Hands-On CLC/TS 50701 (Railway applications – CyberSecurity)

3rd ERA – ENISA Conference CyberSecurity in Railways

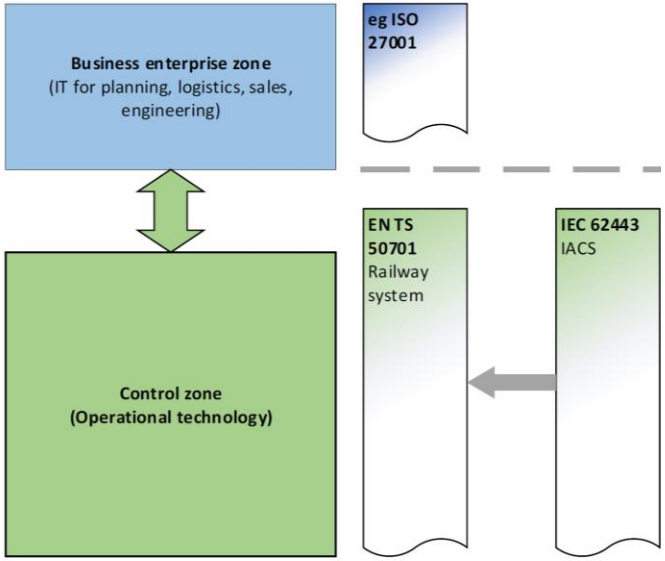
09th of November 2023

Agenda

1. Overview and facts on TS 50701
2. Security Engineering with TS 50701 (in a brief)
    1. Phase 1 – Concept
    2. Phase 2 – Design
    3. Phase 3 & 4 – Risk Analysis and Requirements
    4. Phase 9 & 10 – Assurance
3. Conclusion

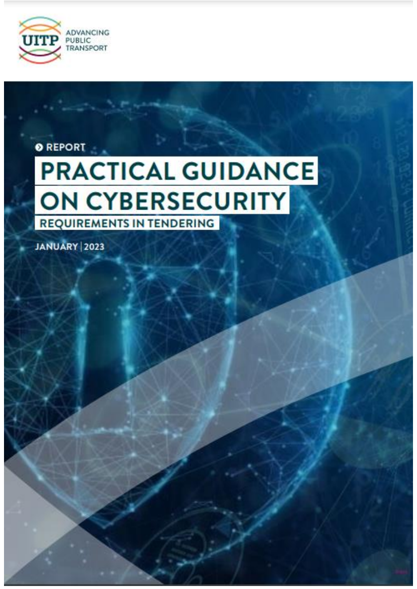
TS 50701 in a nutshell

- Developed by CENELEC TC 9X/WG 26 (team of currently 96 European experts) since July 2017
- Goal: Establish a TS for handling CyberSecurity in a unified way for the whole railway sector
- Based on IEC 62443 series and EN 50126
- First edition published in July 2021
- Second edition published in August 2023



TS 50701 usage examples (excerpt)

- Several European tenders/operators require the application of TS 50701
- Train manufacturers from Europe apply TS 50701 as Security Framework
- Partially applied on projects in Singapore and Australia
- UITP Practical Guidance on CyberSecurity (based on TS 50701)
- Acknowledged by authorities in most parts of the world (e.g. in Germany as standard for fulfilling KRITIS requirements)



UITP ADVANCING PUBLIC TRANSPORT

REPORT

PRACTICAL GUIDANCE ON CYBERSECURITY

REQUIREMENTS IN TENDERING

JANUARY | 2023

Fintraffic

DIGI RATA

Euroopan unionin rahoittama
NextGenerationEU

cen CENELEC

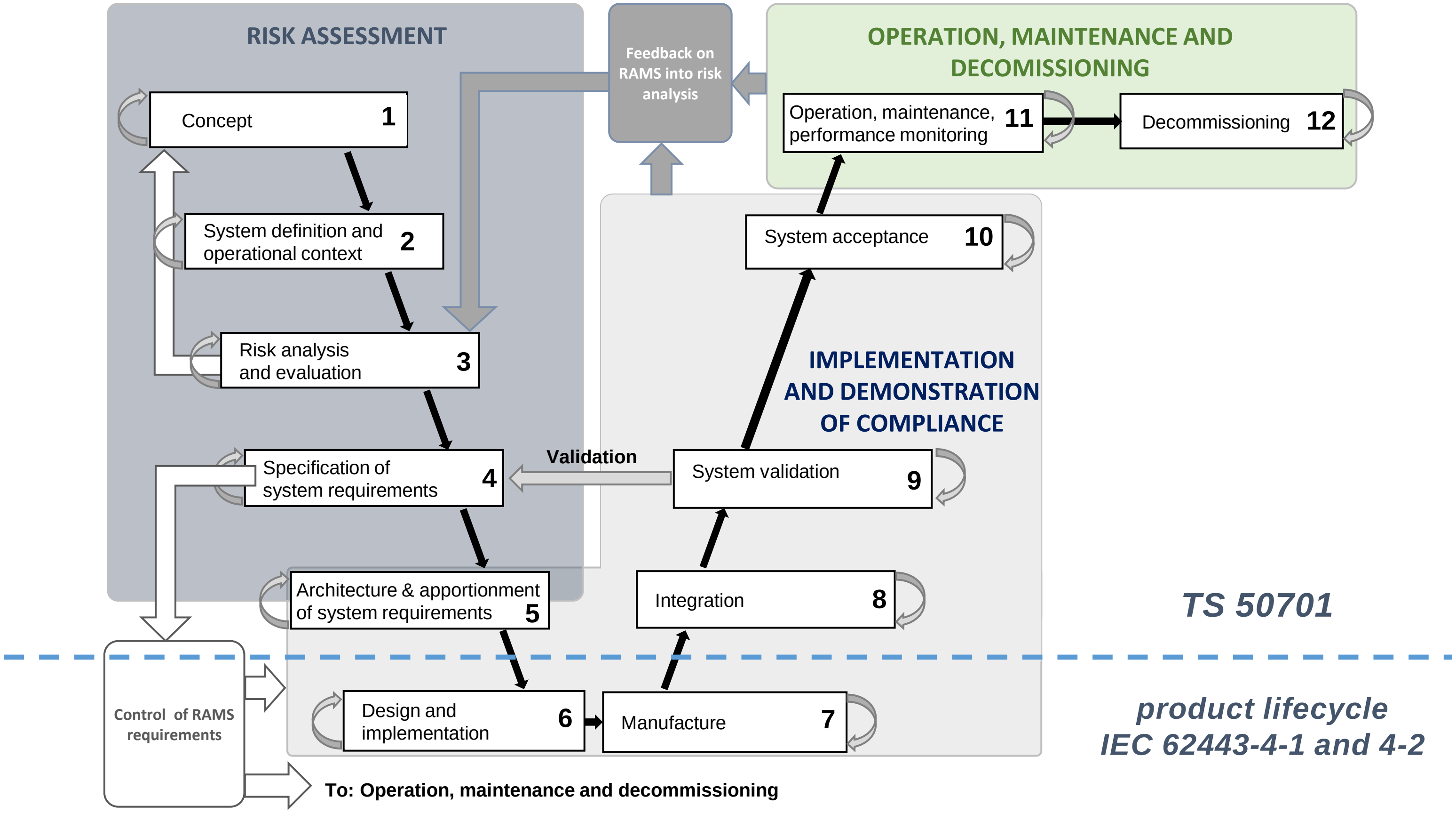
TS 50701 – Security Engineering (short)

How to perform Security Engineering with TS 50701?

Focus today on: Phase 1 to Phase 4 (and a bit Phase 9/10)

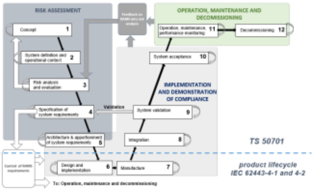
Disclaimer: This talk will only give an overview

TS 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
IMPLEMENTATION AND DEMONSTRATION OF COMPLIANCE
Validation
Control of RAMS requirements
To: Operation, maintenance and decommissioning
TS 50701
product lifecycle
IEC 62443-4-1 and 4-2

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

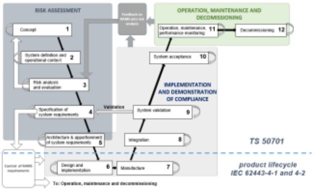
Phase 1

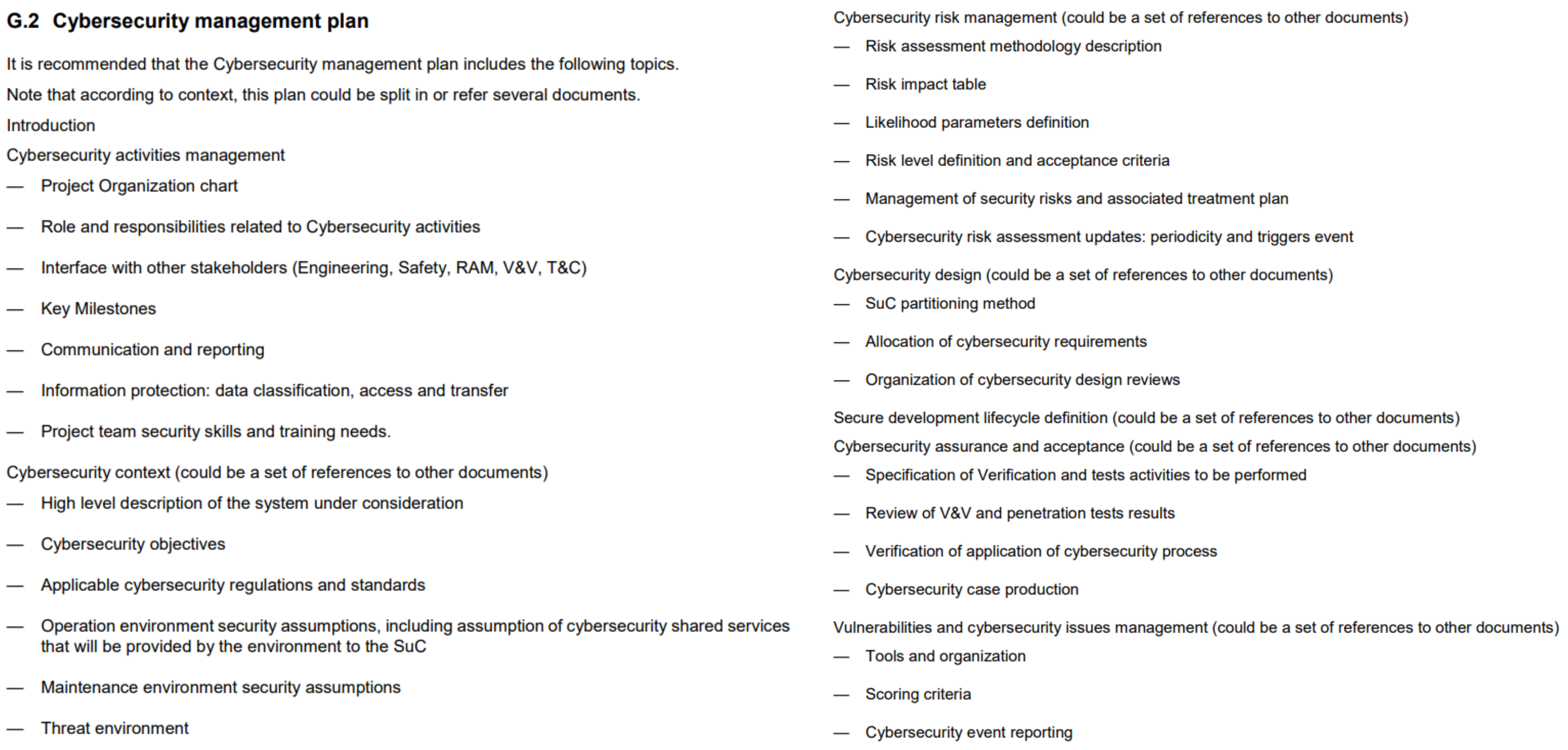


RISK ASSESSMENT
Concept 1
System definition and operational context 2
Risk analysis and evaluation 3
Specification of system requirements 4
Architecture & apportionment of system requirements 5
Design and implementation 6
Manufacture 7
Integration 8
System validation 9
System acceptance 10
Operation, maintenance, performance monitoring 11
Decommissioning 12
Validation
Feedback on RAMS into risk analysis
OPERATION, MAINTENANCE AND DECOMISSIONING
IMPLEMENTATION AND DEMONSTRATION OF COMPLIANCE
TS 50701
product lifecycle IEC 62443-4-1 and 4-2
To: Operation, maintenance and decommissioning

1	**Concept**	SuC Identification: → Operational environment incl. existing security-related controls and High-Level zone model (see Clause 4) → Applicable security standards → Purpose and scope ← Project cybersecurity management plan (incl. cybersecurity context, goals and lifecycle activities (see Annex G, G.2)	— Review of the level of security achieved up to now — Analysis of the project's security implication and context (incl. generic threats) (see 5.4) — Alignment with railway operator / asset owner and stakeholder's security goals — Consideration of security lifecycle aspects (patch management, monitoring, etc.) (see Clause10) — Plan cybersecurity-related activities

Phase 1


RISK ASSESSMENT
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
To: Operation, maintenance and decommissioning
TS 50701
product lifecycle
IEC 62443-4-1 and 4-2



G.2 Cybersecurity management plan

It is recommended that the Cybersecurity management plan includes the following topics.

Note that according to context, this plan could be split in or refer several documents.

Introduction

Cybersecurity activities management

— Project Organization chart

— Role and responsibilities related to Cybersecurity activities

— Interface with other stakeholders (Engineering, Safety, RAM, V&V, T&C)

— Key Milestones

— Communication and reporting

— Information protection: data classification, access and transfer

— Project team security skills and training needs.

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

— High level description of the system under consideration

— Cybersecurity objectives

— Applicable cybersecurity regulations and standards

— Operation environment security assumptions, including assumption of cybersecurity shared services that will be provided by the environment to the SuC

— Maintenance environment security assumptions

— Threat environment

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

— Risk assessment methodology description

— Risk impact table

— Likelihood parameters definition

— Risk level definition and acceptance criteria

— Management of security risks and associated treatment plan

— Cybersecurity risk assessment updates: periodicity and triggers event

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

— SuC partitioning method

— Allocation of cybersecurity requirements

— Organization of cybersecurity design reviews

Secure development lifecycle definition (could be a set of references to other documents)

Cybersecurity assurance and acceptance (could be a set of references to other documents)

— Specification of Verification and tests activities to be performed

— Review of V&V and penetration tests results

— Verification of application of cybersecurity process

— Cybersecurity case production

Vulnerabilities and cybersecurity issues management (could be a set of references to other documents)

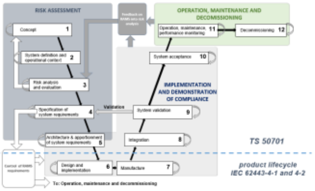
— Tools and organization

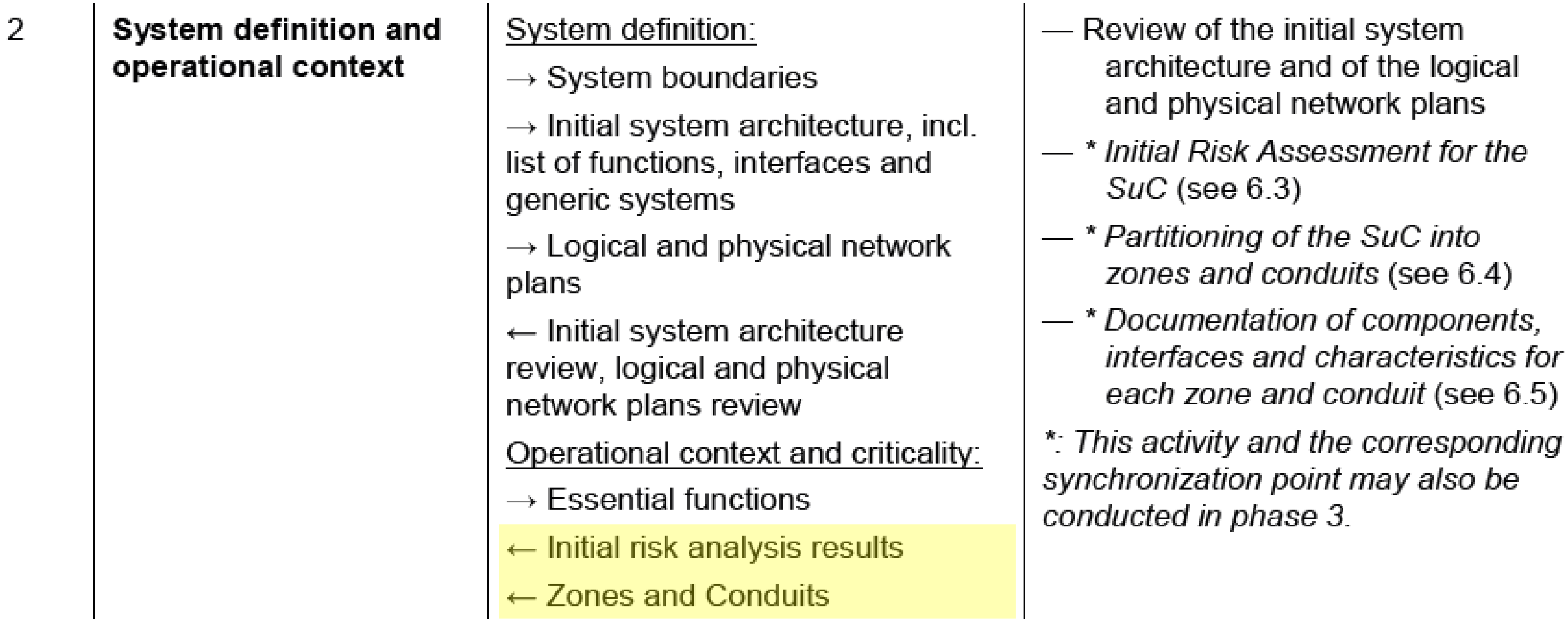
— Scoring criteria

— Cybersecurity event reporting

Attention: Living document!

Phase 2

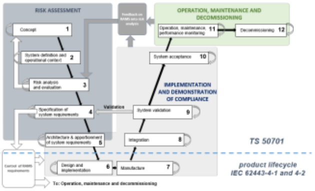

RISK ASSESSMENT
Concept 1
System definition and operational context 2
Risk analysis and evaluation 3
Specification of system requirements 4
Architecture & apportionment of system requirements 5
Design and implementation 6
Manufacture 7
Integration 8
System validation 9
System acceptance 10
Operation, maintenance, performance monitoring 11
Decommissioning 12
Validation
OPERATION, MAINTENANCE AND DECOMISSIONING
IMPLEMENTATION AND DEMONSTRATION OF COMPLIANCE
Feedback on RAMS into risk analysis
Control of RAMS requirements
To: Operation, maintenance and decommissioning
TS 50701
product lifecycle
IEC 62443-4-1 and 4-2

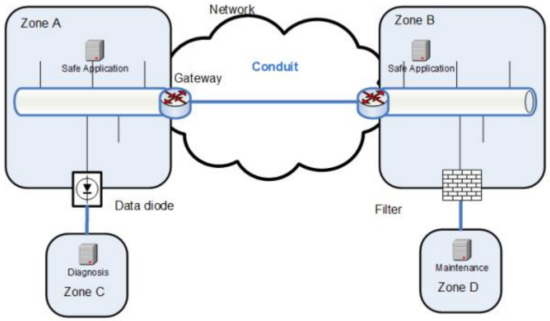


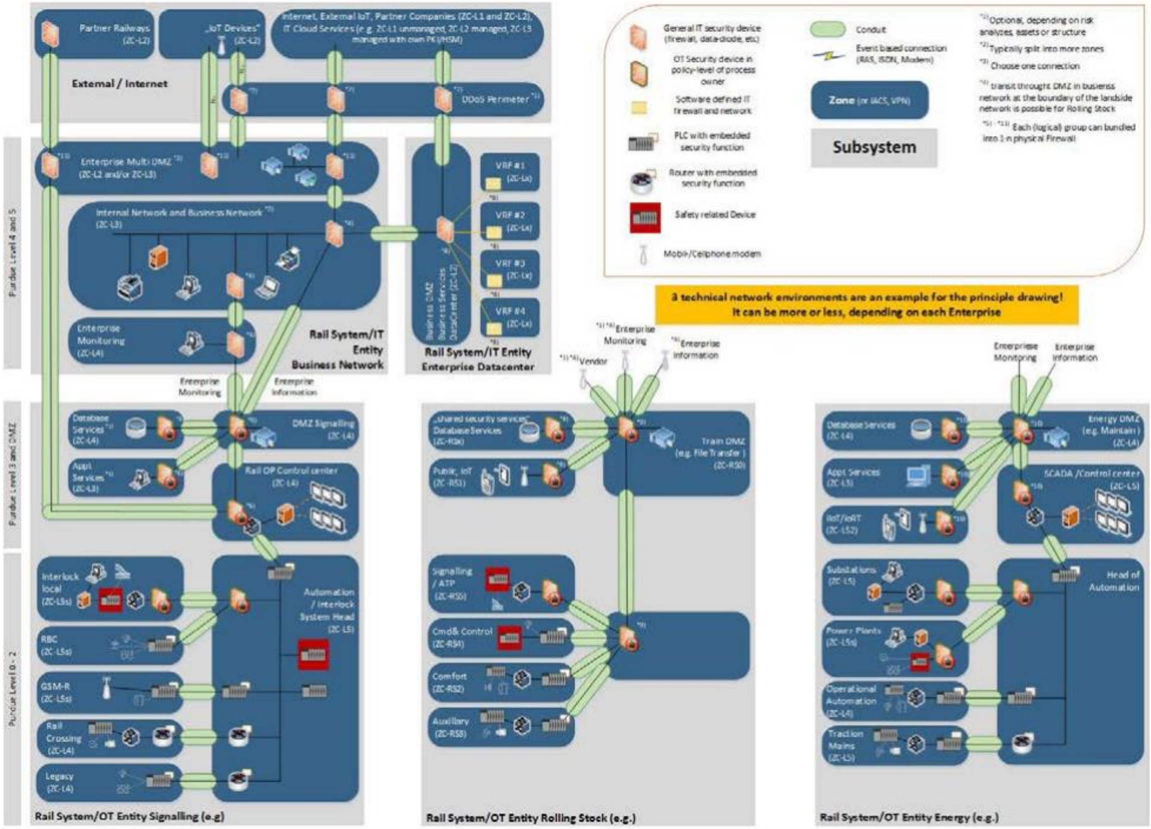
2	**System definition and operational context**	<u>System definition:</u> → System boundaries → Initial system architecture, incl. list of functions, interfaces and generic systems → Logical and physical network plans ← Initial system architecture review, logical and physical network plans review <u>Operational context and criticality:</u> → Essential functions ← Initial risk analysis results ← Zones and Conduits	— Review of the initial system architecture and of the logical and physical network plans — * *Initial Risk Assessment for the SuC* (see 6.3) — * *Partitioning of the SuC into zones and conduits* (see 6.4) — * *Documentation of components, interfaces and characteristics for each zone and conduit* (see 6.5) *: *This activity and the corresponding synchronization point may also be conducted in phase 3.*

Additional reading:
https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways

Phase 2


RISK ASSESSMENT
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
Feedback on RAMS into risk analysis
OPERATION, MAINTENANCE AND DECOMISSIONING
IMPLEMENTATION AND DEMONSTRATION OF COMPLIANCE
Control of RAMS requirements
To: Operation, maintenance and decommissioning
TS 50701
product lifecycle
IEC 62443-4-1 and 4-2




Partner Railways (ZC-L2)
„IoT Devices" (ZC-L2)
Internet, External IoT, Partner Companies (ZC-L1 and ZC-L2), IT Cloud Services (e.g. ZC-L1 unmanaged, ZC-L2 managed, ZC-L3 managed with own PKI/HSM)
External / Internet
DDoS Perimeter *1)
Enterprise Multi DMZ *2) (ZC-L2 and/or ZC-L3)
Internal Network and Business Network *2) (ZC-L3)
Enterprise Monitoring (ZC-L4)
Rail System/IT Entity Business Network
VRF #1 (ZC-Lx)
VRF #2 (ZC-Lx)
VRF #3 (ZC-Lx)
VRF #4 (ZC-Lx)
Business DMZ Business Services DataCenter (ZC-L2)
Rail System/IT Entity Enterprise Datacenter
Purdue Level 4 and 5
Purdue Level 3 and DMZ
Purdue Level 0 - 2
Enterprise Monitoring
Enterprise Information
Database Services *1) (ZC-L4)
DMZ Signalling (ZC-L4)
Appl. Services *1) (ZC-L3)
Rail OP Control center (ZC-L4)
Interlock local (ZC-LSs)
Automation / Interlock System Head (ZC-LS)
RBC (ZC-LSs)
GSM-R (ZC-LSs)
Rail Crossing (ZC-L4)
Legacy (ZC-L4)
Rail System/OT Entity Signalling (e.g)
*1) *4) Vendor
*1) *4) Enterprise Monitoring
*4) Enterprise Information
„shared security services" Database Services (ZC-RSx)
Train DMZ (e.g. File Transfer) (ZC-RS0)
Public, IoT (ZC-RS1)
Signalling / ATP (ZC-RS5)
Cmd& Control (ZC-RS4)
Comfort (ZC-RS2)
Auxiliary (ZC-RS3)
Rail System/OT Entity Rolling Stock (e.g.)
Enterpriese Monitoring
Enterprise Information
Database Services (ZC-L4)
Energy DMZ (e.g. Maintain) (ZC-L4)
Appl. Services (ZC-L3)
SCADA /Control center (ZC-L5)
IIoT/IoRT (ZC-LS2)
Substations (ZC-L5)
Head of Automation
Power Plants (ZC-L5s)
Operational Automation (ZC-L4)
Traction Mains (ZC-L5)
Rail System/OT Entity Energy (e.g.)
General IT security device (firewall, data-diode, etc)
OT Security device in policy-level of process owner
Software defined IT firewall and network
PLC with embedded security function
Router with embedded security function
Safety related Device
Mobile/Cellphone modem
Conduit
Event based connection (RAS, ISDN, Modem)
Zone (or IACS, VPN)
Subsystem

*1) Optional, depending on risk analyzes, assets or structure

*2) Typically split into more zones

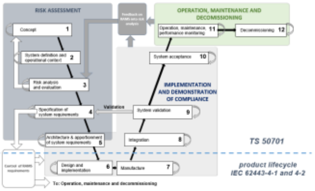
*3) Choose one connection

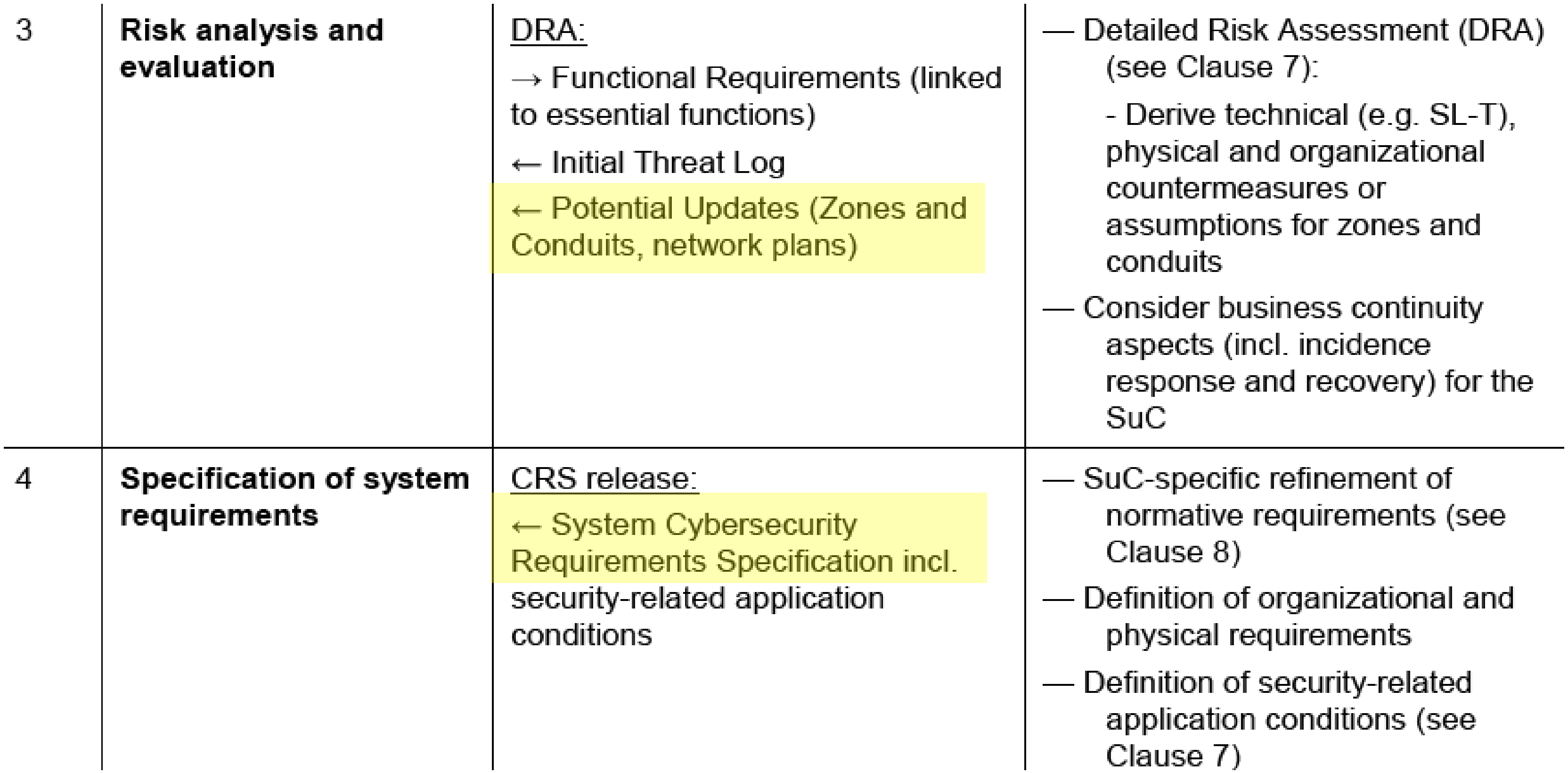
*4) transit throught DMZ in busieness network at the boundary of the landside network is possible for Rolling Stock

*5) - *11) Each (logical) group can bundled into 1-n physical Firewall

3 technical network environments are an example for the principle drawing!
It can be more or less, depending on each Enterprise

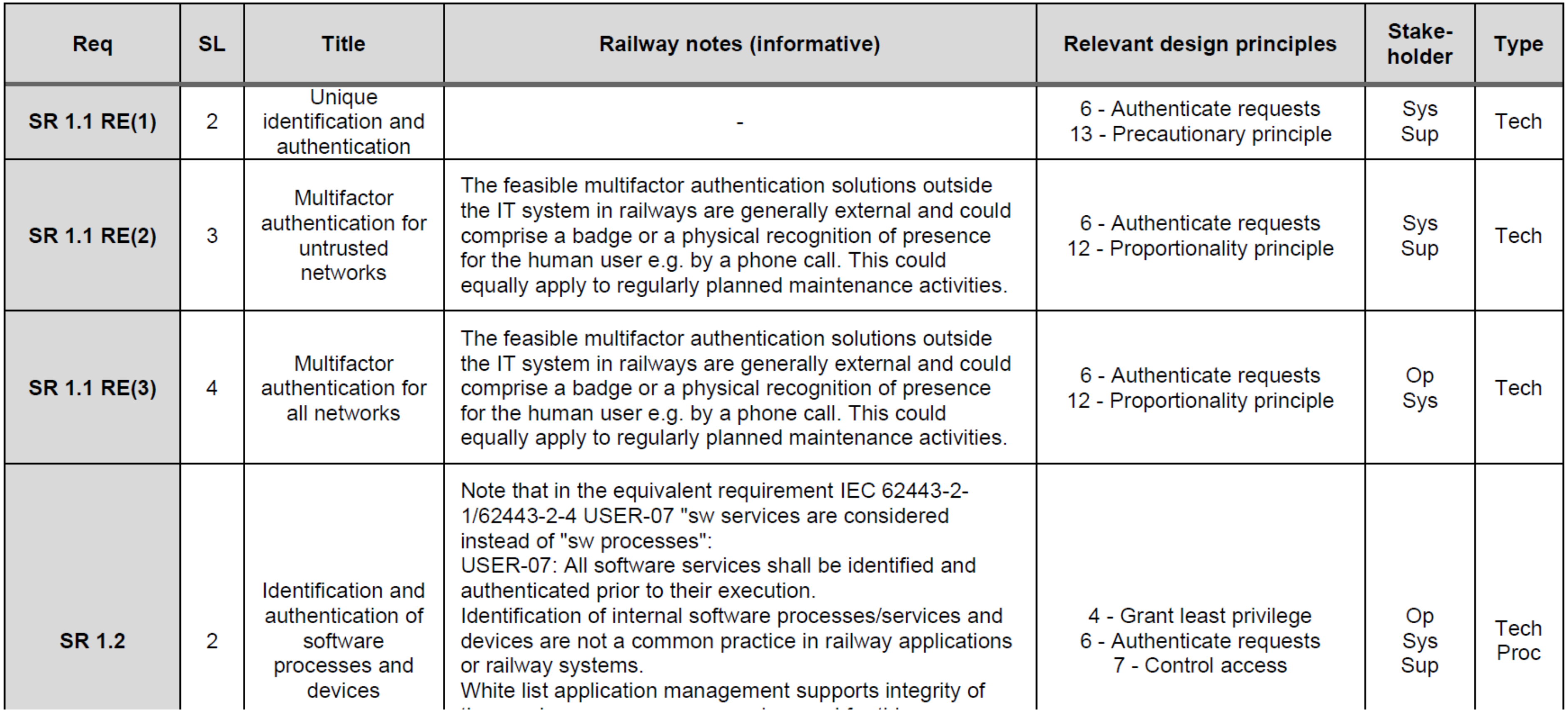
Phase 3 & Phase 4


RISK ASSESSMENT
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
OPERATION, MAINTENANCE AND DECOMISSIONING
IMPLEMENTATION AND DEMONSTRATION OF COMPLIANCE
Validation
TS 50701
product lifecycle
IEC 62443-4-1 and 4-2
To: Operation, maintenance and decommissioning



3	**Risk analysis and evaluation**	DRA: → Functional Requirements (linked to essential functions) ← Initial Threat Log ← Potential Updates (Zones and Conduits, network plans)	— Detailed Risk Assessment (DRA) (see Clause 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 Clause 8) — Definition of organizational and physical requirements — Definition of security-related application conditions (see Clause 7)

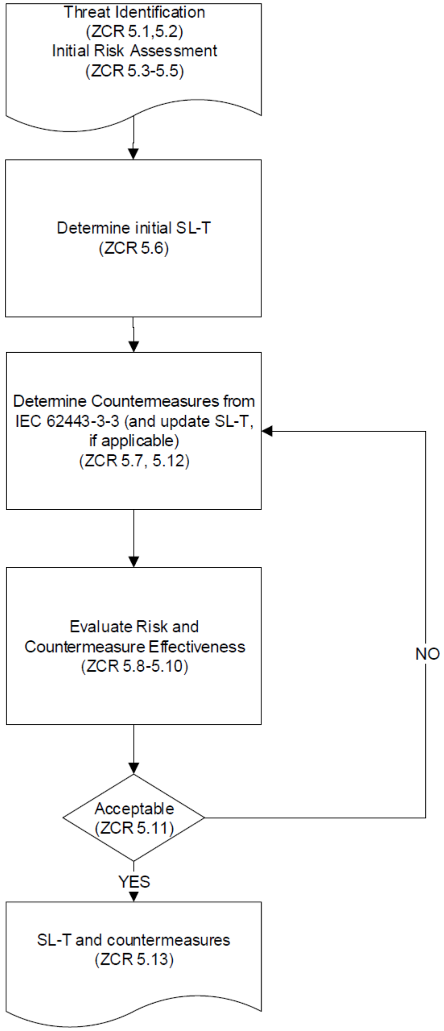
TS 50701 overview – Security Requirements with Rail. notes



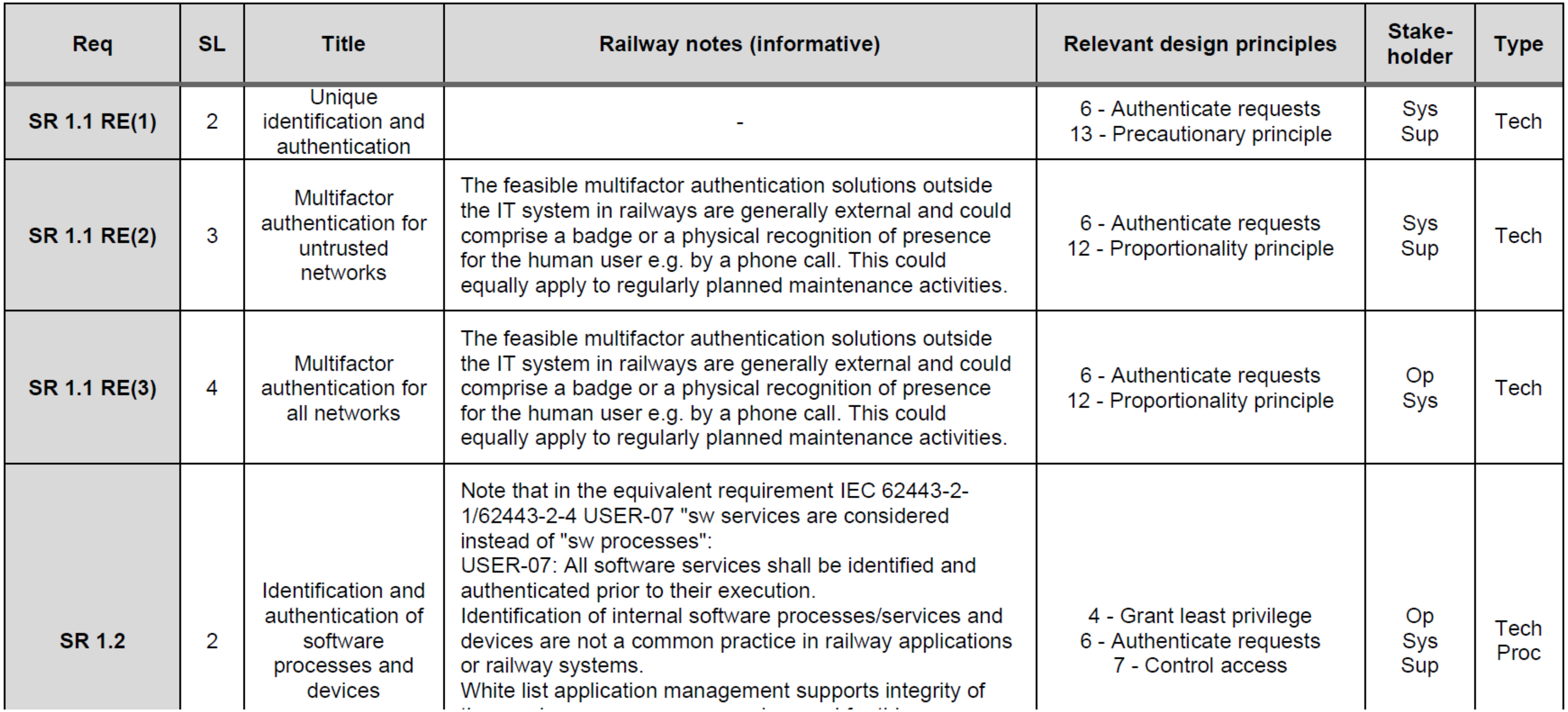
Req	SL	Title	Railway notes (informative)	Relevant design principles	Stake-holder	Type
SR 1.1 RE(1)	2	Unique identification and authentication	-	6 - Authenticate requests 13 - Precautionary principle	Sys Sup	Tech
SR 1.1 RE(2)	3	Multifactor authentication for untrusted networks	The feasible multifactor 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

How is a SL assigned?

- Threats can be identified by using Threat Landscapes from e.g. ENISA, ISF, etc.
- Initial Risk Assessment
  - Zone and conduit building
  - Assessment of possible impacts
- 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.

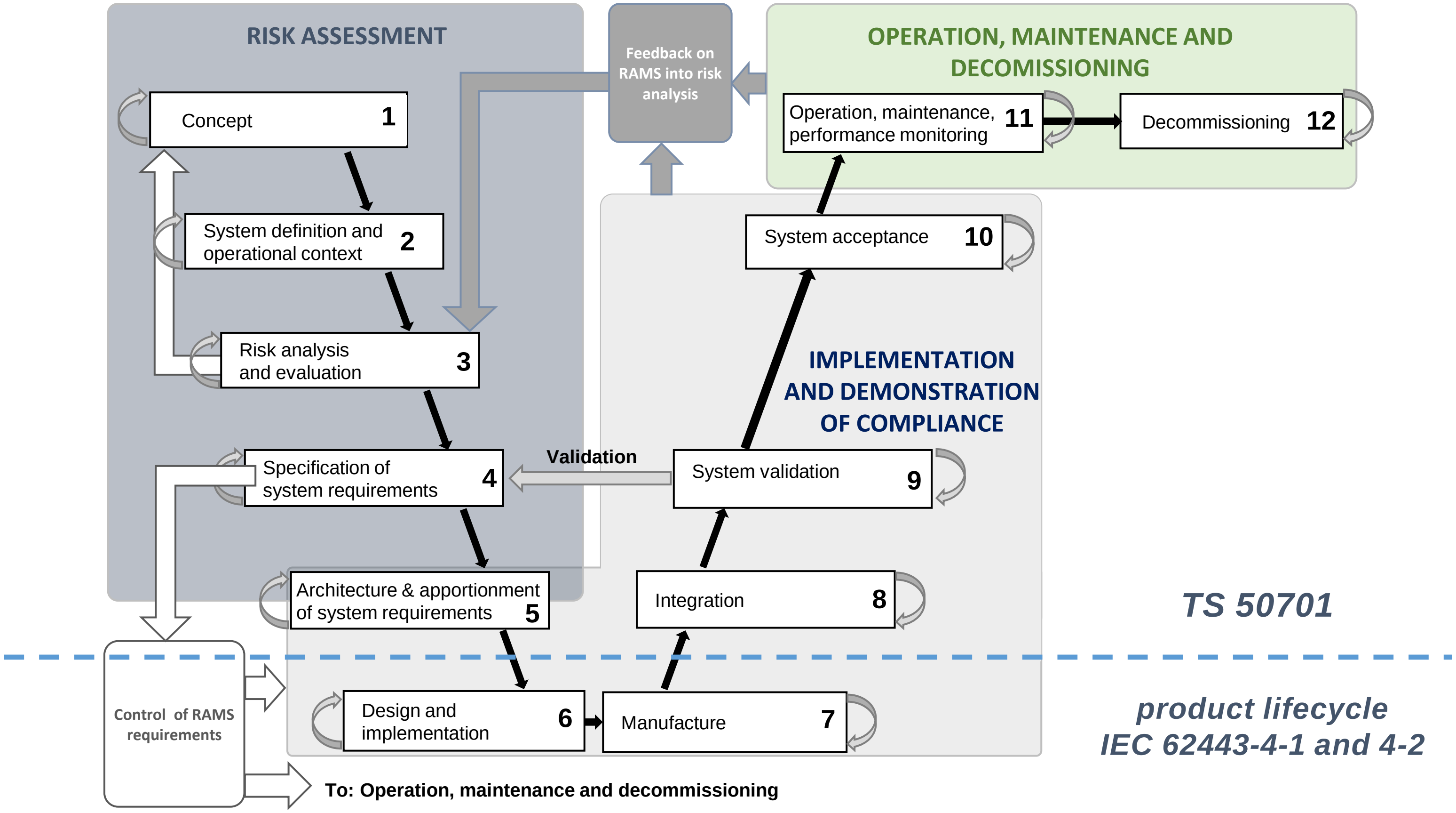


TS 50701 overview – Security Requirements with Rail. notes



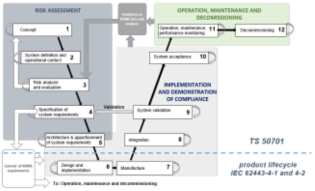
Req	SL	Title	Railway notes (informative)	Relevant design principles	Stake-holder	Type
SR 1.1 RE(1)	2	Unique identification and authentication	-	6 - Authenticate requests 13 - Precautionary principle	Sys Sup	Tech
SR 1.1 RE(2)	3	Multifactor authentication for untrusted networks	The feasible multifactor 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

TS 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
TS 50701
product lifecycle
IEC 62443-4-1 and 4-2

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

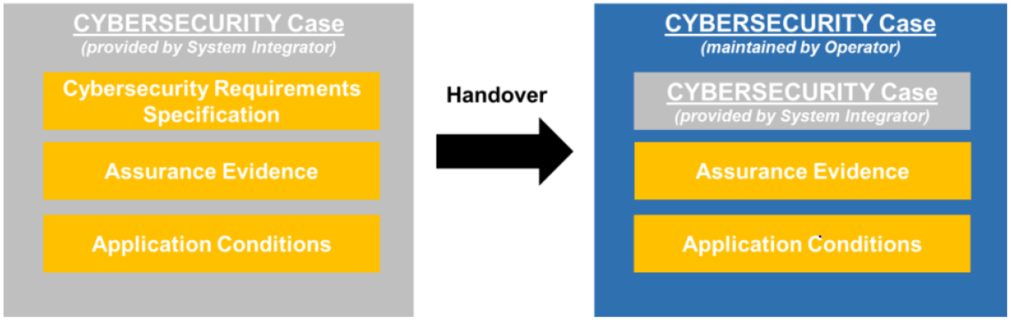
What about Assurance (Phase 9/10)?


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
TS 50701
product lifecycle
IEC 62443-4-1 and 4-2

9	**System Validation**	Cybersecurity validation: ← Cybersecurity case incl. security-related application conditions ← Security guidelines	— Verification of security guidelines — Validation of configuration and security functionality (see 9.4) — Applicability verification of organizational requirements and security-related application conditions (see 9.4)
10	**System acceptance**	Cybersecurity acceptance: ← Cybersecurity case updated incl. security-related application conditions ← Security guidelines updated	— Completion by the System integrator of the cybersecurity case and security-related guidelines (see 9.2 and 9.5) — Security Handover between System Integrator and railway operator — Review of business continuity aspects (incl. incidence response and recovery) for the SuC.

TS 50701 Assurance – 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 must be exported as SecRAC, or
  - partially fulfilled (compensating countermeasures must be defined)
- Safety Case references the Cybersecurity Report
- Cybersecurity Case can be updated without change of the safety case



Content of CyberSecurity Case

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

- Related cybersecurity cases (from includec

Security-related application conditions (could b

- Installation
- Maintenance
- Operation

Conclusion

- Cybersecurity claim
- Residual risks status

Conclusion

- TS 50701 provides a framework for CyberSecurity in the Railway domain
- Today you saw an overview on application during Security Engineering
- Collaboration with IEC in order to make TS 50701 a global CyberSecurity Standard for Railways
  - Work started mid 2022
  - More in the next presentation
- TS 50701 is being improved by returned experience during application
  - Version 2 being published in 2023

Thank you for your attention!

CYBERSHIELD christian.schlehuber@cybershield-consulting.com

Q &A