditions **(see ch. 7)**

prTS 50701 overview – Detailed risk assessment

- The process needs to take into account also legacy solutions or standards, this may be handled by reference systems or codes of practice, that need to be integrated with the SL approach.
- The process is carried out by zone/conduit and by threat.
- Finally the requirements for a zone/conduit are consolidated.
- This allows a non-disruptive move to 62443 but also preserves legacy solutions.

CSM-RA, Risk Acceptance Principles


Selection of Risk Acceptance Principle
CODES OF PRACTICE
SIMILAR REFERENCE SYSTEM(S)
EXPLICIT RISK ESTIMATION
Application of Codes of Practice
Similarity Analysis with Reference System(s)
Identification ofScenarios & associated Safety Measures


Start
System Definition (Zones & Conduits)
For each zone and conduit
Threat & Vulnerability Identification (ZCR 5.1-5.2)
For all threats & vulnerabilities identified
Code of practice?
Yes
Apply Code of practice
No
Reference system?
Yes
Apply requirements from reference system
No
Explicit Risk Evaluation (ZCR 5.3-5.12)
SL-T zone or conduit (ZCR 5.13)
Cybersecurity requirements Specification (ZCR 6)
End

For each zone and conduit

For each threat and vulnerability

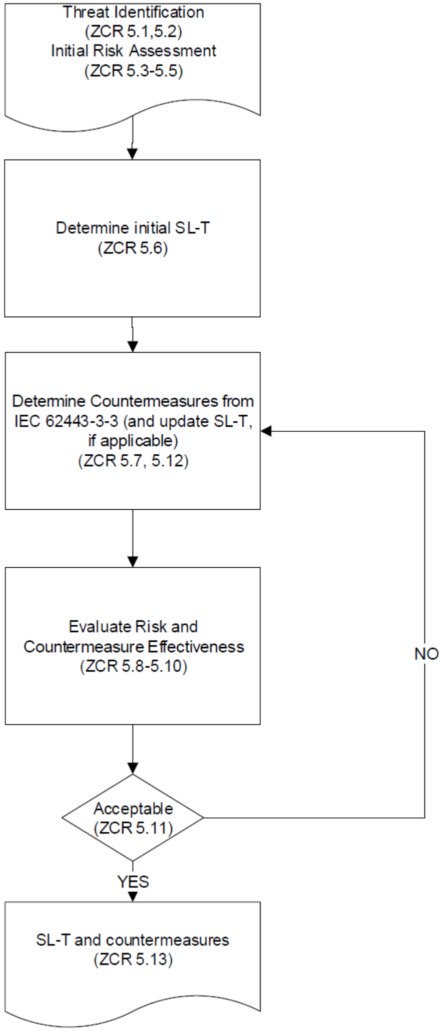
derive the SL-T vector

How is a SL assigned?

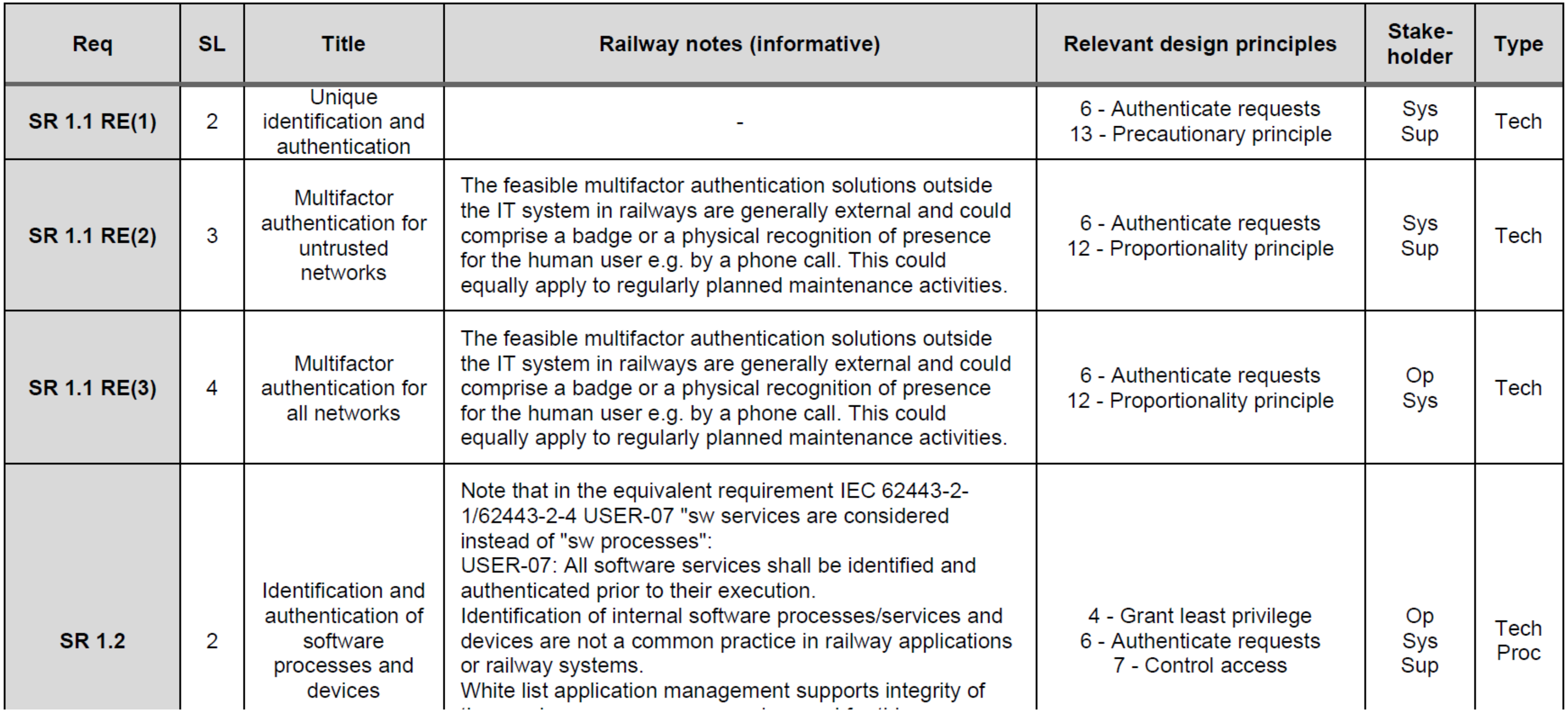
- SL can be viewed as a qualitative means of risk reduction. It is assumed that each organization has a risk matrix with appropriate acceptance criteria.

- To obtain SL, the zone/conduit is evaluated taking into account all measures that a particular (candidate) SL vector implies.

- If the risk is acceptable then the SL-T is found. If not, add additional countermeasures (increase SL-T) and try again.



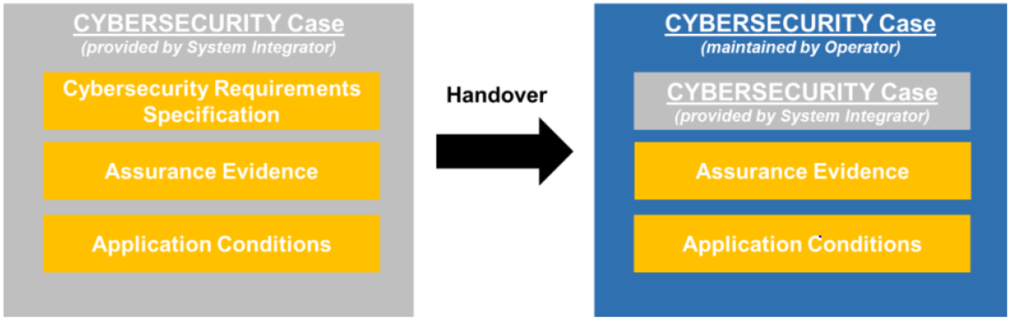
prTS 50701 overview – Railway notes for Security Reqs.



Req	SL	Title	Railway notes (informative)	Relevant design principles	Stake-holder	Type
SR 1.1 RE(1)	2	Unique identification and authentication	-	6 - Authenticate requests 13 - Precautionary principle	Sys Sup	Tech
SR 1.1 RE(2)	3	Multifactor authentication for untrusted networks	The feasible multifactor authentication solutions outside the IT system in railways are generally external and could comprise a badge or a physical recognition of presence for the human user e.g. by a phone call. This could equally apply to regularly planned maintenance activities.	6 - Authenticate requests 12 - Proportionality principle	Sys Sup	Tech
SR 1.1 RE(3)	4	Multifactor authentication for all networks	The feasible multifactor authentication solutions outside the IT system in railways are generally external and could comprise a badge or a physical recognition of presence for the human user e.g. by a phone call. This could equally apply to regularly planned maintenance activities.	6 - Authenticate requests 12 - Proportionality principle	Op Sys	Tech
SR 1.2	2	Identification and authentication of software processes and devices	Note that in the equivalent requirement IEC 62443-2-1/62443-2-4 USER-07 "sw services are considered instead of "sw processes": USER-07: All software services shall be identified and authenticated prior to their execution. Identification of internal software processes/services and devices are not a common practice in railway applications or railway systems. White list application management supports integrity of	4 - Grant least privilege 6 - Authenticate requests 7 - Control access	Op Sys Sup	Tech Proc

prTS 50701 overview – Safety and Security, Cybersecurity Case

- Usually there exist (a few) high-level security requirements that are safety-related
- In the Cybersecurity Case these are either
  - shown to be fulfilled, or
  - fulfilled under assumptions that have to be exported as SecRAC, or
  - partially fulfilled (compensating countermeasures have to be defined)
- Safety Case references the Cybersecurity Report
- Cybersecurity Case can be updated without change of the safety case



Content of CyberSecurity Case 1/2

Introduction (could be a set of references to other documents)

- System under Consideration definition (incl. Zones and Conduits)
- Threat and risks assessment
  - Assumptions
  - List of threat intelligences sources
  - List of threat Scenarios
  - List of sufficiently mitigated risks (with explanation)

Cybersecurity Requirement Specification (CRS) (could be a set of references to other documents)

- Assumptions
- Cybersecurity needs (including safety-related high level objectives)
- Cybersecurity requirements
- List of open risks (with explanation)

Cybersecurity management (could be a set of references to other documents)

- Cybersecurity policy
- Cybersecurity plan
- Cybersecurity process
- Vulnerability assessment and management

Cybersecurity fulfilment (could be a set of references to other documents)

- Implementation of cybersecurity measures - evidences of fulfilment of CRS
- Evidence of application of cybersecurity process
- Verification & validation results
  - Testing of security measures (e.g. V&V, Penetration testing)
  - Traceability to cybersecurity requirements

Content of CyberSecurity Case 2/2

- Related cybersecurity cases (from included components or subsystems, if any)

Security-related application conditions (could be a set of references to other documents)

- Installation
- Maintenance
- Operation

Conclusion

- Cybersecurity claim
- Residual risks status

Next steps

- Dissemination of the TS 50701
- Capture return on experience to improve the TS and transform it into an European Norm (EN)
- Collaboration with other standardization commitee (IEC AHG 20, …)
- Preparation of submission of a NWIP to complete the TS with additional material (e.g. topics related to cybersecurity during operation and maintenance phases as security monitoring and security incident response)

Thank you for your attention!

christian.schlehuber@deutschebahn.com
serge.benoliel@alstomgroup.com

Q &A