SAFETY4RAILS

Legal Framework for Certification and Standardisation

Deliverable 9.4

Lead Author: RINA

Contributors: ERARGE&ERGTECH

Dissemination level: PU - Public
Security Assessment Control: passed

The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883532.

D9.4 Legal Framework for Certification and Standardisation		
Deliverable number:	9.4	
Version:	2.1	
Delivery date:	06/10/2022	
Dissemination level:	PU – Public	
Nature:	Report	
Main author(s)	Luca Macchi Daniele Angiati	RINA RINA
Contributor(s) to main deliverable production	Alper Kanak	ERARGE&ERGTECH
Internal reviewer(s)	Stephen Crabbe Atta Badii Antonio De Santiago Laporte	Fraunhofer UREAD MdM
External reviewer(s)	*Any future feedback to be input into future work.*	

Document control			
Version	Date	Author(s)	Change(s)
0.1	01/01/2022	RINA	Initial version
0.2	16/06/2022	RINA	ToC and summary
0.3	21/07/2022	RINA	1st an 2nd chapter
0.4	01/09/2022	ERARGE	3th chapter
1.0	08/09/2022	RINA	Final version and check
2.0	23/09/2022	RINA	Final Version after comments
2.1	06/10/2022	Fraunhofer	Creation of V2.1 from V2.0 with minor formatting and editing.

DISCLAIMER AND COPYRIGHT

ABOUT SAFETY4RAILS

SAFETY4RAILS is the acronym for the innovation project: **Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS**. Railways and Metros are safe, efficient, reliable and environmentally friendly mass carriers, and they are becoming even more important means of transportation given the need to address climate change. However, being such critical infrastructures turns metro and railway operators as well as related intermodal transport operators into attractive targets for cyber and/or physical attacks. **The SAFETY4RAILS project delivers methods and systems to increase the safety and recovery of track-based inter-city railway and intra-city metro transportation.** It addresses both cyber-only attacks (such as impact from WannaCry infections), physical-only attacks (such as the Madrid commuter trains bombing in 2004) and combined cyber-physical attacks which are important emerging scenarios given increasing IoT infrastructure integration.

SAFETY4RAILS concentrates on rush hour rail transport scenarios where many passengers are using metros and railways to commute to work or attend mass events (e.g. large multi-venue sporting events such as the Olympics). When an incident occurs during heavy usage, metro and railway operators have to consider many aspects to ensure passenger safety and security, for example, carry out a threat analysis, maintain situation awareness, establish crisis communication and response, and they have to ensure that mitigation steps are taken and communicated to travellers and other users. **SAFETY4RAILS will improve the handling of such events through a holistic approach.** It will analyse the cyber-physical resilience of metro and railway systems and deliver mitigation strategies for an efficient response, and, in order to remain secure given everchanging novel emerging risks, it will facilitate continuous adaptation of the SAFETY4RAILS solution; this will validated by two rail transport operators and the results will support the re-design of the final prototype.

TABLE OF CONTENTS

ABOUT SAFETY4RAILS 2
Executive summary 4
1. Introduction 5
1.1 Objectives of the task 5
1.2 The structure of the deliverable 5
2. The Legal Framework for standardisation and certification of S4R operations 6
2.1 Applicable regulations, standard and best practice 6
2.2 Standardisation requirements 7
2.3 Measures from existing engineering background and parallel disciplines 35
3. Certification scheme analysis for a future safety and security certification scheme 36
3.1 Certification typology 36
3.2 The Approach 36
3.3 Objects and actors involved 36
3.4 Boundaries and Constraints of the Certification 37
3.5 Activities and Responsibility within the Certification process 40
3.6 Validity of the Certificates 41
3.7 Certification Bodies 41
3.8 Laboratories 41
4. End-to-end IoT-level security standards 41
4.1 Hardware-level security 41
4.2 Nodes and Person Authentication 42
4.3 AI and Blockchain 42
5. Open Points 43
5.1 Hardware-level security 43
5.2 Nodes and Person Authentication 44
5.3 AI and Blockchain 44
6. Conclusion 44
Bibliography 46
ANNEXES 48
ANNEX I. GLOSSARY AND ACRONYMS 48

List of tables

Table 1: Glossary and acronyms 48

List of figures

Figure 1 – Railway physical architecture model (example) (figure 3 of CLC/TS 50701) 38
Figure 2 - Generic high-level railway zone model (example) 39
Figure 3 - TS 50701 vs 50126 V- cycle left side 40

Figure 4 - TS 50701 vs 50126 V- cycle right side 40

Executive summary

This document is Deliverable D9.4 – *Legal Framework for Certification and Standardisation* – of SAFETY4RAILS, aiming to present the legal framework (regulation, Standard and best practice) relevant for SAFETY4RAILS.
The report presents the results of the activities conducted in T9.3 which addresses the following main topics:

1) «This task analysed and defined the legal framework relevant to the standardisation and the certification of the SAFETY4RAILS operations. In this task the relevant applicable regulations, standards and best practice have been considered to determine and harmonise a subset of measures that can comply with the outputs of the other work packages. The objective was to highlight which measures can be inherited/adapted from the existing engineering background, including parallel disciplines (e.g. safety) or international practices, and which specific needs should be addressed as new measures. Particular attention has been addressed to the results of the assessment performed in WP3 (in particular Task 3.1 and Task 3.2).»
2) «The final part of the task was dedicated to the impact appraisal on the certification mechanism (TSI and other EU Regulations) as derived from this analysis, checking whether practices from the Safety Assessment mechanism can be applied to the security to establish an endring Safety and Security Certification Scheme »
3) «ERARGE concentrated on security standards that are related to end-to-end IoT-level security standards and are encountered within the common criteria and NIST Test suites. Moreover, ERARGE will focus on EU regulations related to the smart city paradigm and potential openings in the transportation domain which should be aligned with EU transport policy.»

The starting point for the standards evaluation has been Deliverable D2.4. Additionally, since the CLC/TS 50701 Ref. [24] was published in July 2021, its requirements were added.

A particular focus has been dedicated to CLC/TS 50701 since it aims at defining a cyber security assessment based on the V-cycle of EN 50126 Ref. [8]. This should avoid possible “wrong interaction” between cyber security assessment and safety assessment.

Additionally, in this deliverable some open points related to the standardisation and certification have been highlighted.

1. Introduction

1.1 Objectives of the task

This deliverable reports the activities carried out in Task 9.3 (T9.3). This task is heterogeneous and is mainly aimed at covering three topics: standardisation, harmonisation between Safety and Security in the Certification scheme and the standard related to end-to-end IoT-level security standard.

The work of Task 9.3 has hence been split in three main activities:

1) «This task analysed and defined the legal framework relevant to the standardisation and the certification of the SAFETY4RAILS operations. In this task the relevant applicable regulations, standards and best practices have been considered to determine and harmonise a subset of measures that can comply with the outputs of the other work packages. The objective was to highlight which measures can be inherited/adapted from the existing engineering background, including parallel disciplines (e.g. safety) or international practices and which specific needs should be addressed as new measures. Particular attention has been addressed to the results of the assessment performed in WP3 (in particular Task 3.1 and Task 3.2).»
2) «The final part of the task was dedicated to the impact appraisal on the certification mechanism (TSI and other EU Regulations) as derived from this analysis, checking whether practices from the Safety Assessment mechanism can be applied in the security to establish a an enduring dedicated Safety and Security Certification scheme»
3) «ERARGE concentrated on security standards that are related to end-to-end IoT-level security standards and are encountered within the common criteria and NIST Test suites. Moreover, ERARGE will focus on EU regulations related to the smart city paradigm and potential openings in the transportation domain which should be aligned with EU transport policy. »

The starting point for the standards evaluation has been Deliverable D2.4. Additionally, since the CLC/TS 50701 was published in July 2021, its requirements were added.

Following the steps identified in the CLC/TS 50701 to support cyber security assessment based on the V-cycle of EN 50126 and avoid possible “wrong interaction” between cyber security assessment and safety assessment.

1.2 The structure of the deliverable

The deliverable is structured as follows:

- Section 1 provides legal framework analysis
- Section 2 analysis of future integrated safety and security certification schemes safety and security.
- Section 3 provides concluding remarks.

2. The Legal Framework for standardisation and certification of S4R operations

2.1 Applicable regulations, standard and best practice

The starting point for the legal framework analysis has been Deliverable D2.4 with some integration and deepening of those norms and standards that are considered applicable to the SAFETY4RAILS platform future applications. In Task 9.3 the following steps have been followed:

The inputs from D2.4 have been taken into account for drafting this section which in particular analyses the standards and regulations adopted in order to have a solid normative reference.
The NIS Directive, which applies to railway infrastructure managers, has been identified as the regulatory text applicable to the S4RIS platform. This Directive has been adopted by the Member States of the European Union with some minor differences made to the national implementations.
The NIS Directive required to put in place an adequate system in order to keep the security threats under control and to communicate in good time any security attack received.
It was considered essential to follow the international standards adopted by all operators, such as ISO 27001 Ref. [4] and IEC 62443 Ref. [5], which are also the most widely used in the field of railway security. These two regulatory standards gave rise to a third standard, CLC/TS 50701. In order to complete the regulatory framework in the railway sector CLC/TS 50701.ISO 27001 provides requirements for the Information Security Management Systems and is applicable to any kind of organisation. So as to be compliant with ISO 27001, the organisations must define and put in place a set of security procedures and measures (namely "controls" within the standard itself). S4RIS will be inevitably integrated within the information system of the Infrastructure Managers who adopt it, and consequently it will have to meet security requirements. Though ISO 27001 is not mandatory, it is considered a valid and proper means to implement the NIS Directive (limited to OES security measures). To identify security measures, extensive use was made of ISO 27002, which provides potential controls and control mechanisms that are designed to be implemented with guidance provided within ISO 27001.
IEC 62443 (especially 62443-3-3 and 62443-4-2) provides a thorough and systematic set of cybersecurity recommendations for industrial control systems. Its applicability to the railway environment is proven by CENELEC CLC/TS 50701, which is essentially based on IEC 62443 and provides IEC 62443 requirements with specific notes relevant to the railway environment. Deriving requirements from IEC 62443 enables future S4RIS products to be in line with TS50701. Though S4RIS does not directly fall within the control systems category, it will be connected to railway control systems and it could be part of Operation Centres of the Infrastructure Managers and Railway Undertakings. Consequently, it has been considered appropriate to take this standard into consideration when defining standardisation requirements for S4RIS.

The standards that will be described in the following section should be compared with CLC/TS 50701, which describes cybersecurity in the railway sector. For a railway system to be compliant with the standard, it is necessary to demonstrate that security levels are met during the normal operation and maintenance cycle.

It was analysed that cybersecurity aspects were taken into account, first bringing back the standards present on D2.4 and supplementing them with the new CLC/TS 50701. The analyses will take into account to:
Provide requirements and guidance on cybersecurity activities and deliverables
Be adaptable and applicable to various system lifecycles
Be applicable to both safety and non-safety related systems
Identify interfaces between cybersecurity and other disciplines contributing to railway system lifecycles
Be compatible and consistent with EN 50126-1 when it is applied to the system under consideration

Due to lifecycle differences between safety and cybersecurity, separate safety approval and cybersecurity acceptance as much as possible
Identify the key synchronisation points related to cybersecurity between system integrator and asset owner
Provide a harmonised and standardised way to express technical cybersecurity requirements
Provide cybersecurity design principles promoting simple and modular systems
Enable the usage of market products such as industrial COTS compliant with the 62443 series.

2.2 Standardisation requirements

Starting from the standards identified in D2.4, those that fit in the railway field have been listed, with a brief description.
The tables below marked with (*) are copied from deliverable D2.4.

Short name	Human user identification and authentication (*)
Key objectives	- identify and authenticate each human user
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 1.1 and SR 1.1 (1).
Comments	This requirement deals with identification and authentication of human users.
Reference	ISO 27001, ISO 27002 (A.9.1) IEC 62443-3-3 (SR 1.1)

Short name	Human user identification and authentication
Key objectives	Grant least privilege - Authenticate requests - Control access
Type of requirement	Tech Proc
Description	This includes application interfaces such as web server, file transfer protocol (FTP) server, OPC, and remote desktop interfaces that provide network access to human users and that do not securely convey the authenticated IACS user identity to the application during connection. It is acceptable to implement this requirement in combination with other external authentication solutions including physical security measures in railways
Comments	-
Reference	CLC/TS 50701

Short name	Human user identification and authentication - multifactor for remote connection (*)
Key objectives	- increase the level of security for remote connections
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should comply with IEC 62443-3-3 SR 1.1 (2).
Comments	Two-factor or multi-factor authentication enables a considerable increase in the level of security. It can be based on OTP codes, biometric devices, smart-cards, etc. For specific suggestions on multi-factor authentication refer to NIST Special Publication 800-63B
Reference	ISO 27001, ISO 27002 (A.9.1) IEC 62443-3-3 (SR 1.1)

Short name	Human user identification and authentication – multifactor (*)
Key objectives	- increase the level of security for authentication for any connection

Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should comply with IEC 62443-3-3 SR 1.1 (3).
Comments	Two-factor or multi-factor authentication allows to greatly increase the level of security. It can be based on OTP codes, biometric devices, smart-cards, etc. For specific suggestions on multi-factor authentication refer to NIST Special Publication 800-63B
Reference	ISO 27001, ISO 27002 (A.9.1) IEC 62443-3-3 (SR 1.1)

Short name	Unique identification and authentication
Key objectives	Authenticate requests - Precautionary principle
Type of requirement	Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Multifactor authentication for untrusted networks
Key objectives	Authenticate requests - Proportionality principle
Type of requirement	Tech
Description	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.
Comments	-
Reference	CLC/TS 50701

Short name	Multifactor authentication for all networks
Key objectives	Authenticate requests - Proportionality principle
Type of requirement	Tech
Description	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
Comments	-
Reference	CLC/TS 50701

Short name	Identification and authentication of software processes and devices
Key objectives	Grant least privilege - Authenticate requests 7 - Control access
Type of requirement	Tech Proc
Description	Note that in the equivalent requirement IEC 62443-2-1 / IEC 62443–2-4 USER-07 “sw services are considered instead of “sw processes”: USER-07: All software services will 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 the running processes as a workaround for this requirement. This capability should be incorporated by the operating system. For implementation please refer to the Proportionality Security Design Principle.
Comments	-
Reference	CLC/TS 50701

Short name	Unique identification and authentication of software processes and devices
Key objectives	Authenticate requests - Proportionality principle - Precautionary principle
Type of requirement	Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Non-human user identification and authentication (*)
Key objectives	- identify and authenticate each non-human user
Type of requirement	Functional
Priority rank	Conditional
Description	S4RIS should comply with IEC 62443-3-3 SR 1.2.
Comments	-
Reference	ISO 27001, ISO 27002 (A.9.1) IEC 62443-3-3 (SR 1.2)

Short name	Account management (*)
Key objectives	- provide support for management of users allowed to use the system
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 1.3.
Comments	This requirement deals with managing access to S4RIS by users.
Reference	ISO 27001, ISO 27002 (A.9.2) IEC 62443-3-3 (SR 1.3)

Short name	Account management
Key objectives	Economize mechanism - Authenticate requests - Control access
Type of requirement	Tech Proc
Description	Railways have mostly a distributed system supported by simple passwords. The full account management requires a major change in the existing control/command and IT infrastructure. The issue of maintenance and multiple commercial contractors complicates the issue.
Comments	-
Reference	CLC/TS 50701

Short name	User account uniqueness (*)
Key objectives	- guarantee uniqueness of each user
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 1.4.
Comments	Unique identification of accounts aims to link each user to his/her actions.
Reference	ISO 27001, ISO 27002 (A.9.2.1) IEC 62443-3-3 (SR 1.4)

Short name	Unified account management
Key objectives	Authenticate requests - Make security usable
Type of requirement	Tech
Description	The operators should install a unique account and user administration system in combination with physical security in fulfilment of this requirement. The decision for the appropriate solution is left to the operators ideally in a standardised manner across the railway industry.

Comments	-
Reference	CLC/TS 50701

Short name	Identifier management (*)
Key objectives	Authenticate requests - Make security usable
Type of requirement	Tech
Description	An Identifier is a construct (username, tag) which is associated closely to a user or subscriber. Authentication is a procedure based on a secret given by an identified user or subscriber which enables the verification of it,uniquely. There are currently no solutions for railway environments for this requirement as an inherent system solution. Railways have mostly a distributed system supported by simple passwords. Full account management is often only supported with an external solution in the form of compensating countermeasures. Example of a compensating countermeasure for rolling stock: Furthermore, for some railway control systems, the capability for the driver or the supervisor to quickly interact with such systems is critical. Local emergency actions for the control system should not be hampered by identification requirements. Access to these systems may be restricted by compensating countermeasures. For example, drivers can have free access to cab control systems, without need of further identification, once they have entered into the cabin (with a key) and have inserted their driver licence card. However, they have to identify themselves on their wireless tablet, even if they are inside the cab, because wireless devices can work outside the restricted area, making the countermeasure useless.
Comments	-
Reference	CLC/TS 50701

Short name	Authenticator management
Key objectives	Authenticate requests - Assume secrets not safe - Make security usable
Type of requirement	Tech Proc
Description	In the case that a unique authentication management system for the railway system is not feasible, an external solution based on compensating countermeasures should be considered. Example of a compensating countermeasure for rolling stock: A possible solution is to demand the authentication responsibility from the system in charge of identification. For example, the driver's card reader would not only identify the driver, but also perform the authentication of the card and would undertake this service for all the subsystems connected to it, which are not able to authenticate the driver but trust the card reader.
Comments	-
Reference	CLC/TS 50701

Short name	Hardware security for software process identity credentials
Key objectives	Assume secrets not safe
Type of requirement	Tech
Description	Credentials used as a base of trust will be stored with a Hardware Secure Mechanism. If this for valid reasons is not possible the chain of trust should be supported by a logically Secure Mechanism plus a compensating countermeasure (e.g. monitoring).
Comments	-
Reference	CLC/TS 50701

Short name	Wireless access management
Key objectives	Secure the weakest link - Authenticate requests - Control access - Proportionality principle
Type of requirement	Tech Proc
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Unique identification and authentication
Key objectives	Secure the weakest link - Authenticate requests - Proportionality principle
Type of requirement	Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Secure log-on (*)
Key objectives	- ensure that log-on is implemented according to current best practice
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 1.5.
Comments	Secure log-on is essential to avoid unauthorised users to access the S4RIS system. It may also be provided by interfacing with existing account management systems. Note: username-password approach could be adopted for pilots.
Reference	ISO 27001, ISO 27002 (A.9.4.2) IEC 62443-3-3 (SR 1.5)

Short name	Secure log-on feature 1 (*)
Key objectives	-avoid disclosures of information to unauthorised users
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should apply the implementation guidance in ISO 27002 9.4.2 a).
Comments	This requirement aims to avoid unwanted disclosure of information.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Short name	Secure log-on feature 2 (*)
Key objectives	- reduce probability of unauthorised users logging-on
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should apply the implementation guidance of ISO 27002 9.4.2 c).
Comments	This requirement to discourage unauthorised users.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Short name	Secure log-on feature 3 (*)
Key objectives	- reduce probability of unauthorised users logging-on
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should comply with IEC 62443-3-3 SR 1.10.
Comments	This requirement deals with not providing hints to unauthorized users.
Reference	ISO 27001, ISO 27002 (A.9.4.2) IEC 62443-3-3 (SR 1.10)

Short name	Secure log-on feature 4 (*)
Key objectives	- prevent brute force log-on attempts
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 1.11.
Comments	This requirement prevents brute force attacks on the log-on system. For the use cases, the following values could be adopted: - number of attempts: 5 - period of time: 60 seconds
Reference	ISO 27001, ISO 27002 (A.9.4.2) IEC 62443-3-3 (SR 1.11)

Short name	Secure log-on feature 5 (*)
Key objectives	- record log-on attempts for analysis
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should apply the implementation guidance of ISO 27002 9.4.2 f).
Comments	The analysis of log allows to identify potential attempted or successful breaches.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Short name	Secure log-on feature 6 (*)
Key objectives	- make the user aware of its log-on attempts
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should apply the implementation guidance of ISO 27002 9.4.2 h).
Comments	This requirement warns the user if an outsider has tried to access their account with their username.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Short name	Secure log-on feature 7 (*)
Key objectives	- enhance security of the log-on procedure
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should apply the implementation guidance in ISO 27002 9.4.2 i).
Comments	This requirement reduces the risk of password peeking by unauthorised people.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Short name	Secure log-on feature 8 (*)
Key objectives	- reduce the probability of the password being intercepted
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will apply the implementation guidance in ISO 27002 9.4.2 j).
Comments	Deprecated cyphering mechanism must be avoided.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Short name	Password management (*)
Key objectives	- adopt appropriate password management system
Type of requirement	Functional
Priority rank	Essential

Description	S4RIS will support password management. It can be implemented using an internal password management system or an external/existing password management system
Comments	The system will provide the password management, using internal or external systems. Features of this system are detailed in requirements "Password management feature N"
Reference	ISO 27001, ISO 27002 (A.9.4.3)

Short name	Password management feature 1 (*)
Key objectives	- enable user to choose and change his/her password
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will apply the implementation guidance of ISO 27002 9.4.3 b.
Comments	Password chosen by the users can be easier to remember.
Reference	ISO 27001, ISO 27002 (A.9.4.3)

Short name	Password management feature 2 (*)
Key objectives	- guarantee strong password choice
Type of requirement	Non-functional
Priority rank	Essential/Conditional
Description	S4RIS will/should comply with IEC 62443-3-3 SR 1.7.
Comments	The concept of quality password is described in NIST SP 800-63-3 Annex A, which defines a set of rules and criteria to be applied to ensure that passwords are not easy to guess or find by attackers.
Reference	ISO 27001, ISO 27002 (A.9.4.3) IEC 62443-3-3 (SR 1.7)

Short name	Password management feature 3 (*)
Key objectives	- ensure periodical change of password
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should apply the implementation guidance of ISO 27002 9.4.3 e).
Comments	The definition of the password duration is the choice of the end-users, based on their internal policies. Note: for the use cases, this duration might be set to few days in order that it may be checked.
Reference	ISO 27001, ISO 27002 (A.9.4.3)

Short name	Password management feature 4 (*)
Key objectives	- avoid password re-use
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should apply the implementation guidance of ISO 27002 9.4.3 f).
Comments	The definition time for which a password cannot be re-used is the choice of end users, based on their internal policies.
Reference	ISO 27001, ISO 27002 (A.9.4.3)

Short name	Strength of password-based authentication
Key objectives	Assume secrets not safe - Make security usable - Secure Defaults
Type of requirement	Tech Proc
Description	This will be a big challenge especially for the maintainers. They are used to very simple passwords today and to a non-personal (role specific) login.

	However SR 1.7 is essential because most components cannot be protected against brute force login attempts. In the case that this requirement cannot be fulfilled the integrity of authentication information should be supported by external means and compensating countermeasures (For example, use of personal card readers to control access to restricted areas and functions)
Comments	-
Reference	CLC/TS 50701

Short name	Password generation and lifetime restrictions for human users
Key objectives	Assume secrets not safe - Make security usable
Type of requirement	Tech
Description	Lifetime restriction for human users is not currently consistently implemented in railways. To support this, an external solution with additional system capability can be used e.g. for authentication control as a compensating countermeasure.
Comments	-
Reference	CLC/TS 50701

Short name	Password lifetime restrictions for all users
Key objectives	Authenticate requests - Assume secrets not safe - Make security usable
Type of requirement	Proc Tech
Description	In addition, the railway application should enforce password minimum and maximum lifetime restrictions for human user
Comments	-
Reference	CLC/TS 50701

Short name	Public Key Infrastructure (*)
Key objectives	- provide support to PKI certificates
Type of requirement	Functional
Priority rank	Conditional
Description	S4RIS should comply with IEC 62443-3-3 SR 1.8.
Comments	Management of Public Key according to recognised best practice is fundamental when Public Key mechanisms are employed. Examples of well-known practice: IETF RFC 3647 or PKCS #11 Cryptographic Token Interface Base Specification.
Reference	ISO 27001, ISO 27002 (A.10.1.2) IEC 62443-3-3 (SR 1.8)

Short name	Public Key Infrastructure (PKI) Certificate
Key objectives	Assume secrets not safe - Make security usable
Type of requirement	Proc Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Public Key authentication (*)
Key objectives	- detail public key authentication
Type of requirement	Functional
Priority rank	Conditional
Description	In relation to public key authentication, S4RIS should provide the capabilities listed by IEC 62443-3-3 SR 1.9

Comments	This requirement provides further details on Public Key authentication.
Reference	ISO 27001, ISO 27002 (A.10.1.2) IEC 62443-3-3 (SR 1.9)

Short name	Strength of public key authentication
Key objectives	Authenticate requests - Assume secrets not safe - Make security usable
Type of requirement	Tech Proc
Description	In the case that the given requirements for validation of certificates cannot be supported in a railway system, an external solution (e.g. an offline copy of the CA that is updated every 24 h) as compensating countermeasure should be established.
Comments	-
Reference	CLC/TS 50701

Short name	Monitoring of access from untrusted networks (*)
Key objectives	- to monitor and control access from untrusted networks
Type of requirement	Functional
Priority rank	Conditional
Description	S4RIS should comply with IEC 62443-3-3 SR 1.3.
Comments	-
Reference	IEC 62443-3-3 (SR 1.13)

Short name	User access provisioning (*)
Key objectives	- provide appropriate level of access based on access policy and user privileges
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 2.1.
Comments	This requirement addresses the concept of segregation of duties. S4RIS functionalities will be available only to users who are authorised to use them. For example, an operator might be enabled to operate the Monitoring part but not authorised to operate the Risk-Analysis part, so the functions will be accessible to authorised users only. Note: it is out of scope to determine the policy to assign user access privileges to operators. For use cases, it can be acceptable to check that different users can access different functions of S4RIS.
Reference	ISO 27001, ISO 27002 (A.9.2.2; A.9.2.3) IEC 62443-3-3 (SR 2.1)

Short name	Information access restriction (*)
Key objectives	- provide a mean to administrate access rights of users
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will apply the implementation guidance in ISO 27002 9.4.1.
Comments	A mechanism to manage the access rights of users will be implemented in S4RIS. For example, a menu accessible only by an administrator could be implemented for this purpose. Note: the definition of the policy to manage access rights of the users is out of the scope of the SAFETY4RAILS project.
Reference	ISO 27001, ISO 27002 (A.9.4.1)

Short name	Identification and monitoring of access through wireless connection (*)

Key objectives	- to identify wireless access - to monitor and restrict wireless connections
Type of requirement	Functional
Priority rank	Conditional
Description	S4RIS should comply with IEC 62443-3-3 SR 1.6 and SR 2.2.
Comments	Wireless access technologies are more vulnerable to physical attacks and should be managed through dedicated measures.
Reference	IEC 62443-3-3 (SR 1.6, SR 2.2)

Short name	Wireless use control
Key objectives	Economize mechanism - Authenticate requests - Control access
Type of requirement	Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Session lock
Key objectives	- ensure that after a period of inactivity, the sessions are locked - reduce probability of unauthorised access
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 2.5.
Comments	The definition of the timer duration is the choice of the end users, based on their internal policies.
Reference	ISO 27001, ISO 27002 (A.9.2; A.12.1.1) IEC 62443-3-3 (SR 2.5)

Short name	Session lock
Key objectives	Economise mechanism - Control access
Type of requirement	Tech
Description	In view of the safety critical nature of the railway environment, session locks should be carefully applied so as not to interact adversely with system availability and access to essential functions. For example, the user screen could be locked upon user request or after a configured period of inactivity and require re-authentication if an authorised user wants to unlock it.
Comments	-
Reference	CLC/TS 50701

Short name	Termination of remote sessions (*)
Key objectives	- ensure that after a period of inactivity, the sessions are terminated - reduce probability of unauthorised access
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 2.6.
Comments	This requirement aims to avoid unauthorised users gaining access to the system using opened and unused sessions. For details refer to IEC 62443-3-3 (SR 2.6)
Reference	ISO 27001, ISO 27002 (A.9.2; A.12.1.1) IEC 62443-3-3 (SR 2.6)

Short name	Remote session termination
Key objectives	Economise mechanism - Control access

Type of requirement	Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Limit of contemporary sessions (*)
Key objectives	- limit the possibility of DoS attack
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 2.7.
Comments	This requirement enables control of the number of connected users. The number of sessions could be pre-defined or configurable by administrators. For details refer to IEC 62443-3-3 (SR 2.7)
Reference	ISO 27001, ISO 27002 (A.9.2; A.12.1.1) IEC 62443-3-3 (SR 2.7)

Short name	Audit of events related to security (*)
Key objectives	- improve effectiveness and efficiency of audit activities - reduce the impact of audit activities
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 2.8.
Comments	The complete definition of auditable events is out of scope of the present document.
Reference	ISO 27001, ISO 27002 (A.12.4.1; A.12.7.1) IEC 62443-3-3 (SR 2.8)

Short name	Audit storage (*)
Key objectives	-avoid accidental loss of audit records
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should comply with IEC 62443-3-3 SR 2.9.
Comments	The definition of the audit storage size is out of the scope of the present document.
Reference	ISO 27001, ISO 27002 (A.12.7.1) IEC 62443-3-3 (SR 2.9)

Short name	Audit storage capacity
Key objectives	Audit and monitor
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Alerting of audit process fail (*)
Key objectives	-minimise the loss of audit records
Type of requirement	Functional
Priority rank	Conditional
Description	S4RIS should comply with IEC 62443-3-3 SR 2.10.
Comments	-
Reference	ISO 27001, ISO 27002 (A.12.7.1) IEC 62443-3-3 (SR 2.10)

Short name	Response to audit processing failures
Key objectives	Audit and monitor
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Timestamp for audit(*)
Key objectives	- improve audit records management
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 2.11.
Comments	-
Reference	ISO 27001, ISO 27002 (9.2; A.12.4.4) IEC 62443-3-3 (SR 2.11)

Short name	Non-repudiation of users (*)
Key objectives	-prevent false claims by users
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 2.12.
Comments	This requirement prevents users claiming they have not performed certain actions. For details refer to IEC 62443-3-3 (SR 2.12)
Reference	ISO 27001, ISO 27002 (A.12.7.1) IEC 62443-3-3 (SR 2.12)

Short name	Access to audit information (*)
Key objectives	-prevent unauthorized modifications to audit records
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 3.9 and SR 6.1.
Comments	The audit information is important for security breach recovery and investigations.
Reference	ISO 27001, ISO 27002 (A.12.4.2, A.12.7.1) IEC 62443-3-3 (SR 3.9, SR 6.1)

Short name	Information classification (*)
Key objectives	- ensure that information receives an appropriate level of protection in accordance with its importance
Type of requirement	Functional
Priority rank	Essential/Conditional
Description	The information generated by S4RIS that can be stored and/or shared will/should be classified according to their value, criticality and sensitivity.
Comments	Classification of information is important for compliance to ISO 27001. In this context, all the information produced by the system and stored/shared (e.g., pdf reports, Excel tables, any other kind of exported files) will be classified according to a scheme. For example, reports generated by The Risk Assessment Tool part of S4RIS might highlight criticalities currently in place within the Infrastructure Manager organisation or systems, and this kind of information will be protected from unauthorised access and circulation.
Reference	ISO 27001, ISO 27002 (A.8.2.1)

Short name	Information classification scheme (*)
Key objectives	- ensure that information receives an appropriate level of protection in accordance with its importance
Type of requirement	Non-functional
Priority rank	Essential/Conditional
Description	The classification of information will/should be carried out: a) according to end-user's existing procedures, or; b) manually by the operator upon generation of information, or; c) automatically by the system upon generation of the information. If case b) is implemented, the classification of generated information will/should not be skippable by the operator.
Comments	Classification of information will/should be carried out according to end-user company procedures, if these are available. If the company does not have any classification procedure, the classification can be applied automatically by the system upon generation of the information (e.g., according to pre-defined rules) or by the operator. In the latter case, he/she will/should be obliged to apply classification before carrying out any other action. NOTE: the definition of classification procedures and criteria is out of the scope and will be determined by the end-user company. S4RIS will only provide the possibility of classifying information.
Reference	ISO 27001, ISO 27002 (A.8.2.1)

Short name	Information labelling (*)
Key objectives	- ensure that information receives an appropriate level of protection in accordance with its importance
Type of requirement	Functional
Priority rank	Essential/Conditional
Description	The information generated by S4RIS that can be stored and/or shared will/should be labelled accordingly to their value, criticality and sensitivity.
Comments	Labelling of classified information is important for compliance with ISO 27001. It enables easy identification of the level of classification of the information
Reference	ISO 27001, ISO 27002 (A.8.2.2)

Short name	Information labelling scheme (*)
Key objectives	- ensure that information receives an appropriate level of protection in accordance with its importance
Type of requirement	Non-functional
Priority rank	Essential/Conditional
Description	The labelling of information will/should be carried out: a) according to end-user's existing procedures, or; b) manually by the operator upon generation of information, or; b) automatically by the system upon generation of the information. In the case that b) is implemented, the labelling of generated information will/should not be skippable by the operator.
Comments	Labelling of classified information will/should be carried out according to end-user's procedures if these are available. If the company does not have any related procedure, the labelling will be carried out automatically by the system upon generation of the information (e.g., according to pre-defined

	rules) or by the operator. In the latter case, they will be obliged to apply classification before carrying out any other action. A sample labelling that might be used for use cases is: - Public: information intended for internal or public distribution whose unintended distribution would cause minimum harmful consequences; Sensitive: information that would have medium-high harmful consequences if disclosed; Confidential: information that would have high harmful consequences if disclosed.
Reference	ISO 27001, ISO 27002 (A.8.2.2)

Short name	Protection of communications (*)
Key objectives	- to guarantee integrity of communications - to guarantee confidentiality of communications
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 (SR 3.1).
Comments	Information integrity and confidentiality are two of the fundamental concepts in security and will be enforced for all the connections that involve exchange of information between clients/servers and S4RIS/external systems.
Reference	ISO 27001, ISO 27002 (A.10.1; A.13) IEC 62443-3-3 (SR 3.1)

Short name	Dealing with errors in a secure way (*)
Key objectives	- avoid disclosures of information that might aid an attacker
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 3.7.
Comments	OWASP (Open Web Application Security Project) CODE REVIEW GUIDE 2.0 provides details on how to deal with error handling.
Reference	ISO 27001, ISO 27002 (A.14.2.1; A.14.2.7) IEC 62443-3-3 (SR 3.7)

Short name	Information backup (*)
Key objectives	- to minimise data loss in case of attacks
Type of requirement	Other
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 7.3.
Comments	ISO 22301 should also be considered. Identification and location of information subject to backup and the definition of the relevant policy is out of the scope of this document.
Reference	ISO 27001, ISO 27002 (A.12.3) IEC 62443-3-3 (SR 7.3) ISO 22301

Short name	Recovery and restore (*)
Key objectives	- to be able to restore the system
Type of requirement	Other
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 7.4.
Comments	ISO 22301 should also be considered.
Reference	ISO 27001, ISO 27002 (A.17.1) IEC 62443-3-3 (SR 7.4)

	ISO 22301

Short name	Inventory of assets (*)
Key objectives	- provide full inventory of assets composing S4RIS system
Type of requirement	Other
Priority rank	Conditional
Description	The assets associated with information processing that are part of S4RIS should be identified and an inventory of these assets should be drawn up.
Comments	The inventory of assets composed byS4RIS would be an added value for companies applying ISO 27001 and ISO 55000 standards. The process of compiling an inventory of assets is an important prerequisite for risk management (refer to ISO/IEC 27005). Examples of assets might be (not comprehensive list): - Hardware; - Software; - Information (digital and physical); - Infrastructure.
Reference	ISO 27001, ISO 27002 (A.8.1.1) IEC 62443-3-3 (SR 7.8)

Short name	Source code protection (*)
Key objectives	- prevent unauthorised access to source code
Type of requirement	Non-functional
Priority rank	Essential
Description	Source code will not be included in clear text within the system, neither on clients nor on servers.
Comments	The S4RIS system will not include any kind of accessible source code in clear text. The overall management of source code is considered out of scope.
Reference	ISO 27001, ISO 27002 (A.9.4.5)

Short name	Infrastructure monitoring(*)
Key objectives	- monitor IT/OT infrastructure
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will comply with IEC 62443-3-3 SR 6.2.
Comments	Monitoring of infrastructures is considered essential for dealing with technical vulnerabilities. Detection and analysis of anomalies enables the ability to identify, prevent and correct vulnerabilities possibly before they are exploited. Note: this requirement should be addressed by means of Monitoring Methods developed in WP4
Reference	ISO 27001, ISO 27002 (A.12.6) IEC 62443-3-3 (SR 6.2)

Short name	Integration of a security incident tracking system form (*)
Key objectives	- to guarantee tracking of incidents
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS will assist the person reporting in order to provide a fast submission of incident tracking forms.
Comments	When possible, fields in the form can be filled automatically from data gathered from the event. The system should distinguish between the

	different incident management phases, with clear roles defined for each phase. For more details, refer to ISO 27035 (A. 5 & Annex B). The topic of incident response and crisis management will be further developed in T3.5. This requirement is also relevant to T5.5. Reference Ref. [45], Ref. [46] and Ref. [47] should be taken into consideration.
Reference	ISO 27035

Short name	Overall security event / incident / vulnerability database (*)
Key objectives	- to keep a record of security events / incidents /vulnerabilities
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will integrate a security event/incident/vulnerability database drawing information from the incident tracking system form.
Comments	The database should be used to keep a historical record of all security events / incidents / vulnerabilities. Read-write and read-only permissions should be enforced under a role-based approach. For more details, refer to ISO 27035 (A. 5 and Annex B). The topic of incident response and crisis management will be further developed in T3.5. This requirement is also relevant to T5.5. Reference Ref. [45], Ref. [46] and Ref. [47] should be taken into consideration.
Reference	ISO 27035

Short name	Automatic correlation of different incidents detected (*)
Key objectives	- to enable better decision support
Type of requirement	Functional
Priority rank	Conditional
Description	S4RIS should perform automatic correlation of different incidents detected.
Comments	This activity is to verify if the incident is connected to any other event/incident or if it is the result of another incident. This is important in prioritising efforts while managing various events/incidents. For more details, refer to ISO 27035 (A 5.2.2).. The topic of incident response and crisis management will be further developed in T3.5. This requirement is also relevant to T5.5. Reference Ref. [45], Ref. [46] and Ref. [47] should be taken into consideration.
Reference	ISO 27035

Short name	Security incident management system governance (*)
Key objectives	- to guarantee that each user accesses only information for which they have authorisation
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS will allow/support the integration of the security incident management system as defined in ISO 27035, following a role-based approach.
Comments	The topic of incident response and crisis management will be further developed in T3.5. This requirement is also relevant to T5.5. Reference Ref. [45], Ref. [46] and Ref. [47] should be taken into consideration.
Reference	ISO 27035

Short name	Attributes relevant to security incident management (*)
Key objectives	- to enable better decision support during response
Type of requirement	Non-functional
Priority rank	Essential

Description	S4RIS security incident management system will include relevant attributes, such as significance, priority and acceptable interruption window should be integrated into the security incident management system. S4RIS will order the responses to information security incidents happening simultaneously based on these attributes.
Comments	This is relevant to the assessment of impacts for each particular incident. For more details, refer to ISO 27035 (A. 5.2). The topic of incident response and crisis management will be further developed in T3.5. This requirement is also relevant to T5.5. Reference Ref. [45], Ref. [46] and Ref. [47] should be taken into consideration.
Reference	ISO 27035

Short name	Collection of evidence before shutdown. (*)
Key objectives	- to collect evidence for future forensics investigations
Type of requirement	Functional
Priority rank	Essential
Description	Once an incident has been detected, S4RIS will collect all volatile data will be collected before the affected system is shut down. For more details, refer to ISO 27035 (A. 5.3).
Comments	The topic of incident response and crisis management will be further developed in T3.5. This requirement is also relevant to T5.5. Reference Ref. [45], Ref. [46] and Ref. [47] should be taken into consideration.
Reference	ISO 27035

Short name	Guidelines to inform as to who is responsible for internal and external communications (*)
Key objectives	- to manage external and internal communications
Type of requirement	Non-functional
Priority rank	Essential
Description	Clear guidelines will be made available and easily accessible to inform those responsible for internal and external communications.
Comments	May need to occur in several stages: a usefulset of recommendations in this regard is provided in ISO 27035 (A. 5.3). Communication procedures could be defined based on incident type. The topic of incident response and crisis management will be further developed in T3.5. This requirement is also relevant to T5.5. Reference Ref. [45], Ref. [46] and Ref. [47] should be taken into consideration.
Reference	ISO 27035

Short name	Video Coding and metadata representation(*)
Key objectives	- to ensure a common format for video applications within the platform
Type of requirement	Other
Priority rank	Conditional
Description	The videos and metadata exported from the system should comply with ISO 22311.
Comments	ISO 22311 defines requirements for video format and metadata in the frame of video surveillance, to ensure compatibility.
Reference	ISO 22311

Short name	Hardware security for public key authentication
Key objectives	Assume secrets are not safe 9 - Make security usable
Type of requirement	Tech

Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Authenticator feedback
Key objectives	Assume secrets not safe - Make security usable
Type of requirement	Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Unsuccessful login attempts
Key objectives	Authenticate requests - Control access - Make security usable
Type of requirement	Tech
Description	For mission or safety critical systems that deliver essential railway functions, limitation on login attempts may result in system or function unavailability and adversely affect safety. Implementation of this requirement should be fully cognisant of safety and operational availability implications. For example, the freezing of a system (e.g. safe stop in an ETCS Level 2 system) can lead to an unsafe situation. Thus, the required system reaction will be defined with respect to safety and availability.
Comments	-
Reference	CLC/TS 50701

Short name	System use notification
Key objectives	Authenticate requests - Make security usable - Promote privacy
Type of requirement	Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Access via untrusted networks
Key objectives	Audit and monitor
Type of requirement	Proc Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Explicit access request approval
Key objectives	Authenticate requests - Precautionary principle
Type of requirement	Proc Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Authorisation enforcement
Key objectives	Grant least privilege - Authenticate requests - Control access
Type of requirement	Tech Proc

Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Authorisation enforcement for all users
Key objectives	Grant least privilege - Authenticate requests - Control access
Type of requirement	Tech Proc
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Permission mapping to roles
Key objectives	Grant least privilege- Authenticate requests - Control access
Type of requirement	Tech Proc
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Supervisor override
Key objectives	Grant least privilege - Authenticate requests - Control access
Type of requirement	Tech Proc
Description	Railway operators do not generally have a supervisor to oversee the integrity of their actions and decisions. There is always one person fully responsible for a task (e.g. cab driver for his train running). Supervisor override is common in railways in order to manually accept exceptional situations. These are documented in a juridical way.
Comments	-
Reference	CLC/TS 50701

Short name	Dual approval
Key objectives	Grant least privilege - Authenticate requests - Control access
Type of requirement	Tech Proc
Description	This may conflict with time critical activities/functions. In the case of such conflicts, this requirement should be implemented with alternative approaches to establish the chain of trust efficiently. For example, changing a set point in the TCMS that can affect the computation of the speed of the train should require a dual approval; bypassing the ETCS control of the speed of the train may require a pre-defined sequence of actions, carefully chosen to minimise the risk of accidental execution, performed by the driver in case of/to avoid danger.
Comments	-
Reference	CLC/TS 50701

Short name	Use control for portable and mobile devices
Key objectives	Authenticate requests - Control access - Secure Defaults
Type of requirement	Tech Proc
Description	Portable and mobile devices are already widely used in railway infrastructure. For example, for diagnostic purposes but also for safety

	relevant purposes such as shunting / track works. A secure management of mobile access is crucial in the safety critical railway environment.
Comments	-
Reference	CLC/TS 50701

Short name	Mobile code
Key objectives	Authenticate requests - Control access - Secure Defaults
Type of requirement	Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Concurrent session control
Key objectives	Economize mechanism - Control access
Type of requirement	Tech Proc
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Auditable events
Key objectives	Audit and monitor
Type of requirement	Tech
Description	-
Comments	-
Reference	CLC/TS 50701

Short name	Centrally managed, system-wide audit trail
Key objectives	Audit and monitor
Type of requirement	Tech
Description	Components and sub-systems that log events locally should ensure the monitoring and logging information is transferred to a centrally managed system. There may be a time delay between the local logging data and the transfer to the central system
Comments	-
Reference	CLC/TS 50701

Short name	Warn when audit record storage capacity threshold reached
Key objectives	Audit and monitor
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Timestamps
Key objectives	Audit and monitor
Type of requirement	Tech
Description	

Comments	-
Reference	CLC/TS 50701

Short name	Internal time synchronisation
Key objectives	Audit and monitor
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Protection of time source integrity
Key objectives	Audit and monitor
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Non-repudiation for human users
Key objectives	Authenticate requests
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Non-repudiation for all users
Key objectives	Authenticate requests
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Communication integrity
Key objectives	Authenticate requests - Continuous protection
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Cryptographic integrity protection
Key objectives	
Type of requirement	
Description	The cryptographic mechanisms employed should be secure. Rolling stock and restricted network segments with an adequate boundary, intrusion detection and diverse transmission channel (e.g. use of Ethernet and MVB) can use these as compensating countermeasures. Open untrusted networks without compensating countermeasures require this extra protection in railways.
Comments	-
Reference	CLC/TS 50701

Short name	Malicious code protection
Key objectives	Secure the weakest link - Defence-in-depth - Audit and monitor - Continuous Protection - Trusted Components
Type of requirement	Tech Proc
Description	Prevention means mechanisms such as removable media control, and workstation and laptop management policies, used in conjunction with means of detection at railway system entry points (e.g. USB cleaning stations, IDS, etc.) may be preferred as a compensating security measure from detection mechanisms deployed on all railway embedded devices. Use of USB ports should be strictly limited. When no other solution is available, USB controller and OS driver hardening should be employed to prevent execution of code from USB devices. A secure boot mechanism and a white list application management on operating system/firmware and application layers is required to ensure only authorised software is permitted and executed.
Comments	-
Reference	CLC/TS 50701

Short name	Malicious code protection on entry and exit points
Key objectives	Control Access - Proportionality principle
Type of requirement	Tech Proc Env
Description	This RE should be managed at SL1 level to be consistent with SR 3.2 in railways
Comments	-
Reference	CLC/TS 50701

Short name	Central management and reporting for malicious code protection
Key objectives	Make security usable
Type of requirement	Tech Proc
Description	Malware and malicious code protection should be centrally managed for integrity and consistency in railways. SIEM protection is largely a dynamic anomaly detection/protection mechanism and may prove inadequate for malicious code protection.
Comments	-
Reference	CLC/TS 50701

Short name	Security functionality verification
Key objectives	Fail secure - Audit and monitor
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Automated mechanisms for security functionality verification
Key objectives	Make security usable
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Security functionality verification during normal operation
Key objectives	Make security usable
Type of requirement	Tech Proc
Description	This RE needs to be carefully implemented to avoid detrimental effects. It may not be suitable for safety systems
Comments	-
Reference	CLC/TS 50701

Short name	Software and information integrity
Key objectives	Assume secrets not safe - Audit and monitor - Precautionary principle
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Automated notification about integrity violations
Key objectives	Make security usable - Continuous Protection
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Input validation
Key objectives	Defence-in-depth - Control Access - Continuous Protection
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Deterministic output
Key objectives	Fail secure - Proportionality principle - Precautionary principle
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Error handling
Key objectives	Make security usable - Promote privacy - Audit and monitor
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Session integrity
Key objectives	Authenticate requests - Control Access
Type of requirement	Tech

Description	
Comments	-
Reference	CLC/TS 50701

Short name	Invalidation of session IDs after session termination
Key objectives	Make security usable
Type of requirement	Tech Op
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Protection of audit information
Key objectives	Grant least privilege
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Audit records on write-once media
Key objectives	Precautionary principle
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Information confidentiality
Key objectives	Grant least privilege - Assume secrets not safe - Secure Metadata Management - Secure Defaults
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Protection of confidentiality at rest or in transit via untrusted networks
Key objectives	Grant least privilege - Authenticate requests - Control access - Assume secrets not safe- Promote privacy
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Protection of confidentiality across zone boundaries
Key objectives	Grant least privilege - Authenticate requests - Control access - Assume secrets not safe- Promote privacy
Type of requirement	Tech Proc
Description	
Comments	-

Reference	CLC/TS 50701

Short name	Information persistence
Key objectives	Control access - Secure Metadata Management - Secure Defaults
Type of requirement	Tech Proc
Description	Current railway applications do not implement extensive permission management so implementation of this requirement for information purging in components and systems is challenging. Read Authorisation should not be the only criteria for data/information criticality that qualifies for purging.
Comments	-
Reference	CLC/TS 50701

Short name	Purging of shared memory resources
Key objectives	Assume secrets not safe
Type of requirement	
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Use of cryptography
Key objectives	Defend in depth - Authenticate requests - Assume secrets not safe
Type of requirement	Tech Proc
Description	The railway application product supplier should document the practices and procedures relating to cryptographic key establishment and management. The railway application should utilise established and tested encryption and hash algorithms, such as the advanced encryption standards.
Comments	-
Reference	CLC/TS 50701

Short name	Network segmentation
Key objectives	Secure the weakest link - Defend in depth
Type of requirement	Tech
Description	In response to an incident, it may be necessary to break the connections between different network segments. In this event, the services necessary to support essential operations should be maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example, dynamic host configuration protocol (DHCP), domain name service (DNS) or local CAs. It may also mean that some critical control systems and safety-related systems be designed from the beginning to be completely isolated from other networks.
Comments	-
Reference	CLC/TS 50701

Short name	Physical network segmentation
Key objectives	Secure the weakest link - Defend in depth
Type of requirement	Tech

Description	Independence from non-control networks is required at SR 5.1 RE(1). In the case that physical segregation is technically not feasible or may even cause an increase in cybersecurity risks, a logical segregation concept is acceptable explicitly if the following associated SRs [SR 1.2, SR 1.8, SR 1.9, SR 3.1/SR 3.1 RE 1, SR 3.7, SR 4.1/SR 4.1 RE 1,, SR 6.2, SR 1.5 RE 1] are fulfilled
Comments	-
Reference	CLC/TS 50701

Short name	Independence from non-railway application networks
Key objectives	Secure the weakest link - Defend in depth
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Logical and physical isolation of critical networks
Key objectives	Secure the weakest link - Defend in depth
Type of requirement	Tech
Description	The criticality of a railway application is determined by the risk assessment and that should influence the logical and physical isolation. The usage of segmentation methods such as different fibres or colours for fibre-optic cables or the usage of cryptographic measures like those mentioned in EN 50159 are ways to implement this requirement in railway applications.
Comments	-
Reference	CLC/TS 50701

Short name	Zone boundary protection
Key objectives	Secure the weakest link - Defend in depth
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Deny by default, allow by exception
Key objectives	Control Access
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Fail close
Key objectives	
Type of requirement	Tech
Description	Railway safety architectures do not generally permit such behaviours on networks. All essential functions should continue, and non-essential functions be stopped in the event of boundary protection violations

Comments	-
Reference	CLC/TS 50701

Short name	General purpose person-to-person communication restrictions
Key objectives	Defend in depth
Type of requirement	Tech
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Audit log accessibility
Key objectives	Grant least privilege - Authenticate requests - Control access - Make security usable - Audit and monitor - Continuous Protection
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Programmatic access to audit logs
Key objectives	Authenticate requests - Control access - Make security usable - Audit and monitor
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Continuous monitoring
Key objectives	Authenticate requests - Control access - Audit and monitor - Continuous Protection
Type of requirement	Tech Proc Tools
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Denial of service protection
Key objectives	Defend in depth - Control access
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Manage communication loads
Key objectives	Defend in depth - Control access
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Limit DoS effects to other systems or networks
Key objectives	Defend in depth - Control access

Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Resource management
Key objectives	Defend in depth - Grant least privilege - Authenticate requests - Control access
Type of requirement	Tech Proc
Description	Watchdog based time allocation and scheduling is prevalent in the safety critical railway environment and applications. This is largely applied at monitoring rather than control level.
Comments	-
Reference	CLC/TS 50701

Short name	Control system backup
Key objectives	Fail secure - Assume secrets not safe - Continuous Protection - Secure Metadata Management - Secure Defaults
Type of requirement	Tech Proc
Description	Configuration management based on baselines are employed in most railway products. The identity and location of critical files should be known at application level. The ability to conduct backups, specifically the critical information and files, should be supported by railway applications.
Comments	-
Reference	CLC/TS 50701

Short name	Backup verification
Key objectives	Fail secure - Assume secrets not safe - Continuous Protection - Secure Metadata Management - Secure Defaults
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Backup Automation
Key objectives	Assume secrets not safe - Secure Metadata Management - Secure Defaults
Type of requirement	Tech Proc
Description	Automate backup based on a configurable frequency
Comments	-
Reference	CLC/TS 50701

Short name	Control system recovery and reconstitution
Key objectives	Fail secure- Assume secrets not safe 14 - Continuous Protection - Secure Metadata Management - Secure Defaults
Type of requirement	Tech Proc
Description	In view of the safety critical nature, Railways have strict policies on recovery and reconstitution to ensure a safe state in addition to a secure state A threat risk assessment will be carried out in order to not breach safety mechanisms for vital data, in case of system recovery from backed up information.
Comments	-
Reference	CLC/TS 50701

Short name	Emergency power
Key objectives	Continuous Protection
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Network and security configuration settings
Key objectives	Fail secure - Assume secrets not safe - Continuous Protection - Secure Metadata Management - Secure Defaults
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Machine-readable reporting of current security settings
Key objectives	Fail secure - Assume secrets not safe - Continuous Protection - Secure Metadata Management - Secure Defaults
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Least functionality
Key objectives	Secure the weakest link - Grant least privilege - Secure defaults
Type of requirement	Tech Proc
Description	
Comments	-
Reference	CLC/TS 50701

Short name	Control system component inventory
Key objectives	
Type of requirement	Tech Proc
Description	Fail secure - Precautionary principle
Comments	-
Reference	CLC/TS 50701

2.3 Measures from existing engineering background and parallel disciplines

Deliverable D3.1 provides a deep analysis on the characterisation and identification of the cyber-physical systems and threats in the railway environment.

The deliverable deeply analyses the most critical assets of the railway infrastructure and network.

Potential cyber and cyber-physical threats have been identified and analysed in terms of probability and impact.

For more details see the D.3.1 (Ref. [16]).

3. Certification scheme analysis for a future safety and security certification scheme

Both certifications, Safety and Security, are regulated by the common norm EN ISO/IEC 17020. The UN ISO/IEC 17020 define the inspection in three big categories:

- Product;
- Process;
- Services.

The inspection could be also related to the installation or design of the three above categories.

The Inspection of processes can include also personnel, facilities, technology or methodology.

The EN ISO/IEC 17020 defines the inspection method and procedures, how to handle inspection item and samples, the records, reports and certificates.

For the Safety assessment the Safety Directive 2016/798 and the EN 50126 define the principles and the requirements to be fulfilled in order to have a “safe” Railway System.

The approach of the TS 50701 is based on the same steps of the V-cycle defined in the EN 50126.

Following the steps identified in the TS 50701 for cyber security will help to have cyber security assessment based on the V-cycle of EN 50126 and avoid possible “wrong interaction” between the two assessments.

In particular, the TS 50701 will be supported by an assessment related to the IT part, like ISO 27001.

There follows the specific certification for railway subsystems is in more detail.

3.1 Certification typology

The NIS directive identifies Railway the Undertaking (RU) and the Infrastructure Manager (IF) as Operators of Essential Services (OES).

This means that they have to take appropriate security measures and to notify serious incidents to the relevant national Authority. The Cybersecurity Railway Standard TS 50701 will be introduced in the next Control Command and Signalling (CCS) Technical Specification for Interoperability (TSI) as an informative document. Due to this, the cyber security certification, currently, is not required as mandatory, but on a voluntary basis.

3.2 The Approach

The following main points have to be taken into account:

- The certification has to be managed by an independent certification body accredited by an Accreditation Body (in accordance with EN ISO/IEC 17020);
- Reference laboratories enabled to perform test campaigns have to be identified. Such laboratories have to guarantee, through an accreditation process (according to ISO/IEC 17025), an adequate level of independence, personnel technical competence and suitability of the test equipment.

3.3 Objects and actors involved

NIS Directive identifies in ANNEX II the OES that have put in place security measures.

In particular, the following entities for the rail transport sector have been identified:

- Infrastructure Managers, as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council (Ref. [2])
- Railway Undertakings, as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU(Ref. [2])

The railway undertakings (RU) and the infrastructure managers (IM) are consequently both in the scope of the NIS Directive, and their identification as operators of essential service (OES) respects the transposition of laws to the majority of Member States (Ref. [3]).
The necessity of RU and IM to meet the Cybersecurity requirements requires the manufacturers to deliver products and subsystems compliant with the applicable Cybersecurity requirements.
In the long term the target is to have product and system “secure by design”. In this way the fulfilment of the security requirements will be easier.

3.4 Boundaries and Constraints of the Certification

The boundaries of the certification are defined, at least at high level, in the TS 50701. In this Standard, the different subsystems of the railway domain have been apportioned as follow:

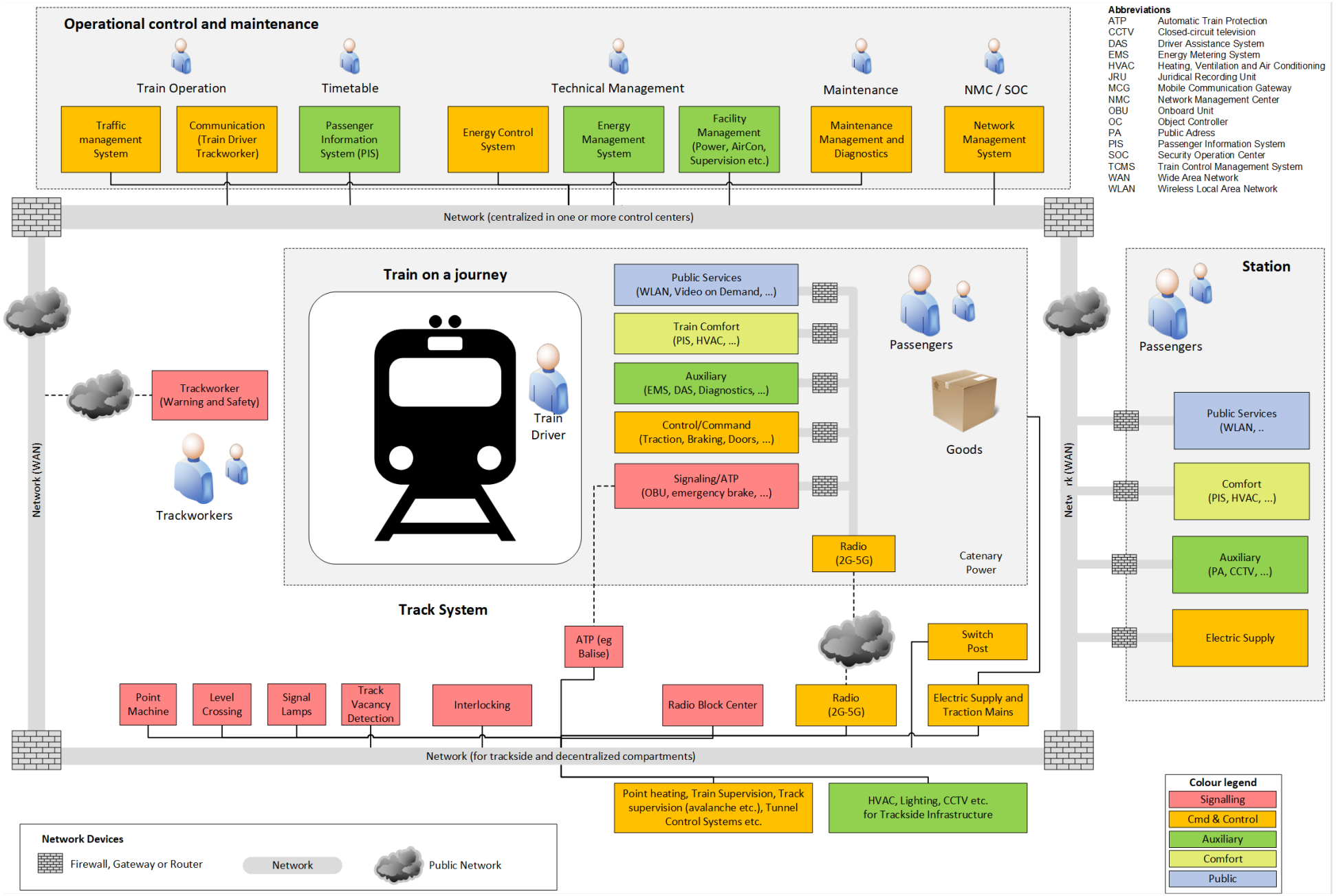

FIGURE 1 – RAILWAY PHYSICAL ARCHITECTURE MODEL (EXAMPLE) (FIGURE 3 OF CLC/TS 50701)

The above description has to be tailored on each certification process based on the preliminary definition of the system under assessment.
The boundaries are defined during the high-level zone and conduits modelling.
As for the physical architecture, a model example has been defined in the CLC/TS 50701 and it is shown in the figure below:

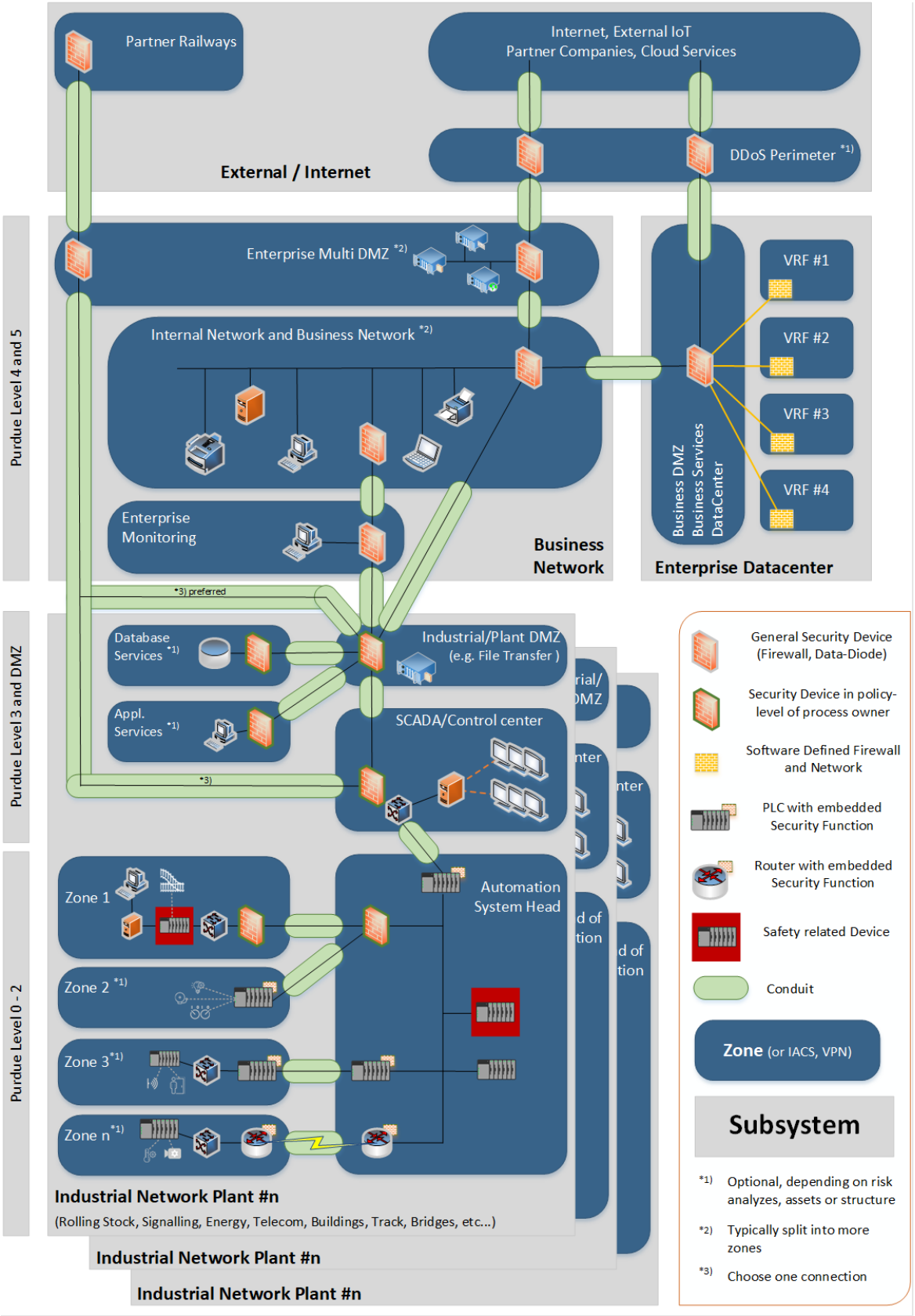

FIGURE 2 - GENERIC HIGH-LEVEL RAILWAY ZONE MODEL (EXAMPLE)

The zones and conduits apportionment is very important and will be undertaken during the system definition phase.

3.5 Activities and Responsibility within the Certification process

The certification body, following what is required by EN ISO/IEC 17020, will follow the method and procedure defined in the relevant specification. If this method is not defined, the assessment body has to define the most appropriate method and procedure in order to assess the system.
For example, the CLC/TS 50701 defines some examples of risk assessment methods. For each risk method, the following information will be documented:

- Impact Assessment
- Likelihood Assessment
- Risk Acceptance
- Justification

The certification process is based on the EN 50126-1 V-cycle.

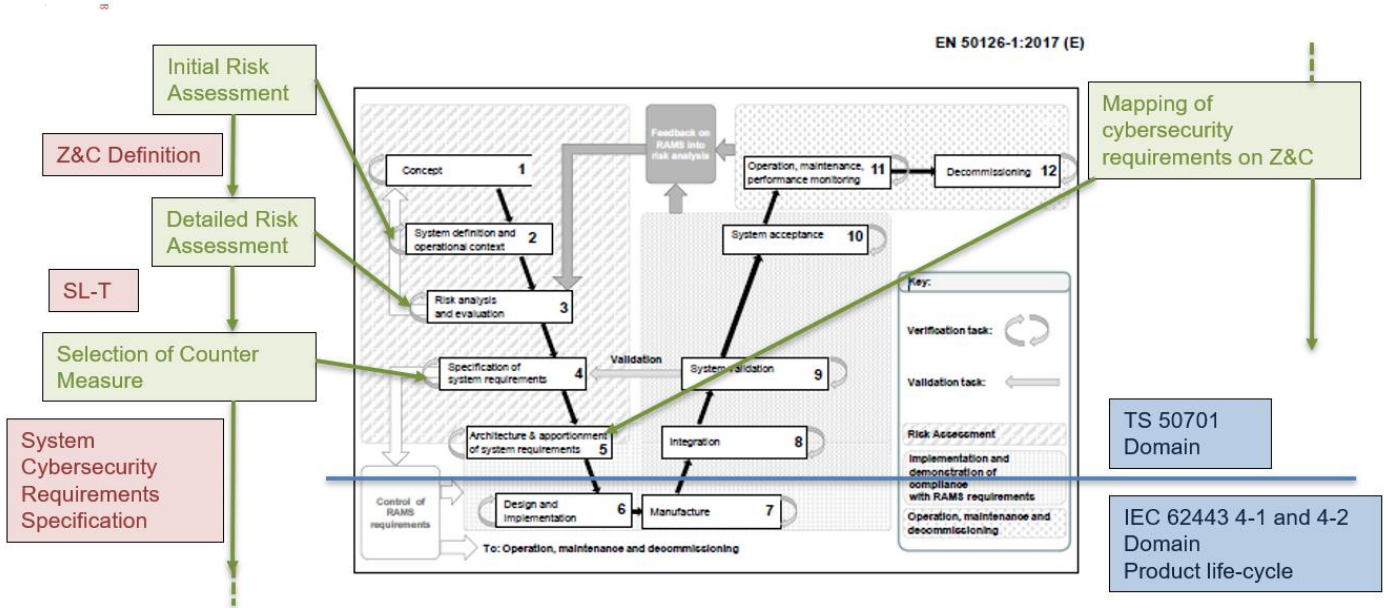

FIGURE 3 - TS 50701 VS 50126 V- CYCLE LEFT SIDE

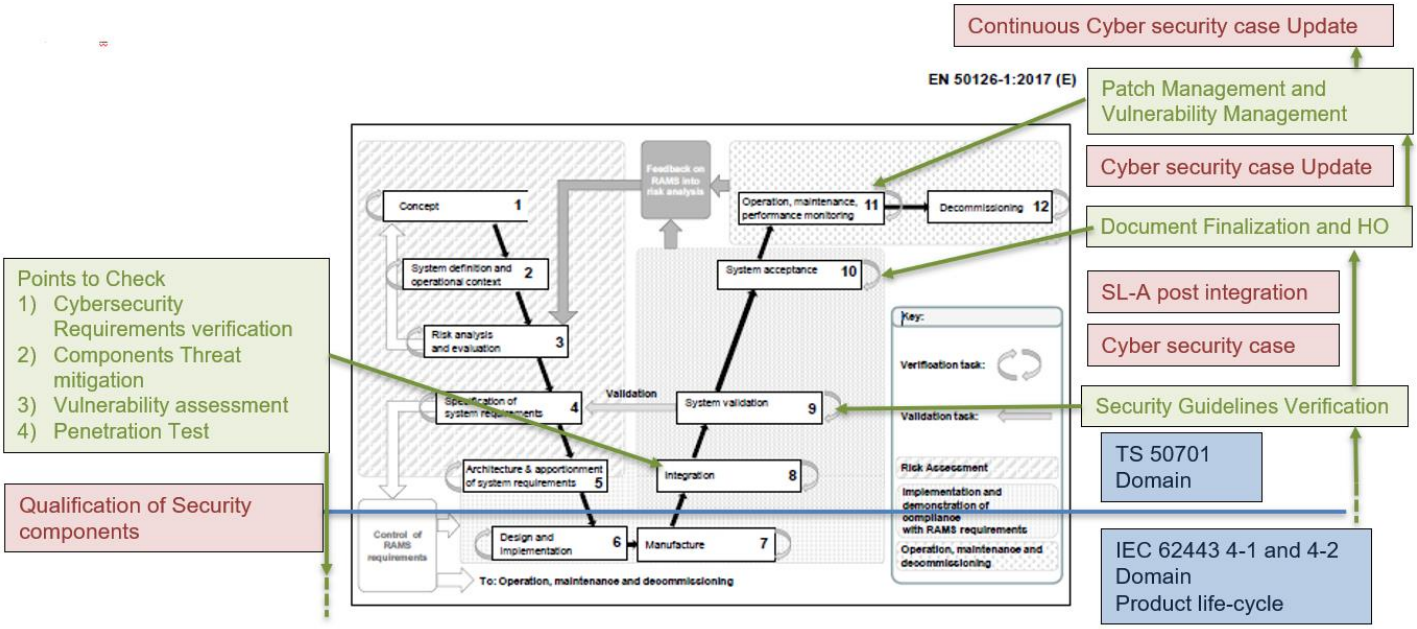

FIGURE 4 - TS 50701 VS 50126 V- CYCLE RIGHT SIDE

Figure 3 and Figure 4 describe how the TS 50701 is harmonised with the EN 50126.
The figures highlight that the TS 50701 is dedicated to assessing the Subsystem part.
TS 50701 applies to the Communications, Signalling and Processing domain, to Rolling Stock and to Fixed Installations. It provides references to models and concepts from which requirements and recommendations can be derived to manage the risks, due to security threats, and to keep them at an acceptable level.
The security models, the concepts and the risk assessment process described in TS 50701 are based on or derived from the IEC 62443 series standards. This document is consistent with the application of IEC 62443 and with ISO 27001 and ISO 27002.

3.6 Validity of the Certificates

The validity of the Certificate will be guaranteed keeping under control the process by the customer keeping alive the ISO 27001 Certificate.
As well as the Security Case, result of the CLC/TS 50701 assessment, will be maintained and any modification will be communicated to the CB for further evaluation.

3.7 Certification Bodies

A Company in Europe, in order to become a Certification Body, has to be accredited by a legally recognised Accreditation Body, according to specific Norms such as:

- EN ISO/IEC 17065: «Conformity assessment- Requirements for bodies certifying products, processes and services».
- EN ISO/IEC 17020: «Conformity assessment- Requirements for the operation of various types of bodies performing inspection».
- EN ISO/IEC 17021: «Conformity assessment- Requirements for bodies providing audit and certification of management systems».

As already said, the Certification Body, in order to certify according to cybersecurity standards, will be accredited in accordance with EN ISO/IEC 17020.

3.8 Laboratories

As the Certification Bodies, also Laboratories need to be accredited to demonstrate their capability to perform the specific tests. The European Norm dedicated to the accreditation of the Laboratories is EN ISO/IEC 17025.
As an alternative to the accreditation, a Laboratory can be qualified, according to EN ISO/IEC 17025, by the Certification Body itself. In this case, the qualification is only valid for the Certification Body that issued it and it is not subject to any mandatory mutual recognition.

4. End-to-end IoT-level security standards

4.1 Hardware-level security

Cyber-physical security is indispensable in any smart system where the generated and flowing data is to be encrypted. This is a very natural need of any cyber-physical system where cryptographic operations, for example, encryption/decryption, hashing, key generation, and key management take place.
One of the basic principles of cryptography is Kerckhoff's hypothesis [Ref. [17]]. According to this hypothesis, the overall security of any crypto-system is completely dependent on the security of the key, and all other parameters of the crypto-systems are publicly observable. Thus, the cryptographic algorithms are assumed to be open as long as the key generation scheme is not secure. In real life, many systems actually use well-known symmetric and asymmetric cryptographic algorithms (AES, 3DES, RSA, ECDSA, SHA) which have been applied to many dimensions and experts are aware of their strengths and weaknesses. As a matter of fact, the randomness criteria play a crucial role in cryptographic key generation.

There are two basic types of generators used to produce random sequences: true random number generators (TRNGs) and pseudo random number generators (PRNGs) [Ref. [19]]. TRNGs generate random numbers from a physical process, rather than employing an algorithm. Such devices are often based on microscopic phenomena that generate low-level, statistically random "noise" signals, such as thermal noise, the photoelectric effect involving a beam splitter, and other quantum phenomena. The presence of unpredictability in these phenomena can be justified either by the theory of unstable dynamical systems and chaos theory [Ref. [18]] or by the non-deterministic nature of quantum mechanics. While TRNGs take the advantage of non-deterministic entropy sources, PRNGs generate bits in a deterministic manner. The PRNG-generated sequence is not truly random, because it is completely determined by an initial value, called the PRNG seed (which may include truly random values). PRNGs tend to benefit from the external source of randomness (e.g., mouse movements, the delay between keyboard presses etc.) which are practical in use but still predictable.

The vulnerability analysis of a cryptosystem is to check whether the system relies on a hardware-based RNG or not. Then, this RNG should be TRNG. To meet the true randomness criteria, three test suites are applied on a sufficient length of bit sequences, which have been accepted as the de-facto method for randomness testing:

- NIST-800-22 Randomness Test Suite [Ref. [20]]
- DieHard Test Suite [Ref. [21]]
- Big Crush Test Suite [Ref. [22]]

Among these three tests, the NIST-800-22 randomness test suite is the widely accepted and practical standard, as addressed by the well-known FIPS-140-2[1] and FIPS-140-3[2] published by NIST. As standardised by NIST, the security requirements for cryptographic modules emphasise the use of TRNGs in cryptographic modules, as addressed in the use of PRIGM in simulation exercises.

4.2 Nodes and Person Authentication

Authentication is indispensable in railway processes not only for improving the security of systems and access control of any critical logical or physical infrastructure but also for privacy preservation. Authentication is usually perceived as “person authentication”. However, with recent advancements in IoT, “things” or “node” authentication has become crucial to building more resilient infrastructures.

For person authentication, FIDO (Fast IDentity Online) authentication is presented as a set of standards for fast, simple, and strong authentication which has been developed by the FIDO Alliance[3]. The FIDO Alliance is an industry association with representatives from a range of organisations including Google, Microsoft, Mozilla, and Yubico. The proposed standards aim to enable phishing-resistant, passwordless (if possible), and multi-factor authentication. The main motivation of this standard is to ease the authentication process for end users and to keep their interest during the long and impractical authentication procedures. The alliance has improved online user interfaces by making strong authentication easier to implement and use, such as WebAuthn and FIDO2 for Android. The applications over web browsers involve passing a cryptographic challenge from the server to the authenticator and returning the authenticator's response to the server for validation. The server stores the user's public key credentials and account information. During an authentication or registration flow, the server generates a cryptographic challenge in response to a request from the application. It then evaluates the response to the challenge.

4.3 AI and Blockchain

The recent technological advancements force and drive system integrators to utilise new technologies such as AI and blockchain. Although these novel techniques are becoming mature they are also

[1] https://csrc.nist.gov/publications/detail/fips/140/2/archive/2001-10-10
[2] https://csrc.nist.gov/publications/detail/fips/140/3/final
[3] https://fidoalliance.org/

becoming diversified as numberless variants of the developed algorithms are used in cyber-physical systems. Railway systems are also at the top of the list of most promising domains where AI and blockchain can be used.

In some ways, Blockchain upends traditional models of standard-setting, given the decentralised governance and ability to embed standards within the build of the protocol. Other areas have mimicked structures used to create coherence in distributed systems such as the internet.
Concerning emerging (recently published or upcoming) Blockchain and DLT standards produced by the ISO/TC 307 working group, the contents of the following ISO documents are known as the foremost ones, i.e. ISO 22739:2020 - Blockchain and distributed ledger technologies: Vocabulary, ISO/TR 23244:2020 - Blockchain and distributed ledger technologies: Privacy and personally identifiable information protection considerations, ISO/TR 23455:2019 - Blockchain and distributed ledger technologies: Overview of and interactions between smart contracts in Blockchain and distributed ledger technology systems, ISO/DIS 23257 - Blockchain and distributed ledger technologies: Reference architecture, ISO/DTS 23258 - Blockchain and distributed ledger technologies: Taxonomy and Ontology, ISO/DTS 23635 - Blockchain and distributed ledger technologies: Guidelines for governance, etc.

Similarly, standardisation and certification of AI services will gain more importance in the upcoming years. The European Commission published the Artificial Intelligence Act (AI Act)[4] on 21 April 2021, which aims to introduce a common regulatory and legal framework for AI. Based on a risk-based approach[5], the regulation categorises the risks of AI applications into four different levels: unacceptable risk, high risk, limited risk, and minimal risk. AI applications with an unacceptable risk will be banned. An independent assessment by third parties is required for high-risk AI applications.However, for limited-risk AI applications, a self-assessment is required.

5. Open Points

At the current stage of development of the S4RIS platform, it represents a powerful tool to support cybersecurity threats identification and mitigation. In this regard the S4RIS platform is then a part but not the whole system or subsystem according to the definition of the norms. It implies that just a part of the requirements are applicable and that the certification cannot be restricted to the platform. The Certification has to be applied to an entire subsystem that will include a specific implementation and configuration of the S4RIS platform. The reuse of the results across different systems and implementation is not yet fully clear and will be deepened through future research projects and through applications of the S4RIS platform in real railway systems.

Although there exists a strong background in standardisation of railway systems, there still exist open points of detail. The V-cycle presented in Section 3.5 draws a comprehensive procedure to verify the cyber-physical and safety resilience that forms a basis for the certification of the railway systems and subsystems. However, this certification process can be improved with more standardised techniques and hardware and/or software solutions. The following findings are presented here to improve the certification procedure and can support the pre-normative studies to improve the existing and/or new standards.

5.1 Hardware-level security

The existing standards, such as ISO 15408 form the basis of Common Criteria Evaluation Assurance Levels and do not rely directly on the reliability, robustness, unpredictability and resilience of the random number generation. The NIST-800-22 randomness test suite only focuses on the randomness analysis of the TRNG. However, there is no direct standard to verify the reliability and robustness of the TRNGs. As reported in the paper Ref. [23], true randomness may not be enough

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
[5] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

as the random number generation mechanism can be hacked and the secret parameters of the nonlinear equation sets can be revealed.

Hence, there is a big demand to improve and standardise the true random number and cryptographic key generation schemes which is indispensable in any cyber-physical system used in railway infrastructures.

5.2 Nodes and Person Authentication

FIDO and FIDO2 present authentication solutions for mobile phones or desktops, over web browsers, which usually aim to utilise a password and/or token, and recently biometrics for passwordless authentication. Such easy-to-use authentication mechanisms can be used in railway operations which can be even helpful for workers in the field or users with relatively less adoption or awareness. However, there is a trade-off here. While the authentication schemes are becoming easier, security and privacy concerns may increase. This may become more painful when node authentication takes place. There is a strong demand to define a consensus to merge both person and node authentication in complex cyber-physical environments by considering security, privacy, accountability, integrity, interoperability and practicality.

The joint use of PRIGM and Senstation in SAFETY4RAILS can be seen as an effective solution which enables active person and node authentication during a process. Here, PRIGM automatically generates truly random secret keys which can be used either as one-time passwords or instantly-created secrets for the devices, subsystems, systems and applications at nodes (things in general). These exercises can support the pre-normative studies in the near future to improve standardisation activities and also the certification of authentication and access control services in railway operations.

5.3 AI and Blockchain

Despite the dense work on standardisation activities, there is still a big need to improve the certification schemes for the decentralised networks. This will become more important as the multinational, cross-organisation and cross-border railway operations will get more widespread, especially when integrated with other modes of transportation (i.e. transition towards centralised to decentralised railway operations)

There still exist large gaps for standardising the new concepts, such as trustworthy AI, explainable AI, and bias-aware and ethical AI that requires additional effort in upcoming standardisation activities.

6. Conclusion

This report deals with the identification of the present legal framework for standardisation and certification applicable to cyber-physical systems. These activities have been carried out in the scope of Task 9.3. The report contains three major sections:

- Chapter 2 Legal Framework based on D2.4 report (Ref. [15])
- Chapter 3 Certification scheme for future integration of Safety and Security
- Chapter 4 IOT-level security standards
- Chapter 5 Open Points for standardisation

In Chapter 2 the step forward compared to deliverable D2.4 is the introduction of the requirements related to the CLC/TS 50 701 and the definition of a future certification process based on the applicable requirements and on the current state of the art of the Certification in the Railway domain. CLC/TS 50 701 requirements are derived from the “mother” specification IEC 62443 and specialised for the railway environment and these represent the European standard approach to cybersecurity in Railway sector.

The process to follow for the assessment described in the CLC/TS 50701 has been developed following the steps of the well-known safety assessment process. In this way the two assessments have the same steps, of course with different aims. At the end of the security assessment there is a Security Case that will be maintained along the whole life cycle of the system.
In Chapter 4 the state of the art of applicable standards related to hardware-level security, node and person authentication and AI and blockchain have been presented.

The open points relate to the need for the certification needing to apply to the integrated cyber-physical system as a whole.
Nevertheless, at the present stage, the certification will be applied to a subsystem or system and the S4RIS platform can help to meet part of the set of requirements.

For future application in the railway sector a standardisation of the true random number and cryptographic key generation schemes is needed because the Random Generation Number mechanism can be hacked.

Due to the application of new technologies like AI and BlockChain an additional effort in upcoming standardisation activities is required.

Bibliography

Ref. [1] DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Ref. [2] Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32)

Ref. [3] ENISA, Railway Cybersecurity report, Security Measures in the Railway Transport Sector, November 2020

Ref. [4] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

Ref. [5] ISA/IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

Ref. [6]

Ref. [7] Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety

Ref. [8] EN 50126-1 Railway applications —The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS Process

Ref. [9] EN 50126-2 Railway Applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Systems Approach to Safety

Ref. [10] EN 50128 Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems

Ref. [11] EN 50129 Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling

Ref. [12] EN 50159 Railway applications — Communication, signalling and processing systems

Ref. [13] NIST SP 800-63-3 Annex A (https://pages.nist.gov/800-63-3/)

Ref. [14] NIST SP 800-61 rev. 2, Computer Security Incident Handling Guide (http://dx.doi.org/10.6028/NIST.SP.800-61r2)

Ref. [15] SAFETY4RAILS, Deliverable D2.4 Specific requirements for standardisation and interoperability

Ref. [16] SAFETY4RAILS, Deliverable D3.1Identification and characterization of cyber(-physical) systems and threats in railway environment.

Ref. [17] Martin, K., 2017. Everyday Cryptography: Fundamental Principles and Applications. 2nd Edition, Oxford University Press

Ref. [18] Ergün, S., Güler, Ü. & Asada, K., 2011. IC truly random number generators based on regular & chaotic sampling of chaotic waveforms. *Nonlinear Theory and Its Applications, IEICE 2.2 (2011): 246-261.*

Ref. [19] Ergün, S. & Özog, S., 2007. Truly random number generators based on a non-autonomous chaotic oscillator. *AEU-International Journal of Electronics and Communications 61, no. 4 (2007): 235-242.*

Ref. [20] NIST 800-22, 2010. Sp 800-22 rev. 1a. a statistical test suite for random and pseudorandom number generators for cryptographic applications, s.l.: National Institute of Standards & Technology.

Ref. [21] Marsaglia, G., n.d. DIEHARD Statistical Tests. [Online] Available at: https://tams.informatik.uni-hamburg.de/paper/2001/SA_Witt_Hartmann/cdrom/Internetseiten/stat.fsu.edu/source.tar.gz

Ref. [22] L'Ecuyer, P. & Simard, R., 2007. TestU01: A C library for empirical testing of random number generators. *ACM Transactions on Mathematical Software (TOMS) 33, no. 4 (2007): 1-40.*

Ref. [23] Ergün, Salih, and Burak Acar. "Revealing the secret parameters of an fpga-based “true” random number generator." 2020 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, 2020.

Ref. [24] European Standard, CLC/TS 50701:2021 Railway applications – Cybersecurity.

ANNEXES

ANNEX I. GLOSSARY AND ACRONYMS

TABLE 1: GLOSSARY AND ACRONYMS

Term	Definition/description
AL	Activity leader
AB	Advisory Board
API	Application Programming Interface
CO	Confidential
CSIRT	Computer Security Incident Response Team
CSMs	Common Safety Methods
D	Deliverable
DC	Data controller
DM	Dissemination manager
DMS	Distributed Messaging System
DoA	Description of the Action (Annex 1 to the Grant Agreement)
EB	Ethical Board
EC	European Commission
EM	Ethics manager
ENISA	European Network and Information Security Agency
ERA	European Railway Agency
ERTMS	European Railway Traffic Management System
ETCS	European Train Control System
EU	European Union
GUI	Graphical User Interface
EUB	End-user Board
EUC	End-users coordinator
EXM	Exploitation manager
IM	Innovation manager
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISA	International Society for Automation
MS	Member State
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
OES	Operator of Essential Services
OT	Operational Technologies
PC	Project coordinator
PGA	Project General Assembly
PMT	Project Management Team
PR	Partner representatives
PU	Public
QM	Quality manager

Term	Definition/description
REST	Representational State Transfer
SAB	Security Advisory Board
SM	Standardisation manager
S4RIS	SAFETY4RAILS Information System
TL	Task leader
TM	Technical manager
ToC	Table of Contents
TRL	Technology Readiness Level
WP	Work package
WPL	Work package leader

SAFETY4RAILS

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883532.