SPECIFIC REQUIREMENTS FOR STANDARDISATION AND INTEROPERABILITY

Deliverable 2.4

Lead Author: RINA

Contributors: FHG, CEIS, MTRS, STAM, ETRA

Dissemination level: PU - Public

Security Assessment Control: passed

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

D2.4 SPECIFIC REQUIREMENTS FOR STANDARDISATION AND INTEROPERABILITY

Deliverable number:	2.4		
Version:	1.2		
Delivery date:	02/03/2022 (Update)		
Deliverable due date:	31/03/2021		
Dissemination level:	PU – Public		
Nature:	Report		
Main author(s)	Fabrizio Crismer Luca Macchi	RINA RINA	
Contributor(s) to main deliverable production	Katja Faist	Fraunhofer	Author of Interoperability requirements
	Florence Ferrando	CEIS	Contribution for GUI requirements, review
	Gilad Rafaeli	MTRS	Contribution to Standardisation requirements
	Paul Abbott	MTRS	Contribution to Standardisation requirements, review
	Eduardo Villamor Medina	ETRA	Contribution to Standardisation requirements
	Davide Ottonello	STAM	Contribution to GUI assessment and user stories
Internal reviewer(s)	Antonio De Santiago Laporte	MdM	*Security Advisory Board*
	Atta Badii	UREAD	*Ethics Board*
	Andreas Georgakopoulos	WINGS	*Quality Manager*
	Stephen Crabbe	Fraunhofer	*Project coordinator*
External reviewer(s)	Pauline Massart	CEIS	*Person not involved in T2.4*

Document control

Version	Date	Author(s)	Change(s)
0.1	20/01/2021	RINA	Initial version
0.2	26/02/2021	RINA, MTRS, ETRA	Draft including Standardisation requirements
0.3	03/03/2021	RINA, CEIS	GUI section partially filled-in
0.4	04/03/2021	CEIS, MTRS	Review
0.5	11/03/2021	RINA, STAM	Update of chapters 2 and 4 including outputs from end-user workshop n°2
1.0	18/03/2021	RINA, Fraunhofer	Overall review Chapter 3 added
1.1	01/04/2021	RINA, Fraunhofer	Update after internal and external reviews
1.2	02/03/2022	CEIS, Fraunhofer, RINA	Updates to inlcude contents requested following EC review: - Page 14: Addition of footnote to section on ISO / IEC15408, noting identification also by EC reviewer during mid-term project review - Page 15: One protocol added in Table 2 - Page 60 and 61: Addition of further detail regarding functional interface specification aspects under requirement tables for IO-3 and IO-4 in the “Comment” row - Page 63: Broken link in Figure 4 repaired - Page 88: D1.4 and D2.3 added in the Bibliography - Backpage with consortium logos updated

DISCLAIMER AND COPYRIGHT

The information appearing in this document has been prepared in good faith and represents the views of the authoring organisation(s). Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authoring organisation(s) accept no statutory, contractual or other legal liability for any error or omission to the fullest extent that liability can be limited in law.

This document reflects only the view of its authoring organisation(s). Neither the authoring organisation(s), nor the Research Executive Agency, nor the European Commission are responsible for any use that may be made of the information it contains. The use of the content provided is at the sole risk of the user. The reader is encouraged to investigate whether professional advice is necessary in all situations.

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 2014) and combined cyber-physical attacks, which are important emerging scenarios are 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 must consider many aspects to ensure passenger safety and security, e.g., 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 be validated by two rail transport operators and the results will support the re-design of the final prototype.

TABLE OF CONTENTS

ABOUT SAFETY4RAILS 3
Executive summary 6
1. Introduction 7
1.1 Objectives of the task 7
1.2 Structure of the deliverable 7
2. Standardisation requirements 9
2.1 Introduction 9
2.1.1 Background on security EU legislation and standards 9
2.1.2 Focus on railway sector 17
2.1.3 Methodology adopted 21
2.2 List of standardisation requirements 22
2.3 Additional guidelines and recommendations 37
2.3.1 Alerting and public warning systems: OASIS - Common Alerting Protocol (CAP) 37
2.3.2 Risk Management Standard (ISO 31000) Overview 41
2.3.3 Secure coding 43
3. Interoperability requirements 44
3.1 Introduction 44
3.1.1 Definition of interoperability in S4RIS context 44
3.1.2 Methodology adopted 44
3.2 Operational interoperability requirements 45
3.2.1 Overview on the “is” status of the tools foreseen to contribute to the S4RIS platform 46
3.2.2 Operational interoperability to internal and external systems and technical interoperability 59
4. Graphical User Interface requirements 63
4.1 Introduction 63
4.1.1 Principles for GUI design 63
4.1.2 Methodology adopted 64
4.1.3 Assessment of the existing GUIs of the tools 65
4.2 GUI definition 68
4.2.1 GUI requirements list 68
4.2.2 User stories 74
4.2.3 GUI examples 80
5. Conclusions 85
6. Bibliography 86
ANNEXES 89
ANNEX I. GLOSSARY AND ACRONYMS 89

List of tables

Table 1: Standards mainly related to cyber security 12

Table 2: Standards mainly related to physical security 14

Table 3: Standards related to organisational resilience 16

Table 4: Other security-related standards 17

Table 5: Characteristic of existing tools 66

Table 6: S4RIS GUI user Stories 76

Table 7: Glossary and acronyms 89

List of figures

Figure 1: Overview of 4th Railway Package 18

Figure 2: Risk Management Process 42

Figure 3: Scheme identifying complexity of possible communication connections between provided tools and external systems 46

Figure 4: Types of interfaces in existing tools 65

Figure 5: Sign-in page 80

Figure 6: Home-page layout proposal #1 81

Figure 7: Home-page layout proposal #2 81

Figure 8: Example of interface for interaction with CLI tools (e.g., BB3D) 82

Figure 9: Settings page 82

Figure 10: Language selection page 83

Figure 11: Account management 83

Figure 12: Error pop-up 84

Executive summary

This document is the deliverable D2.4 – *Specific requirements for standardisation and interoperability* – of SAFETY4RAILS, aiming to present the collection of standardisation and interoperability requirements relevant for SAFETY4RAILS. Furthermore, the report also includes requirements and guidelines defined, with the support of the end-users, for the development of the Graphical User Interface (GUI) of the SAFETY4RAILS Information System (S4RIS) platform.

The report presents the results of the activities performed in T2.4, which addresses three main topics:

1. Definition and identification of standardisation requirements: the legal texts, standards and best practices recognised as effective to provide an appropriate level of security for complex systems and organisations have been analysed, with a focus on the railway (including metro) sector. A set of requirements for S4RIS is defined starting from a relevant selection of standards. These requirements and the identified legal texts, standards, etc., will constitute the basis for the definition of the legal framework of a future certification scheme, objective of Task 9.3.
2. Definition and identification of interoperability requirements, aimed to provide an interoperability concept defining the data exchange and alignment within S4RIS, as well as a concept for the interoperability between the S4RIS and external systems.
3. Definition of GUI requirements aimed to provide valuable inputs to drive the GUI development that will be carried out in Work Package 6. Inputs and feedbacks received from the end-users are used for this purpose.

The report is organised as follows:

- ❖ Introduction.
- ❖ Standardisation requirements
- ❖ Interoperability requirements
- ❖ Graphical User Interface requirements
- ❖ Conclusions

1. Introduction

1.1 Objectives of the task

This report describes the activities carried out within the Task 2.4 (T2.4). This task is heterogeneous and is mainly aimed to cover three topics: standardisation, interoperability, and graphical user interface (GUI) requirements.

The work of Task 2.4 was therefore split in three main activities:

1) Definition and identification of standardisation requirements, aimed to identify requirements deriving from legal texts, standards and best practices that are recognised as effective to provide an appropriate level of security for complex systems such as S4RIS and organisations, with a focus on the railway (including metros) sector. These requirements constitute the basis for building up a system in line with the European legal framework and with security standards. Furthermore, the identified legal texts, standards and requirements will constitute an important input for a feasibility study in order to investigate how currently adopted safety certification schemes can be enhanced taking into considerations security aspects that will be carried out within the Task 9.3 of the project, also led by RINA.
2) Definition and identification of interoperability requirements, aimed to provide an interoperability concept defining the data exchange and alignment within S4RIS, based on the characteristics of the tools to be integrated, as well as a concept for the interoperability between the S4RIS and existing external systems.
3) Definition of GUI requirements, aimed to provide essential inputs to drive the GUI development activity that will be carried out in Work Package 6, Task 6.2. The GUI requirements take into account the characteristics of the tools that will be integrated in the S4RIS platform and the inputs received from the end-users involved, with questionnaires and results discussed during a workshop.

These activities are described in the three central sections of this report, following a common structure:

- Firstly, an introduction to the activity is provided, along with any information valuable to better understand the importance of the activity, its background and the methodology followed for the definition and validation of the defined requirements.
- Secondly, the specific requirements are listed adopting a structure suitable for the specific type of requirements.
- Finally, if necessary, further guidelines and recommendations are provided.

In terms of the overall methodological framework for specifying the stakeholder-centred requirements in the three areas of concern in this work namely standardisation, interoperability and graphical user interface, it has to be noted here at the outset of this report that, it is acknowledged that the determination of these requirements would have benefit from being predicated on already established priority use-contexts and their respective use-scenarios. At this stage, the end-user workshops necessarily included an implicit consideration of the priority configurations and use-scenarios involving tool-subsystems inter-operation and/or user-tool interactivity as would be required in the respective situated use-contexts. The resulting standardisation, interoperability and GUI requirements arising from this stage shall remain open to possible refinements in light of the priority demonstrator use-scenarios as shall be confirmed and furtherly detailed later with WP6 (for the GUI) and WP8.

1.2 Structure of the deliverable

This document comprises of the following main sections:

- *Section 1 - Introduction: providing an overview of the deliverable objectives and structure.*
- *Section 2 - Standardisation requirements: reporting the activity carried out regarding the definition of requirements derived from legal texts, standards, and best practices.*
- *Section 3 - Interoperability requirements: reporting the activity carried out regarding the definition of interoperability requirements.*

- *Section 4 - Graphical User Interface requirements: reporting the activity carried out regarding the definition of GUI requirements.*
- *Section 5 - Conclusions: summarising the activities carried out in Task 2.4.*
- *Annex I - Glossary and Acronyms*

2. Standardisation requirements

2.1 Introduction

This section reports on the activity carried out within the Task 2.4 to address the definition of standardisation requirements.

Firstly, an overview on the legal texts, standards, and best practices related to security is provided to introduce the audience to the topic. Secondly, the report focuses on the railway environment, highlighting the current approach to both safety and security. Thirdly, the methodology adopted to define the standardisation requirements is presented. Then, the list of requirements is reported in the format common to other WP2 tasks. Finally, a set of additional guidelines and recommendations is provided

The main purpose of this activity is to identify the legal texts, standards and best practices relevant for the development of S4RIS. Essentially, the target is to define a set of requirements that will ensure the compliance of S4RIS to existing applicable European laws in the field of security and, contemporarily, to ensure as much as possible the compliance with existing standards. When feasible, furthermore, the adoption of best practices is encouraged.

2.1.1 Background on security EU legislation and standards

This chapter presents an overview of the current EU legal framework and standards regarding security.

2.1.1.1 EU Legislation

NIS Directive

In this context, the EU started to address the topic of cybersecurity through the EU Cybersecurity plan (Ref. [1]), released in 2013, that represented the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks.

Among the initiatives undertaken in the frame of EU Cybersecurity plan, that with the major impact on the approach towards security was the proposal for a Directive on network and information security (NIS). The proposed NIS Directive was considered a key component of the overall strategy, since it would establish requirements for all Member States, digital service providers and critical infrastructure operators to ensure a secure and trustworthy digital environment throughout the EU.

In 2016, that proposal actually became part of the EU legislation through the **Network and Information Security (NIS) Directive** (Ref. [2]). The NIS Directive is the first piece of EU-wide cybersecurity legislation, whose goal is to enhance cybersecurity across the EU. Every EU member state has transposed the Directive in their national legislation. As with all EU directives, NIS gives to EU countries some level of flexibility to take into account national circumstances, for example to re-use or align existing organisational structures and national legislation.

Summarising, the NIS Directive essentially addresses three main topics:

1) *National capabilities*: the Directive requires the EU Member States to have certain national cybersecurity capabilities, e.g., they must have a national CSIRT, perform cyber exercises, etc.
2) *Cross-border collaboration*: Cross-border collaboration between EU countries, for example, the operational EU CSIRT network, the strategic NIS cooperation group, etc.
3) *Supervision of critical sectors*: EU Member states must supervise the cybersecurity of critical market operators in their country, including critical sectors (energy, transport, water, health, digital infrastructure and finance sector), and critical digital service providers (online marketplaces, cloud and online search engines)

The NIS Directive aims to enhance security across sectors which are vital for our economy and society and rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as Operators of Essential Services (OES) must take appropriate security measures and notify serious incidents to the relevant national authority. OES means a public or private entity of a type referred to in Annex II of the Directive, which meets the criteria laid down in Article 5(2) of the Directive. In particular, the Annex II lists Rail transport among the type of entities that qualify for being considered to be an OES, together with Air, Water and Road transport. Specifically, the following entities for the rail transport subsector are 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. [3])
- 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

The railway undertakings (RU) and the infrastructure managers (IM) are consequently both in the scope of the NIS Directive, and their identification as Operator of Essential Services (OES) respects the transposition of laws by the majority of member states (Ref. [4]).

As a consequence, this topic is very relevant to the SAFETY4RAILS project, since S4RIS will be used by Railway Infrastructure Managers to enhance their level of security. For the sake of completeness, it needs to be underlined that the definition of essential services related to the railway subsector has not been standardised and Member Statesinterpreted the definition of rail essential services at variable levels of abstraction, resulting in cross-nationally inhomogeneous definition of Railway Essential Services (Ref. [5]).

Chapter IV of the NIS Directive “Security of the Network and Information Systems of Operators of Essential Services” provides high-level requirements to address risks posed by security threats. By requiring OES to comply with “appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems”, the NIS Directive aims at raising the level of security of OES to face the serious risks posed to the security of critical information systems supporting their essential operations.

In order to provide a consistent and coherent approach toward this goal, the NIS Coordination Group issued the “Reference document on security measures for Operators of Essential Services” (Ref. [6]). This provides a clear and structured picture of current and often common approaches to the security measures of OES foreseen in article 14 (1) and (2). The security measures defined in this document, though at high-level, help the OES to address security providing a common approach to governance and ecosystem, protection of IT, defence from threats, and resilience. A further step in the direction of implementation and compliance to the NIS Directive by OES is represented by the “Mapping of OES Security Requirements to Specific Sectors” (Ref. [7]), a publication by ENISA that aims to provide a substantial and comprehensive mapping of the security requirements for OES, as they have been agreed in the NIS Cooperation Group, to sector specific information security standards. In order to achieve a common, cross-sector (horizontal) framework of security measures for the OES, the security requirements for the OES are primarily mapped to the most frequently used international information security standards by operators in each of these sectors. Specifically, for the rail sector, the following standards have been selected and mapped (further details on these standards will be provided later in section 2.1.1.2):

- ISO/IEC 27001 - Information technology — Security techniques — Information security management systems — Requirements (Ref. [8]), this is the most commonly followed standard;

- ISA/IEC 62443 - Industrial communication networks - IT security for networks and systems, in particular ISA/IEC 62443-3-3 (Ref. [9]), applicable to Industrial Automation and Control Systems (IACS) that are often the core components of OES business.

This mapping enables the OES to efficiently identify a minimum set of standards requirements that may allow them to reach compliance with the NIS Directive. The mapping has been made available online by ENISA through an interactive tool on their web site (Ref. [11]) and can be periodically updated.

Summarising, the NIS Directive currently represents the main EU legislation in the field of cybersecurity that explicitly applies to the Infrastructure Managers business and activities. Therefore, it will have to be considered for the SAFETY4RAILS project.

Proposal for a revised NIS Directive (NIS2)

A new legislative proposal (Ref. [13]) was presented on 16 December 2020, as a result of the review of the NIS Directive. This proposal is part of a package of measures to improve further the resilience and incident response capacities of public and private entities, competent authorities and the Union as a whole in the field of cybersecurity and critical infrastructure protection. The proposal builds on and repeals the current NIS Directive. It modernises the existing legal framework taking account of the increased digitisation of the internal market in recent years and an evolving cybersecurity threat landscape.

Concerning OES (renamed Essential Entities in the proposal), the proposal greatly increases the number of involved sectors and also establishes the definition of important entities. From the point of view of the SAFETY4RAILS project, Infrastructure Managers continues to be included in the list of essential entities. Considering exclusively the scope of Infrastructure Managers, though NIS2 is just a proposal and not a binding legal act, it basically provides additional and more detailed requirements with respect to the NIS Directive and does not undermine the provisions of NIS.

In particular, Article 18 (1) of Ref. [13] state that “Member States shall ensure that essential and important entities shall take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which those entities use in the provision of their services” and Article 18 (2) indicates a set of topics to be addressed by these measures. Anyway, at present, no specific technical or methodological specifications are indicated, though they could be laid down in the future according to Article 18 (5).

To summarise : the NIS2 proposal provides further details on the measures to be adopted by essential entities (OES). These proposed provisions might also be taken into consideration also for the SAFETY4RAILS project together with the NIS Directive, so that S4RIS is ready, as much as this is possible, for future EU legislation.

European Critical Infrastructure Directive and Critical Entities Resilience Directive (proposal)

The EU adopted the European Critical Infrastructure (ECI) Directive (Ref. [14]) in 2008, which applies to the energy and transport sectors. This was the first text providing a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people. In the last few years, the importance of ensuring the resilience of critical infrastructures grew dramatically, in the face of emerging physical and digital risks.

The 2019 evaluation of the ECI Directive (Ref. [15]) has found that existing European and national measures do not ensure sufficiently ensure that operators are able to confront the increasingly complex operational challenges that they face today. For this reason, a proposal has been put forward for a new Critical Entities Resilience (CER) Directive (Ref. [16]). With this proposal, the Commission intends to create an all-hazards framework to support Member States in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents, no matter wheter they are caused by natural hazards, accidents, terrorism, insider threats, or public health emergencies such as the one the world faces today. The proposal covers the same sectors of the NIS2 Directive, namely energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration and space. Noteworthy provisions include:

- Member States would be obligated to have a strategy for ensuring the resilience of critical entities, carry out a national risk assessment and identify critical entities.
- Critical entities would be required to carry out risk assessments of their own, take appropriate technical and organisational measures in order to increase resilience, and report disruptive incidents to national authorities.
- Regular cross-border cooperation with regard to the implementation of the directive would be facilitated through an expert group, the Critical Entities Resilience Group.

In order to ensure alignment between CER and NIS2 Directives, all critical entities identified under the CER Directive would be subject to cyber resilience obligations under NIS2.

2.1.1.2 Standards related to security

In this section, an overview of most widespread and adopted standards in the field of security is presented. It is not intended as a fully comprehensive overview of existing security standards, since the number of standards directly or indirectly related to cyber and/or physical security is very large. Nevertheless, this overview aims to collect a set of the most common and adopted standards in this field.

The standards are presented in four subsections that report:

1. Standards mainly related to cyber security.
2. Standards mainly related to physical security.
3. Standards related to organisational resilience.
4. Other standards related to security.

They have been collected by Task 2.4 partners relying on research, on standards and practices implemented at their companies and on previous experience on ongoing and past projects.

It shall be noted that most of the standards illustrated hereinafter provide requirements and guidelines for organisations to increase their security. The security measures provided are usually high-level measures, consisting in the approach to be followed, controls to be implemented, policies to be adopted. It is rare that specific implementations are required.

Cyber Security Standards

In this section, the most used standards relating to cyber security are reported and described. These standards are primarily related to cyber security, but since cyber and physical security are sometimes strictly related, they may provide inputs also for physical security. They may refer to ICT, as the ISO/IEC 27000 family, or to OT systems such as Industrial Control Systems.

TABLE 1: STANDARDS MAINLY RELATED TO CYBER SECURITY

Title	**ISO/IEC 27001:2013 – Information technology — Security techniques — Information security management systems — Requirements**
Description	It is an Information Security Management Systems (ISMS) standard published in October 2013 by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control. Its best-practice approach helps organisations manage their information security by addressing people and processes as well as technology.
Title	**ISO/IEC 27002:2013 – Information technology — Security techniques — Code of practice for information security controls**
Description	The ISO 27002 standard is a collection of information security guidelines that are intended to help an organisation implement, maintain, and improve its information

	security management. It provides hundreds of potential controls and control mechanisms that are designed to be implemented with guidance provided within ISO 27001. The suggested controls listed in the standard are intended to address specific issues identified during a formal risk assessment. The standard is also intended to provide a guide for the development of security standards and effective security management practices.
Title	**ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management**
Description	This document provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. It is applicable to all types of organisations (e.g., commercial enterprises, government agencies, non-profit organisations) which intend to manage risks that can compromise the organisation's information security.
Title	**ISO/IEC 27032:2012 – Information technology — Security techniques — Guidelines for cybersecurity**
Description	ISO 27032 mainly aims to provide a guide for cybersecurity through specific recommendations. It focuses on cyberspace and is a framework for collaboration and to address issues focused on different security domains in cyberspace.
Title	**ISO/IEC 27033:2015 - Parts: 1,2,3,4,5 – Security techniques: Network security.**
Description	The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. It provides detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002. It applies to the security of networked devices and the management of their security, network applications/services and users of the network, in addition to security of information being transferred through communications links. It is aimed at network security architects, designers, managers, and officers.
Title	**ISO/IEC 27034:2015 - Parts 1,2 – Security techniques – application security.**
Description	ISO/IEC 27034 offers guidance on information security to those specifying, designing and programming or procuring, implementing and using application systems, in other words business and IT managers, developers and auditors, and ultimately the end-users of ICT. The aim is to ensure that computer applications deliver the desired or necessary level of security in support of the organisation's Information Security Management System, adequately addressing many ICT security risks.
Title	**ISO/IEC 27036-1:2014 Information technology — Security techniques — Information security for supplier relationships**
Description	ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information risks involved in the acquisition of goods and services from suppliers. The implied context is business-to-business relationships, rather than retailing, and information-related products.
Title	**ISA/IEC 62443 – Industrial Network and System Security.**
Description	ISA (International Society of Automation) and IEC have developed the IEC 624434 series of standards in order to address the need to design cybersecurity robustness and resilience into industrial automation control systems (IACS). It provides a thorough and systematic set of cybersecurity recommendations. The concept of industrial automation and control systems electronic security is applied in the broadest possible sense, encompassing all types of plants, facilities, and systems in

	all industries. IEC 62443 targets people, processes, systems, solutions and components/products.
Title	**NIST SP 800-82 rev. 2 Guide to Industrial Control Systems (ICS) Security Date Published: May 2015**
Description	This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DFRCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors. This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.
Title	**NIST Framework for Improving Critical Infrastructure Cybersecurity**
Description	This Framework enables organisations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The Framework provides structure to present day multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. Moreover, because it references globally recognised standards for cybersecurity, the Framework can also be used by organisations located outside the United States and can serve as a model for international cooperation on strengthening critical infrastructure cybersecurity.
Title	**ISO/IEC 15408-1:2009 – Information technology — Security techniques — Evaluation criteria for IT security**[1]
Description	ISO/IEC 15408 is commonly known as Common Criteria for Information Technology Security Evaluation (Common Criteria or CC) and it is an international standard for IT product security certification. It is a framework that provides criteria for independent, scalable and globally recognised security inspections for IT products. It is especially designed for products destined for highly security-intensive markets, such as governmental, banking or military sectors.

Physical Security Standards

In this section, the most used standards related to physical security are reported and described. These standards are primarily related to physical security, but since cyber and physical security are sometimes strictly related, they may have an impact also on the cyber security.

TABLE 2: STANDARDS MAINLY RELATED TO PHYSICAL SECURITY

Title	**CENELEC - EN 50132-7:2012 – Alarm systems - CCTV surveillance systems for use in security applications - Part 7: Application guidelines**
Description	This European Standard gives recommendations and requirements for the selection, planning, installation, commissioning, maintaining and testing of CCTV systems comprising of image capture device(s), interconnection(s) and image handling device(s), for use in security applications.
Title	**IEC 62676-1-4:2013 – Video surveillance systems for use in security applications - Video System Requirements, Transmission and Interoperability.**

[1] Also identified by EC reviewer during mid-term project review as could be required/appropriate in critical applications.

Description	This standard specifies the minimum requirements and gives recommendations for Video Surveillance Systems (VSS) (so far called CCTV), installed for security applications
Title	**ISO 22311:2012 – Societal security — Video-surveillance — Export interoperability**
Description	This standard is mainly for societal security purposes and specifies a common output file format that can be extracted from the video-surveillance contents collection systems (standalone machines or large-scale systems) by an exchangeable data storage media or through a network to allow end-users to access digital video-surveillance contents and perform their necessary processing.
Title	**DD CLC/TS 50131-7:2010 Alarm systems - Intrusion and hold-up systems. Application guidelines**
Description	These application guidelines are intended to provide advice relating to the design, installation, operation and maintenance of Intruder and Hold-up Alarm Systems (I&HAS). The purpose of this document is to ensure, as far as is practical, that I&HAS provide the required performance with a minimum of unwanted alarms
Title	**OASIS CAP: Common Alerting Protocol, specification version 1.2, 2010.**
Description	The Common Alerting Protocol (CAP) is a simple but general format for exchanging all-hazard emergency alerts and public warnings over all kinds of networks. CAP allows a consistent warning message to be disseminated simultaneously over many different warning systems, thus increasing warning effectiveness while simplifying the warning task. CAP also facilitates the detection of emerging patterns in local warnings of various kinds, such as might indicate an undetected hazard or hostile act. CAP also provides a template for effective warning messages based on best practices identified in academic research and real-world experience
Title	**ISO/TR 22351:2015 - Emergency management — Message structure for exchange of information**
Description	ISO/TR 22351:2015 describes a message structure for the exchange of information between organisations involved in emergency management. An organisation can ingest the received information, based on the message structure, in its own operational picture. The structured message is called Emergency Management Shared Information (EMSI). ISO/TR 22351:2015 describes the message structure built in order to facilitate interoperability between existing and new information systems.
Title	**ONVIF: ONVIF Core Specifications.**
Description	The ONVIF Core Specification aims to standardize the network interface (on the network layer) of network video products. It defines a network video communication framework based on relevant IETF and Web Services standards including security and IP configuration requirements.
Tittle	**OPC: Open Platform Communications**
Description	The OPC interoperability standard aims to ensure security and reliability of data exchanges in industries, while enabling a seamless flow of information among devices of multiples vendors. Its specifications cover the interface definition between clients- servers and servers-servers, including access to real-time data, monitoring of alarms and events and access to historical data.

Organisational Resilience Standards

In this section, the most used standards related to organisational resilience are reported and described.

TABLE 3: STANDARDS RELATED TO ORGANISATIONAL RESILIENCE

Title	**ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements**
Description	This document specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. The requirements specified in this document are generic and intended to be applicable to all organisations, or parts thereof, regardless of type, size and nature of the organisation. The extent of application of these requirements depends on the organisation's operating environment and complexity.
Title	**ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity**
Description	ISO/IEC 27031:2011 describes the concepts and principles of information and communication technology (ICT) readiness for business continuity and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving the ICT readiness of and organisation to ensure business continuity. It applies to any organisation (private, governmental, and non-governmental, irrespective of size) developing its ICT readiness for business continuity programme, and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions.
Title	**BS 65000:2014 - Guidance on Organisational Resilience.**
Description	This standard provides an overview of resilience, describing the foundations required and explaining how to build resilience. It therefore deals with the capacity of an organisation to anticipate, respond and adapt – which could be crucial to its survival. BS 65000 provides guidance on achieving enhanced organisational resilience and articulates the benefits of doing so. Currently, standards exist within the crisis management and business continuity management arenas which impact on the overall governance of an organisation. This standard can help to enhance these practices by integration of the disciplines that are essential for resilience. BS 65000 references other activities including risk management, horizon scanning and change management.
Title	**ISO 27035-1:2016 - Information Security Incident Management.**
Description	The ISO/IEC 27035 Information Security Incident Management is an international standard that provides best practices and guidelines for conducting a strategic incident management plan and preparing for an incident response. The ISO/IEC 27035 Information Security Incident Management delivers the prime principles of security to prevent and respond effectively to information security incidents. In addition, the ISO/IEC 27035 incorporates specific processes for managing information security incidents, events, and potential vulnerabilities.

Other standards related to security

In this section, some standards related to security but not falling explicitly within the previous categories are reported. They are related to risk management and to asset management, topics having a direct impact on security in its wider meaning.

TABLE 4: OTHER SECURITY-RELATED STANDARDS

Title	**ISO 31000:2018 Risk management - Guidelines**
Description	ISO 31000 is an international standard that provides principles and guidelines for effective risk management. It outlines a generic approach to risk management, which can be applied to different types of risks (financial, safety, project risks) and used by any type of organisation. The standard provides a uniform vocabulary and concepts for discussing risk management. It provides guidelines and principles that can help to undertake a critical review of the risk management process of an organisation.
Title	**ISO 55001:2014 Asset management — Management systems — Requirements**
Description	ISO 55001 is an asset management system standard, the main objective of which is to help organisations manage the lifecycle of assets more effectively. By implementing ISO 55001 organisations will have better control over daily activities, achieve higher return with their assets, and reduce the total cost of risk. This standard can be applied to all organisational structures of companies, and to all types of assets. The concrete outcomes consist of a growth in effectiveness accompanied by a dramatic drop in unit cost. This framework also supports continual improvement of performance and offers improvements for an organisation of any industry, type or size.

2.1.2 Focus on railway sector

In this section, a focus on railway sector is presented together with an overview of the current regulatory approach from technical and safety points of view. Especial attention will be put on the current approach to safety and on recent novelties in the approach to security.

The rail industry has always been one of the most regulated sectors. At a European Level, the railway sector is primarily regulated by means of the so-called 4th Railway Package, a set of legislative texts designed to complete the single market for rail services (Single European Railway Area).

The main pillars of the 4th Railway Package are:

- Directive (EU) 2016/797 (Recast Interoperability Directive) (Ref. [17])
- Directive (EU) 2016/798 (Recast Safety Directive) (Ref. [18])
- Regulation (EU) 2016/796 (‘The Agency’ Regulation) (Ref. [19])

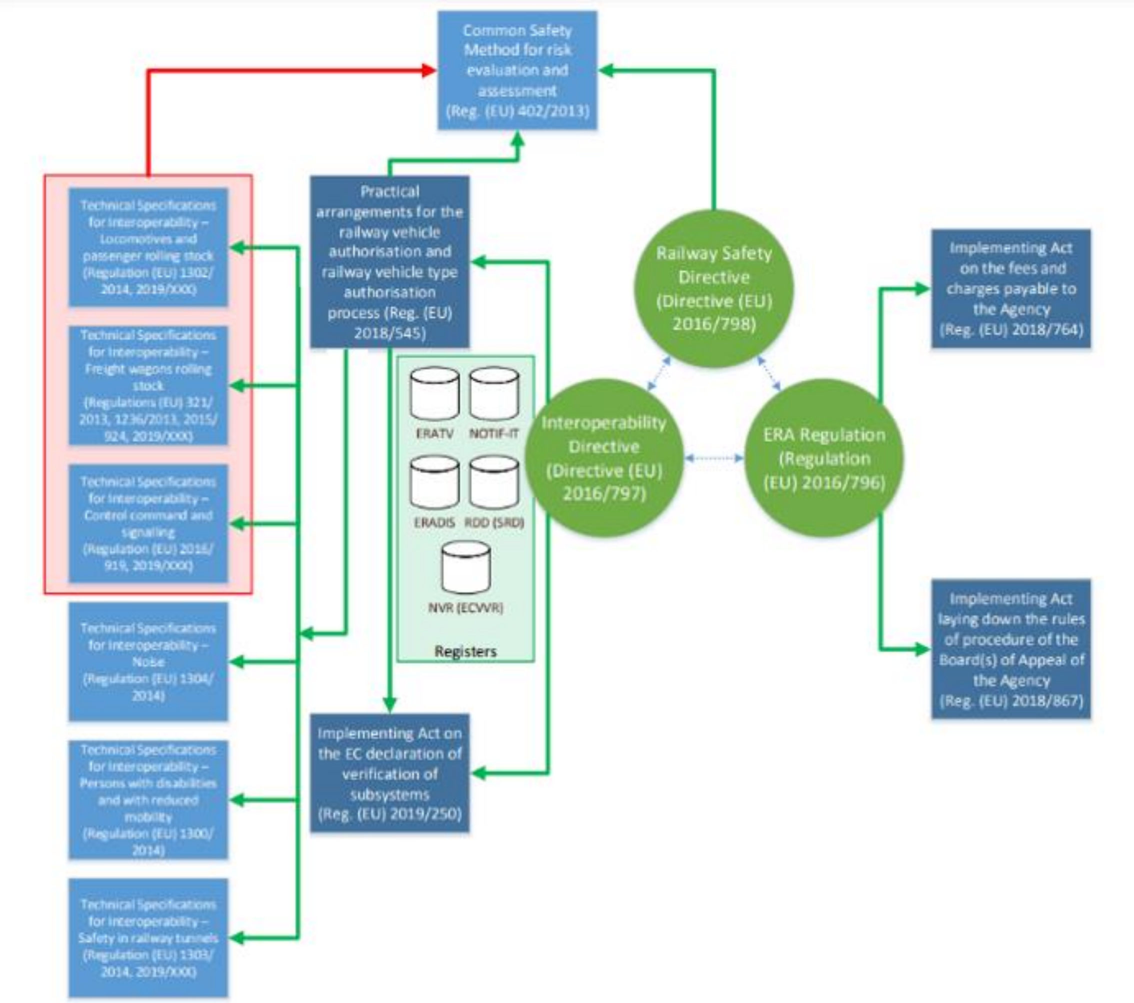

Common Safety Method for risk evaluation and assessment (Reg. (EU) 402/2013)
Practical arrangements for the railway vehicle authorisation and railway vehicle type authorisation process (Reg. (EU) 2018/545)
Railway Safety Directive (Directive (EU) 2016/798)
Implementing Act on the fees and charges payable to the Agency (Reg. (EU) 2018/764)
Technical Specifications for Interoperability – Locomotives and passenger rolling stock (Regulation (EU) 1302/ 2014, 2019/XXX)
Technical Specifications for Interoperability – Freight wagons rolling stock (Regulations (EU) 321/ 2013, 1236/2013, 2015/ 924, 2019/XXX)
Technical Specifications for Interoperability – Control command and signaling (Regulation (EU) 2016/ 919, 2019/XXX)
ERATV
NOTIF-IT
ERADIS
RDD (SRD)
NVR (ECVVR)
Registers
Interoperability Directive (Directive (EU) 2016/797)
ERA Regulation (Regulation (EU) 2016/796)
Technical Specifications for Interoperability – Noise (Regulation (EU) 1304/ 2014)
Implementing Act laying down the rules of procedure of the Board(s) of Appeal of the Agency (Reg. (EU) 2018/867)
Implementing Act on the EC declaration of verification of subsystems (Reg. (EU) 2019/250)
Technical Specifications for Interoperability – Persons with disabilities and with reduced mobility (Regulation (EU) 1300/ 2014)
Technical Specifications for Interoperability – Safety in railway tunnels (Regulation (EU) 1303/ 2014, 2019/XXX)

FIGURE 1: OVERVIEW OF 4TH RAILWAY PACKAGE

The Interoperability Directive (EU) 2016/797 sets out the conditions to be met to achieve interoperability within the Union rail system. These conditions concern the design, construction, placing in service, upgrading, renewal, operation and maintenance of the parts of this system as well as the professional qualifications and health and safety conditions of the staff who contribute to its operation and maintenance.

The Directive (EU) 2016/797 defines the subsystems forming part of the railway system of the European Union. For each of those subsystems, the essential requirements can be summarised as safety, reliability and availability, health, environmental protection, technical compatibility and accessibility. They are specified in the Technical Specifications for Interoperability (TSIs) (Ref. [20]), a set of regulations that defines the technical and operational standards which must be met by each subsystem or part of subsystem in order to meet the essential requirements and ensure the interoperability of the railway system of the European Union.

The Safety Directive (EU) 2016/798 extends the scope of safety whilst centralising supervision at the EU level. This is achieved by making ERA the single body for granting single safety certificates and by creating new bodies, tools and processes with the ERA to enable it to exercise its new mandate. This Directive also establishes the Common Safety Methods (CSMs), that describe how the safety levels, the achievement of safety targets and compliance with other safety requirements should be fulfilled. The CSMs are directly applicable and enforceable in the Member States.

The Agency Regulation (EU) 2016/796 extends the mandate and tasks of the ERA in line with the scope of Interoperability and Safety Directives. The Agency becomes an authority responsible for issuing authorisations for the placing on the market of railway vehicles and vehicle types, for issuing single safety certificates for railway undertakings in the European Union and for granting European

Rail Traffic Management System (ERTMS) trackside approval. With this new Regulation the Agency becomes the ERTMS system authority.

At national level, the railway sector is regulated by means of the so-called national rules, i.e., all binding rules adopted in a Member State, irrespective of the body issuing them, which contain railway safety or technical requirements, other than those laid down by Union or international rules, and which are applicable within that Member State to railway undertakings, infrastructure managers or third parties. National rules may be applied in addition to European rules only under certain conditions, as defined in Directive (EU) 2016/797 and in Directive (EU) 2016/798 (Ref. [18]), e.g., to cover TSIs open points, when they relate to the placing on the market or placing in service of structural subsystems, the operation of the Union rail system, the role of the actors, the safety certification, the safety authorisation and the accident investigation. National rules, which are often based on national technical standards, are being gradually replaced by rules based on common standards, established by Common Safety Methods (CSMs) and Technical Specifications for Interoperability (TSIs).

Approach to railway safety

The current approach to safety, as mentioned above, is ruled by the application of the Common Safety Methods, as required by Safety Directive. Common safety methods (CSMs) are developed to ensure that safety is maintained at a high level and, when and where necessary and reasonably practicable, improved. They aim to provide a common approach to assessing, supervising and managing railway safety at EU level and in Member States.

CSMs can be applied for several purposes:

- Common Safety Methods for risk evaluation and assessment
- Common Safety Methods for monitoring
- Common Safety Methods on safety management system requirements
- Common Safety Methods on supervision
- Common Safety Method on common safety targets
- Common Safety Methods for conformity assessment

Focusing on the Common Safety Methods for risk evaluation and assessment (CSM-RA), the Commission Implementing Regulation (EU) 402/2013 (Ref. [22]) harmonises processes for risk evaluation and assessment and the evidence and documentation produced during the application of these processes. The CSM-RA is a framework that describes a common mandatory European risk management process for the railways. The processes are intended to complement requirements in other legislation, for example on interoperability or safety certification, and not to duplicate them. In particular, this Regulation sets out:

- The risk assessment process to be applied in case of technical, operational or organisational changes;
- The criteria to be fulfilled by the assessment body responsible for checking the correct application of the risk assessment process and the results of this application, and the necessary requirements for the accreditation or recognition of its competence in order to achieve a similar quality of independent assessment;
- The harmonised design targets for technical systems which should help with mutual recognition of those systems across the European Union.

Focusing on technical electronic systems, such as Control-Command and Signalling (CCS) systems, that essentially constitutes the core of technical safety in the railway sector, the most common approach to safety in the frame determined by CSMs is the application of the well-known CENELEC standards EN 50126 (Ref. [23] and Ref. [24]), EN 50128 (Ref. [25]), EN 50129 (Ref. [26]) and EN 50159 (Ref. [27]). Their application depends on the specific part of the system whose safety shall be proven (i.e., not all of them are applicable to all electronic components). The CCS Technical Specification of Interoperability (Ref. [28] amended by Ref. [29]) explicitly state that the application of the aforementioned EN standards, and their subsequent amendments when published as harmonised standard, is an appropriate means to fully comply to the risk management process as set out in Annex

I of the Commission Implementing Regulation (EU) No 402/2013. Consequently, they constitute the most adopted approach towards fulfilment of safety requirements for CCS systems.

Security in railway sector

Currently, the European mandatory legal framework in the field of security explicitly regarding the railway sector is limited. Basically, the major legal text aimed to increase security and addressing railway sector (i.e., at least Infrastructure Managers and Railway Undertakings) is the NIS Directive. This Directive provides high-level requirements applicable in principle to a number of sectors; it does not directly introduce very specific and detailed requirements for addressing security in the railway sector.

On the other hand, at a national level, railway organisations are often subject to national security requirements that may derive from specific implementations of NIS Directive or from other legislation covering aspects not treated by NIS. For example, specific arrangements may exist regarding interaction with Police on security issues such as notification of, and the response to, threats or attacks.

Within the railway legal framework in the previous subsection, few requirements somehow related to security requirements are defined. In some cases, the existing technical and safety integrity requirements cover some security aspects: as an example, the ERTMS signalling system, that represents the core of the Single European Railway Area, can be considered.

ERTMS comprises of the European Train Control System (ETCS), i.e., a cab-signalling system that incorporates automatic train protection, the Global System for Mobile communications for Railways (GSM-R) and operating rules, as specified by the related TSIs (see Ref. [30] for further details). ERTMS has high availability and safety integrity requirements, as these are related to service provision and safety. Some cybersecurity measures are already available, such as the use of cryptographic keys for authentication between on-board and trackside subsystems when communicating through GSM-R and the encryption of the exchanged data (though not using a very recent encryption algorithm). An in-depth analysis of threats, attack vectors and measures to be derived in this context has not been conducted yet, as highlighted by ENISA in the report on cybersecurity in railway (Ref. [4]).

The availability and safety of the railway systems are also strictly related both to ICT systems and to maintenance tools and external interfaces (interlocking, maintenance system, traffic management system, etc.). These are open and not specified at EU level, so they depend on the chosen system supplier. Security requirements should be enforced on them, in order to also increase the availability and safety.

In this regard, the ENISA report on cybersecurity in railway (Ref. [4]) provides an interesting picture on the current security approach and progresses in the railway sector. Provided that the implementation of the NIS Directive in the railway sector varies between the MS and the OES, the report highlights that the security measures most widely implemented by OES regards:

- Cybersecurity basics (e.g., administrative accounts, security policy, logging, traffic filtering),
- Business continuity measures,
- Legal requirements such as safety and physical security (e.g., physical and environmental safety, incident and crisis management, incident reporting).

Security measures requiring special cybersecurity expertise and strict cybersecurity governance are instead more complex to implement. The characteristics of the railway environment (geographical extension, presence of legacy systems in place since a long time, strong dependence on the supply chain) and the complexity and lack of harmonisation constitute an obstacle to improvements in security.

The CENELEC EN 50129:2018 is one of the first norms introducing security in railway equipment and systems. It deals with safety related electronic systems for signalling and has introduced requirements imposing the evaluation of impact of IT security threats on functional safety by means of risk assessment, without specifying the specific methodology to be adopted. It does not specify requirements for development, implementation, maintenance and operation of systems, but it refers to ISO27000 and IEC 62443 series as standards related to the topic of IT security.

A very recent and interesting initiative is the elaboration by the CENELEC's Technical Committee 9X "Electrical and electronic applications for railways" of the European technical specification prTS 50701 (Ref. [31], currently reviewed, not yet published), which aims to introduce the requirements as well as provide recommendations for addressing cybersecurity within the railway sector. prTS 50701 provides the railway operators, system integrators and product suppliers, with guidance and specifications on how cybersecurity will be managed in the context of the EN 50126-1 RAMS lifecycle process. It also aims at the implementation of a consistent approach to the management of the security of the railway systems. prTS 50701 applies to 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 it at an acceptable level.

The security models, the concepts and the risk assessment process described in prTS 50701 are based on or derived from IEC 62443 series standards. This document is consistent with the application of IEC 62443 and with ISO 27001 and ISO 27002.

prTS50701 defines the activities related to cyber-security that must be carried out within the EN 50126-1 railway lifecycle and the process to be applied by the relevant stakeholders. This process is derived from IEC 62443. Additionally, it defines a set of cybersecurity requirements: they are essentially requirements from IEC 62443 accompanied by "railway notes" that informs the stakeholders about the existence of railway specifics consideration as guidance (informative).

2.1.3 Methodology adopted

The methodology adopted for the definition of standardisation requirements is described in this section.

As a first step, a questionnaire has been prepared by RINA and shared with all the partners involved in the Task, both technical partners and end-users. The goals of the questionnaire were primarily to:

- Identify a set of legal texts and standards related to security aspects (cyber, physical, cyber-physical, resilience, etc.) (input for section 2.1.1, as reported above);
- Identify the standards that are typically required, even if not mandatory by law (input for section 2.1.1, as reported above);
- Obtain some feedback on their applicability to S4RIS;
- Collecting opinions regarding a possible future certification of S4RIS.

Following the first collection of feedbacks, the information was processed in order to especially focus on those topics of interest for the Task 2.4.

All the collected feedbacks will in any case be useful also for the Task 9.3, since it will take the Task 2.4 as an input.

As a second step, a set of meetings was held to discuss the more applicable standards and to identify an approach to select/identify/define the requirements in principle applicable to S4RIS as a future product. The development cycle within SAFETY4RAILS aims at reducing the gap between what is available at the start of the project with the contributory tools and what has been identified as needed for marketable products.

Basically, the only legal text identified as applicable to S4RIS platform is the NIS Directive, since it is applicable for Infrastructure Managers and Railway Undertakings. As the Directive is not mandatory by itself but transposed to national legislations, differences may be present at national level between the Member States (as explained in section 2.1.1.1). SAFETY4RAILS is a project developed at EU level targeting Technology Readiness Level 7: System prototype demonstration in operation environment (Ref. [32]) and as noted above national technical standards, are being gradually replaced by rules based on common standards. On this basis, considering also the resource constraints in the project, it was agreed it is appropriate for SAFETY4RAILS not to focus in detail on potential specific variables derived from national legislation. (However, if a tool provider(s) in the project identifies a requirement(s) from specific national legislation(s) which could have a large impact on the marketability of a future product(s); specification(s) in answer to the requirement(s) can be defined in SAFETY4RAILS and development to achieve the specification(s) can be worked on in the project.)

In line with this approach, it was agreed to follow the standards that are more often internationally recognised and adopted by companies. So, the major drivers for the definition of the standardisation requirements have been identified as the ISO 27001 and the IEC 62443. This approach is implicitly endorsed by ENISA report Ref. [7] and tool Ref. [11], that mainly refer to these standards as the most widespread when mapping security measures to OES in railway environment.

- ISO 27001 provides requirements for the Information Security Management Systems and is applicable to any kind of organisation. In order to be compliant with ISO 27001, the organisations must define and put in place a set of security procedures and measures (namely called "controls" within the standard itself). S4RIS will be inevitably integrated within the information system of the Infrastructure Managers that will 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, that 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 railway environment is proven by CENELEC prTS 50701, that is essentially based on IEC 62443 and that provides IEC 62443 requirements with specific notes relevant to the railway environment. Deriving requirements from IEC 62443 allows future S4RIS products to be already in line with prTS50701.

  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.

Some additional specific requirements have been identified from other standards that have been identified as relevant, such as ISO 27035 regarding incident management.

When relevant, references to specific standards or best practices are provided with the requirements.

The ECI and the (proposed) CER Directives have been also taken into consideration. S4RIS will help Railway and Metro stakeholders to meet requirements that will derive from the CER Directive, providing tools and capabilities aimed to increase physical security. For the scope of this document, no explicit requirements for the S4RIS platform have been derived from them.

The list of requirements has been reviewed internally by Task 2.4 partners and has been subject to discussion and review during the second end-users' workshop held on 10/03/2021. The workshop's main outcomes regarding standardisation requirements were the following:

- The process adopted for defining standardisation requirements has been validated;
- The ranking of a large set of requirements allowed to collect end-users' perspective on the topic. The rankings reported in the next section reflects this activity;
- Review of the approach toward internal and external interoperability;
- Confirmation of the set of possibilities for integrating S4RIS with end-users' existing systems.

2.2 List of standardisation requirements

This section reports the standardisation requirements defined through the methodology illustrated in section 2.1.3.

Note: the functionalities described in the requirements below might be performed by an external component and not directly by S4RIS (e.g., centralized user identification system). In such a case, the system shall provide an 'interface' to that external component.

Requirement ID	STD-R01
Short name	Human user identification and authentication
Key objectives	- identify and authenticate each human user
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS shall comply with IEC 62443-3-3 SR 1.1 and SR 1.1 (1).
Comments	This requirement deals with to identification and authentication of human users.
Reference	ISO 27001, ISO 27002 (A.9.1) IEC 62443-3-3 (SR 1.1)

Requirement ID	STD-R02
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 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)

Requirement ID	STD-R03
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)

Requirement ID	STD-R04
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)

Requirement ID	STD-R05
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 shall 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)

Requirement ID	STD-R06
Short name	User account uniqueness
Key objectives	- guarantee uniqueness of each user
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS shall comply with IEC 62443-3-3 SR 1.4.
Comments	Unique identification of accounts is aimed to link each user to his/her actions.
Reference	ISO 27001, ISO 27002 (A.9.2.1) IEC 62443-3-3 (SR 1.4)

Requirement ID	STD-R07
Short name	Secure log-on
Key objectives	- ensure that log-on is implemented according to current best practices
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS shall comply with IEC 62443-3-3 SR 1.5.
Comments	Secure log-on is essential to avoid unauthorized human users to access the S4RIS system. It may be provided also 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)

Requirement ID	STD-R08
Short name	Secure log-on feature 1
Key objectives	-avoid disclosures of information to unauthorized users
Type of requirement	Non-functional
Priority rank	Conditional
Description	S4RIS should apply the implementation guidance of ISO 27002 9.4.2 a).
Comments	This requirement is aimed to avoid unwanted disclosure of information.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Requirement ID	STD-R09
Short name	Secure log-on feature 2
Key objectives	- reduce probability for unauthorized users to log-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 is aimed not to help unauthorized users.

Reference	ISO 27001, ISO 27002 (A.9.4.2)

Requirement ID	STD-R10
Short name	Secure log-on feature 3
Key objectives	- reduce probability for unauthorized users to log-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)

Requirement ID	STD-R11
Short name	Secure log-on feature 4
Key objectives	- protect from brute force log-on attempts
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS shall comply with IEC 62443-3-3 SR 1.11.
Comments	This requirement protects from brute force attacks to 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)

Requirement ID	STD-R12
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)

Requirement ID	STD-R13
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 allows the user to understand if someone else has tried to access with its username.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Requirement ID	STD-R14
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 of ISO 27002 9.4.2 i).

Comments	This requirement reduce the risk of password peeking by unauthorized people.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Requirement ID	STD-R15
Short name	Secure log-on feature 8
Key objectives	- reduce the probability for the password to be intercepted
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS shall apply the implementation guidance of ISO 27002 9.4.2 j).
Comments	Deprecated cyphering mechanism must be avoided.
Reference	ISO 27001, ISO 27002 (A.9.4.2)

Requirement ID	STD-R16
Short name	Password management
Key objectives	- adopt appropriate password management system
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS shall support the management of password. It can be implemented using an internal password management system or an external/existing password management system
Comments	The system shall provide the possibility to manage passwords, using internal or external systems. Features for this system are detailed in requirements "Password management feature N"
Reference	ISO 27001, ISO 27002 (A.9.4.3)

Requirement ID	STD-R17
Short name	Password management feature 1
Key objectives	- allow user to choose and change his/her password
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS shall 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)

Requirement ID	STD-R18
Short name	Password management feature 2
Key objectives	- guarantee strong password choice
Type of requirement	Non-functional
Priority rank	Essential/Conditional
Description	S4RIS shall/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, that 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)

Requirement ID	STD-R19
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 up to the end-users, based on their internal policies. Note: for the use cases, this duration might be set to few days in order to be able to check it
Reference	ISO 27001, ISO 27002 (A.9.4.3)

Requirement ID	STD-R20
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 up to end users, based on their internal policies.
Reference	ISO 27001, ISO 27002 (A.9.4.3)

Requirement ID	STD-R21
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 practices is fundamental when Public Key mechanisms are employed. Examples of well-known practices: 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)

Requirement ID	STD-R22
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)

Requirement ID	STD-R23
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)

Requirement ID	STD-R24
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 shall comply with IEC 62443-3-3 SR 2.1.
Comments	This requirement addresses the concept of segregation of duties. S4RIS functionalities shall be available only to users that are authorized to use them. For example, an operator might be allowed to operate the Monitoring part but not allowed to operate the Risk-Analysis part, so the functions shall be accessible to authorized 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)

Requirement ID	STD-R25
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 shall apply the implementation guidance of ISO 27002 9.4.1.
Comments	A mechanism to manage the access rights of users shall be implemented in S4RIS. For example, a menu accessible only by administrator could be implemented for this purpose. Note: the definition of the policy to manage access rights of the users is out of scope of SAFETY4RAILS project.
Reference	ISO 27001, ISO 27002 (A.9.4.1)

Requirement ID	STD-R26
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)

Requirement ID	STD-R27
Short name	Session lock
Key objectives	- ensure that after a period of inactivity, the sessions are locked - reduce probability of unauthorized access
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS shall comply with IEC 62443-3-3 SR 2.5.
Comments	The definition of the timer duration is up to 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)

Requirement ID	STD-R28

Short name	Termination of remote sessions
Key objectives	- ensure that after a period of inactivity, the sessions are terminated - reduce probability of unauthorized access
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS shall comply with IEC 62443-3-3 SR 2.6.
Comments	This requirement aims to avoid that unauthorized users get 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)

Requirement ID	STD-R29
Short name	Limit of contemporary sessions
Key objectives	- limit the possibility of DoS attack
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS shall comply with IEC 62443-3-3 SR 2.7.
Comments	This requirement allows to control 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)

Requirement ID	STD-R30
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 shall 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)

Requirement ID	STD-R31
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)

Requirement ID	STD-R32
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)

Requirement ID	STD-R33
Short name	Timestamp for audit
Key objectives	- improve audit records management
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS shall 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)

Requirement ID	STD-R34
Short name	Non-repudiation of users
Key objectives	-prevent false claims by users
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS shall comply with IEC 62443-3-3 SR 2.12.
Comments	This requirement allows to avoid that users claim of not having performed some 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)

Requirement ID	STD-R35
Short name	Access to audit information
Key objectives	-prevent unauthorized modifications to audit records
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS shall 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)

Requirement ID	STD-R36
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 shall/should be classified accordingly 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) shall be classified according to some 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 shall be protected from unauthorized access and circulation.

Reference	ISO 27001, ISO 27002 (A.8.2.1)

Requirement ID	STD-R37
Short name	Information classification scheme
Key objectives	- ensure that information receives an appropriate level of protection in accordance to its importance
Type of requirement	Non-functional
Priority rank	Essential/Conditional
Description	The classification of information shall/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. In case b) is implemented, the classification of generated information shall/should not be skippable by the operator.
Comments	Classification of information shall/should be carried out according to end-user company's 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 shall/should be obliged to apply classification before doing any other action. NOTE: the definition of classification procedures and criteria is out of the scope and shall be determined by the end-user company. S4RIS shall only provide the possibility to classify information.
Reference	ISO 27001, ISO 27002 (A.8.2.1)

Requirement ID	STD-R38
Short name	Information labelling
Key objectives	- ensure that information receives an appropriate level of protection in accordance to its importance
Type of requirement	Functional
Priority rank	Essential/Conditional
Description	The information generated by S4RIS that can be stored and/or shared shall/should be labelled accordingly to their value, criticality and sensitivity.
Comments	Labelling of classified information is important for compliance to ISO 27001. It allows to easily identify the level of classification of the information
Reference	ISO 27001, ISO 27002 (A.8.2.2)

Requirement ID	STD-R39
Short name	Information labelling scheme
Key objectives	- ensure that information receives an appropriate level of protection in accordance to its importance
Type of requirement	Non-functional
Priority rank	Essential/Conditional
Description	The labelling of information shall/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 case b) is implemented, the labelling of generated information shall/should not be skippable by the operator.
Comments	Labelling of classified information shall/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, he/she must be obliged to apply classification before doing 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)

Requirement ID	STD-R40
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 shall comply with IEC 62443-3-3 (SR 3.1).
Comments	Information integrity and confidentiality are two of the fundamental concepts in security and shall be enforced to 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)

Requirement ID	STD-R41
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 shall 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)

Requirement ID	STD-R42
Short name	Information backup
Key objectives	- to minimize data loss in case of attacks
Type of requirement	Other
Priority rank	Essential
Description	S4RIS shall 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 scope of this document.
Reference	ISO 27001, ISO 27002 (A.12.3) IEC 62443-3-3 (SR 7.3)

	ISO 22301

Requirement ID	STD-R43
Short name	Recovery and restore
Key objectives	- to be able to restore the system
Type of requirement	Other
Priority rank	Essential
Description	S4RIS shall 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

Requirement ID	STD-R44
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 composing S4RIS 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)

Requirement ID	STD-R45
Short name	Source code protection
Key objectives	- prevent unauthorized access to source code
Type of requirement	Non-functional
Priority rank	Essential
Description	Source code shall not be included in clear text within the system, neither on clients nor on servers.
Comments	The S4RIS system shall 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)

Requirement ID	STD-R46
Short name	Infrastructure monitoring
Key objectives	- monitor IT/OT infrastructure
Type of requirement	Functional
Priority rank	Essential
Description	S4RIS shall 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

	possibility 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)

Requirement ID	STD-R47
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 shall 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 among 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] could be considered.
Reference	ISO 27035

Requirement ID	STD-R48
Short name	Overall security event / incident / vulnerability database
Key objectives	- to keep record of security events / incidents /vulnerabilities
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS shall 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 roles-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] could be considered.
Reference	ISO 27035

Requirement ID	STD-R49
Short name	Automatic correlation of different incidents detected
Key objectives	- to allow 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 it is the effect of another incident. This is important in prioritizing 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] could be considered.
Reference	ISO 27035

Requirement ID	STD-R50
Short name	Security incident management system governance
Key objectives	- to guarantee that each user accesses only information he/she is allowed to
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS shall allow/support the integration of the security incident management system as defined in ISO 27035, following a roles-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] could be considered.
Reference	ISO 27035

Requirement ID	STD-R51
Short name	Attributes relevant for security incident management
Key objectives	- to allow for better decision support during response
Type of requirement	Non-functional
Priority rank	Essential
Description	S4RIS security incident management system shall include relevant attributes, such as significance, priority and acceptable interruption window should be integrated into the security incident management system. S4RIS shall 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] could be considered.
Reference	ISO 27035

Requirement ID	STD-R52
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 shall collect all volatile data shall 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] could be considered.
Reference	ISO 27035

Requirement ID	STD-R53
Short name	Guidelines to inform 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 shall be made available and easily accessible to inform those responsible for internal and external communications.

Comments	May need to occur in several stages: a good set 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] could be considered.
Reference	ISO 27035

Requirement ID	STD-R54
Short name	Video Coding and metadata representation
Key objectives	- to ensure 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

Requirement ID	STD-R55
Short name	Alerting protocol for emergencies
Key objectives	- to provide support for alerting and public warnings
Type of requirement	Non-functional
Priority rank	Conditional
Description	If an automated alerting system will be implemented in the S4RIS platform, the used protocol should be OASIS CAP.
Comments	OASIS CAP is one of the most widespread protocol for exchanging messages for exchanging messages and public warnings between alerting systems. Further details are provided in the guidelines below.
Reference	-

2.3 Additional guidelines and recommendations

In this section, some additional guidelines and recommendations are provided. They should be taken in consideration for the development of the S4RIS platform.

2.3.1 Alerting and public warning systems: OASIS - Common Alerting Protocol (CAP)

Alerting and public warning systems are used worldwide to exchange information between regional or national public bodies (such as police, firefighters, civil protection, etc.) and for warning citizens of ongoing emergencies of any kind. This matter is typically managed at national level and various implementations are possible. Since S4RIS will also deal with emergency management, it could be convenient to adopt a common and widespread mechanism for exchanging alerts and warning.

In this sense, a possible and desirable choice is represented by the OASIS CAP protocol (Ref. [33]) since it is one of the most widespread protocols adopted for this purpose at international level. Hereafter, a description of the protocol and of its characteristics is provided supporting this statement. The content of the following sections (from 2.3.1.1 to 2.3.1.4) is extracted from Ref. [33], with minor rewording to fit the context[2].

[2] Notices from Ref. [33]

2.3.1.1 CAP Purpose, Capabilities and Key Benefits (extract from §1.1 from Ref. [33])

CAP provides an open, non-proprietary digital message format for all types of alerts and notifications. Its format is compatible with both existing formats and emerging ones, such as Web services. The CAP message format can be converted to and from the "native" formats of all kinds of sensor and alerting technologies, forming a basis for a technology-independent national and international "warning Internet."

CAP offers enhanced capabilities, including:

(1) Flexible geographic targeting using geospatial representations in three dimensions;

(2) Multilingual and multi-audience messaging;

(3) Phased and delayed effective times and expirations;

(4) Enhanced message update and cancellation features;

(5) Template support for framing complete and effective warning messages;

(6) Compatible with digital signature capability; and

(7) Facility for digital images and audio.

Key benefits of CAP include reduction of costs and operational complexity by eliminating the need for multiple custom software interfaces to the many warning sources and dissemination systems involved in all-hazard warning. The CAP Alert Message reduces the workload associated with using multiple warning systems, while enhancing technical reliability and target-audience effectiveness.

2.3.1.2 Structure of the CAP Alert Message (extract from §1.3 from Ref. [33])

2.3.1.2.1 Structure

Each CAP Alert Message consists of an <alert> segment.

Each <alert> segment may contain one or more <info> segments.

Each <info> segment may include one or more <area> and/or <resource> segments.

Under most circumstances, CAP messages with a <msgType> value of "Alert" should include at least one <info> element.

2.3.1.2.2 <alert>

The <alert> segment provides basic information about the current message: its purpose, its source and its status, as well as a unique identifier for the current message and links to any other, related messages. An <alert> segment may be used alone for message acknowledgements, cancellations or other system functions, but most <alert> segments will include at least one <info> segment.

2.3.1.2.3 <info>

The <info> segment describes an anticipated or actual event in terms of its urgency (time available to prepare), severity (intensity of impact) and certainty (confidence in the observation or prediction), as well as providing both categorical and textual descriptions of the subject event. It may also provide instructions for appropriate response by message recipients and various other details (hazard duration, technical parameters, contact information, links to additional information sources, etc.) Multiple <info> segments may be used to describe differing parameters (e.g., for different probability or intensity "bands") or to provide the information in multiple languages.

2.3.1.2.4 <area>

The <area> segment describes a geographic area to which the <info> segment in which it appears applies. Textual and coded descriptions (such as postal codes) are supported, but the preferred representations use geospatial shapes (polygons and circles) and an altitude or altitude range, expressed in standard latitude / longitude / altitude terms in accordance with a specified geospatial datum.

2.3.1.2.5 <resource>

The <resource> segment provides an optional reference to additional information related to the <info> segment within which it appears, as a digital asset, such as an image or audio file.

2.3.1.3 Applications of the CAP Alert Message (extract from §1.4 from Ref. [33])

The primary use of the CAP Alert Message is to provide a single input to activate all kinds of alerting and public warning systems, while also helping ensure consistency in the information transmitted over multiple delivery systems. A secondary CAP application is to normalise warnings from various sources, so that they can be aggregated and compared in tabular or graphic form, as an aid to situational awareness and pattern detection. Although primarily designed as an interoperability standard for use among warning systems and other emergency information systems, the CAP Alert Message can be delivered directly to alert recipients over various networks, including data broadcasts. Location-aware receiving devices could use the information in a CAP Alert Message to determine, based on their current location, whether that particular message was relevant to their users. The CAP Alert Message can also be used by sensor systems as a format for reporting significant events to collection and analysis systems and centres.

2.3.1.4 CAP Alert Message Design Principles and Concepts

2.3.1.4.1 CAP Alert Message Design Principles (extract from §2.1 from Ref. [33])

The OASIS CAP sets the following design principles:

(1) **Interoperability** – the message should provide a means for interoperable exchange of alerts and notifications among all kinds of emergency information systems.

(2) **Completeness** – the message format should provide for all the elements of an effective public warning message.

(3) **Simple implementation** – the design should not place undue burdens of complexity on technical implementers.

(4) **Simple XML and portable structure** – although the primary anticipated use of the CAP Alert Message is as an XML document, the format should remain sufficiently abstract to be adaptable to other coding schemes.

(5) **Multi-use format** – one message schema supports multiple message types (e.g., alert / update / cancellations / acknowledgements / error messages) in various applications (actual / exercise / test / system message).

(6) **Familiarity** – the data elements and code values should be meaningful to warning originators and non-expert recipients alike.

(7) **Interdisciplinary and international utility –** the design should allow a broad range of applications in public safety and emergency management and allied applications and should be applicable worldwide.

2.3.1.4.2 Requirements for Design (extract from §2.2 from Ref. [33])

The following requirements for design are achieved by OASIS CAP:

(1) Provide a specification for a simple, extensible format for digital representation of warning messages and notifications;

(2) Enable integration of diverse sensor and dissemination systems;

(3) Be usable over multiple transmission systems, including both TCP/IP-based networks and one-way "broadcast" channels;

(4) Support credible end-to-end authentication and validation of all messages;

(5) Provide a unique identifier (e.g., an ID number) for each warning message and for each message originator;

(6) Provide for multiple message types, such as:

   a. Warnings
   b. Acknowledgements
   c. Expirations and cancellations
   d. Updates and amendments
   e. Reports of results from dissemination systems

f. Administrative and system messages

(7) Provide for multiple message types, such as:

a. Geographic targeting

b. Level of urgency

c. Level of certainty

d. Level of threat severity

(8) Provide a mechanism for referencing supplemental information (e.g., digital audio or image files, additional text);

(9) Use an established open-standard data representation;

(10) Be based on a program of real-world cross-platform testing and evaluation;

(11) Provide a clear basis for certification and further protocol evaluation and improvement; and,

(12) Provide a clear logical structure that is relevant and clearly applicable to the needs of emergency response and public safety users and warning system operators.

2.3.1.5 Examples of Use Scenarios (extract from §2.3 from Ref. [33])

2.3.1.5.1 Manual Origination

The Incident Commander at an industrial fire with the potential of a major explosion can issue a public alert as a CAP message, covering: a) Evacuation of the defined area; b) A shelter-in-place instruction for people in the downward plume; and c) A request for all civilian aircraft in the vicinity to remain above a certain altitude.

2.3.1.5.2 Automated Origination by an Autonomous Sensor System

Individual CAP messages are generated by a wireless network of tsunami sensors, when triggered. Each message contains the generating sensor's location and sensed data needed for tsunami determination. Each sensor is co-located with a siren, which is activated when the combination of its own readings and those reported at by other devices on the network indicate an immediate tsunami threat. A network component assembles a summary CAP message describing the event and feeds it to regional and national alerting networks.

2.3.1.5.3 Aggregation and Correlation on a Real-time Map

At the State Operations Centre a computerised map of the state depicts, in real time, all current and recent warning activity throughout the state. All major warning systems in the state have been equipped to report the details of their activation in the form of a CAP message. Using this visualisation tool, state officials can monitor for emerging patterns of local warning activity and correlate it with other real time data.

2.3.1.5.4 Integrated Public Alerting

As part of an integrated warning system funded by local industry, all warning systems in a community can be activated simultaneously by the issuance, from an authorised authority, of a single CAP message. Each system converts the CAP message data into the form suitable for its technology (text captioning on TV, synthesized voice on radio and telephone, activation of the appropriate signal on sirens, etc.). Systems that can target their messages to particular geographic areas implement the targeting specified in the CAP message with as little "spillover" as their technology permits. In this way, not only is the reliability and reach of the overall warning system maximized, but citizens also get corroboration of the alert through multiple channels, which increases the chance of the warning being acted upon.

2.3.1.5.5 Repudiating a False Alarm

Inadvertently, the integrated alerting network has been activated with an inaccurate warning message. This activation comes to officials' attention immediately through their own monitoring facilities. Having determined that the alert is, in fact, inappropriate, the officials issue a cancellation message that refers directly to the erroneous prior alert. Alerting systems that are still in the process of delivering the alert (e.g., telephone dialling systems) stop doing so. Broadcast systems deliver the cancellation message. Other systems (e.g., highway signs) simply reset to their normal state.

2.3.2 Risk Management Standard (ISO 31000) Overview

Security is typically approached starting from a risk-analysis basis. This section provides guidelines on a very commonly adopted risk management standard, ISO 31000. These guidelines might be taken into consideration for the development of the Risk Assessment tool for S4RIS. Furthermore, in the future they could be useful also for less mature Infrastructure Managers and Railway Undertakings that have started implementing security measures only recently (e.g., small/regional Infrastructure Managers and Railway Undertakings)

2.3.2.1 Purpose

ISO 31000, Risk management – Guidelines, provides principles, a framework and a process for managing risk, and allows comparing with an internationally recognized benchmark. Risk management is a structured process whose goal is to develop and implement safeguards that will protect an organisation from the consequences of specific threats it faces, should they materialize. In the context of security, it enables mitigating the various risks arising from security threats to a predefined manageable level, utilizing the means – both internal and external – at the disposal of the organisation.

2.3.2.2 Risk Management Principles

Efficient risk management is achieved when it:

(1) Creates and protects value.
(2) Is an integral part of all organisational processes.
(3) Is part of decision making.
(4) Explicitly addresses uncertainty.
(5) Is systematic, structured and timely.
(6) Is based on the best available information.
(7) Is tailored.
(8) Takes human and cultural factors into account.
(9) Is transparent and inclusive.
(10) Is dynamic, iterative and responsive to change.
(11) Facilitates continual improvement of the organisation.

2.3.2.3 Risk Management Process

The risk management process should be an integral part of the organisation's management, embedded in its culture and practices, and tailored to its business processes.

Figure 2 describes the process and interfaces.

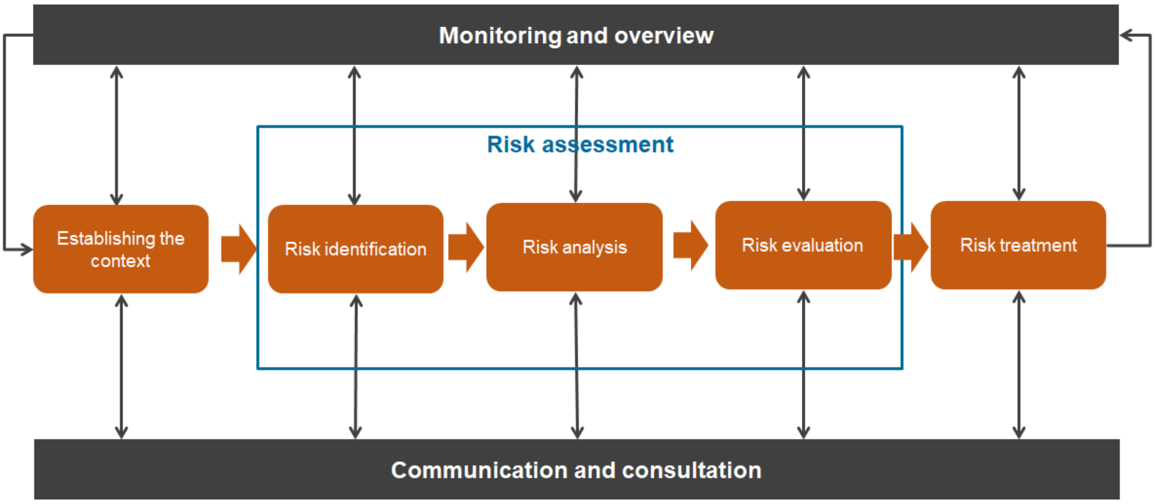


FIGURE 2: RISK MANAGEMENT PROCESS

According to the ISO 31000 standard, the process of risk management consists of the following five steps:

(1) **Establishing the context.** This includes the planning stage, mapping the scope, objectives & constraints, and defining the framework and agenda.

(2) **Risk identification.** Identification of the sources of risk, areas of impact, the events and their potential consequences.

(3) **Risk analysis.** To serve as input for the risk evaluation process and decision making on whether risks need to be treated, and on the most appropriate risk treatment strategies and methods.

(4) **Risk evaluation.** Aimed to assist in making decisions, based on the outcomes of the risk analysis and the priority for treatment implementation.

(5) **Risk treatment.** Selecting and executing one or more optional actions to reduce the risks.

Each step of the risk management process is reviewed and discussed with relevant stakeholders. The entire process is repeated periodically to ensure changes in the organisation and in the threat environment are taken into account.

2.3.2.4 Risk treatment strategies

The risk management standard defines four risk management strategies:

(1) Risk mitigation (control or reduction). Techniques that reduce the severity of the consequences or the likelihood of their occurrence. Risk mitigation is the security management strategy most often implemented by infrastructure managers, railway undertaking and public transport operators.

(2) Risk acceptance (retention). Advance acceptance of potential consequences. Risk acceptance is a viable strategy in the case of small risks, where the cost of insuring against the risk would be greater, over time, than the total losses sustained. Self-insurance falls into this category.

(3) Risk transfer. As insurance that compensates for losses caused by security attacks does not comprise a total risk transfer strategy, it is not commonly implemented by infrastructure managers, railway undertaking and public transport operators. A good example is the transfer of risks of attack with weapons of mass destruction or risk from LIC (Low Intense Conflict) to state authorities who assume the handling of the risk by implementing proper preparatory measures, and are also responsible for compensating the infrastructure managers, railway undertaking, other public transport operators and the passengers if such a risk is realised.

(4) **Risk avoidance (or elimination).** A strategy of not taking action, which inherently requires taking risks. In the case of railway and public transport systems, this strategy is inappropriate, since it implies there will be no public transport systems in order to avoid exposure to any risk connected with operating them.

2.3.3 Secure coding

Software is essential to the operation of the critical infrastructures. In order to reduce the risk of exploitable code flaws that could lead to severe consequences, there exist a set of secure coding practices that should be followed. They can help to ensure that software is safeguarded against software security vulnerabilities. Hereafter, some examples of secure coding practices are presented.

2.3.3.1 Open Web Application Security Project (OWASP)

OWASP is the Open Web Application Security Project (Ref. [37]). It is an international non-profit organisation that educates software development teams on how to conceive, develop, acquire, operate, and maintain secure applications.

On the website of the project, a set of guidelines to develop and test secure software are available. In particular, the project maintains the OWASP Top 10 (Ref. [38]), a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications. The project also published the OWASP Code Review Guide (Ref. [34]), that has been developed to advise software developers on the best practices in secure code review. It starts analysing the OWASP Top 10 issue.

The use of these best practices might be considered.

2.3.3.2 CERT Coding Standard

CERT is a set of secure coding standards (Ref. [39]) that supports the commonly used programming languages C, C++, Java and Perl. It is also available for Android development.

The standards are developed through a broad-based community effort by members of the software development and software security communities. The rules and recommendations target insecure coding practices and undefined behaviours that lead to security risks.

For each guideline included in the secure coding standard, there is a risk assessment to help determine the possible consequences of violating that specific rule or recommendation. There are three sections to the risk assessment: Severity, Likelihood, and Remediation Cost. Each section is assigned a value between 1 and 3, and based upon the results of the assessment, it allows to determine the priority of the violation.

The use of these standards might be considered, if available, for the languages used in S4RIS.

2.3.3.3 Public lists of vulnerabilities

Several lists of vulnerabilities are available online, to inform developers of the most common and risky exposures. Some of the most common and used lists are:

- **CWE** (Common Weaknesses Enumeration) is a list of software security weaknesses in software and hardware, which includes programming languages C, C++, and Java. In addition, the CWE Top 25 is a compilation of the most widespread and critical weaknesses that could lead to severe software vulnerabilities (Ref. [40]).
- **CVE** (Common Vulnerabilities and Exposures) is a list of cybersecurity vulnerabilities and exposures found in a specific software product (Ref. [41]).
- **NVD** (National Vulnerability Database) is the U.S. government repository of standards-based vulnerability management data and it is connected with the CVE list and provides additional content, including how to fix vulnerabilities, severity scores, and impact ratings. (Ref. [42]);

The consultation of these lists is advisable when developing S4RIS.

3. Interoperability requirements

3.1 Introduction

In the project SAFETY4RAILS, software tools coming from different organisations will be integrated with S4RIS. To ensure useful and working integration, an interoperability concept is designed in this section. The concept considers software tools coming from different partners including their functionalities and contribution to the overall system.

3.1.1 Definition of interoperability in S4RIS context

S4RIS aims to develop an information system platform to establish an intermodal technology. The various systems or tools developed by SAFETY4RAILS technological partners are independent in technical requirements and compatibilities. From the user perspective, the concept of software-based integration should be unified and compatible with existing information technological environments. The interoperability is hence responsible: to unite the standards and shared information for the tool developers; to make the system accessible in order to ensure (cyber and physical) security on railway operation and infrastructure for the end-users. This means that the S4RIS will be an information system which should be able to communicate with existing information systems used in the railway sector. Therefore, interoperability definitions in the field of information systems are used to elaborate the interoperability concept in SAFETY4RAILS.

Interoperability has several definitions and concepts targeted at reaching adequate integration of different systems and tools as well as their alignment, depending on the application field. In collaborative information technology, a term of interoperability has been introduced to organise different enterprise systems and propose solutions to handle two or more incompatible systems to operate together in a coherent manner and avoid apparition of related problems (Ref. [48]). The definition given by the Institute of Electrical and Electronics Engineers (IEEE) (Ref. [49]) as well as the definition by the International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC) (Ref. [51]) state that interoperability defines the data alignment and the exchange of information in-between two or more components or systems. The authoritative Dictionary of IEEE Standard terms (Ref. [50]) defines the interoperability of the system with four aspects, mentioned in [SOSI Final Report (Ref. [52])]:

- *“The ability of two or more systems or elements to exchange information and to use the information that has been exchanged.*
- *The capability for units of equipment to work together to do useful functions.*
- *The capability, promoted but not guaranteed by joint conformance with a given set of standards, that enables heterogeneous equipment, generally built by various vendors, to work together in a network environment.*
- *The ability of two or more systems or components to exchange information in a heterogeneous network and use that information.”*

Summarised, an interoperability concept is used to define the information exchange and data alignment in heterogenous systems consisting of various components. In other words, it defines which components exchange information, how they exchange this information and how the information is used in the system.

3.1.2 Methodology adopted

The definitions given above imply for SAFETY4RAILS that an interoperability concept defining the data exchange and alignment within the S4RIS needs to be implemented, as well as a concept for the interoperability between the S4RIS and external systems since the S4RIS is a heterogenous system connecting to heterogenous systems at end-user’s side (at least when implemented as a product).

To guarantee an adequate use of each tool and an adequate integration and contribution to the S4RIS, the tool providers in the project were asked to provide information about their tools within a questionnaire. It asked amongst other information for existing interfaces including Graphical User Interfaces (GUI), technical interfaces (e.g., REST/API) and main focus of the tools (e.g., Resilience Phase(s), Monitoring, Simulation). Based on this information, the operational interoperability requirements were defined for the S4RIS as well as for external systems. This is input into the architecture for the S4RIS and for integration in / with external systems (through further tasks in the project). The foreseen architecture should be very flexible and generic, particularly during the project, to ensure a working integration of the heterogenous systems and to provide possibilities for adapting the S4RIS prototype(s) to the end-users' needs.

The topic of interoperability has been discussed and reviewed during the second end-users' workshop held on 10/03/2021. The workshop's main outcomes regarding interoperability were the following:

- Review of the approach toward internal and external interoperability;
- Discussion and confirmation of the set of possibilities for integrating S4RIS with end-users' existing systems.

3.2 Operational interoperability requirements

Following on from the previous section above, the information gathered from the tool providers contained tool name and the partner providing it, input and output parameters, information regarding interfaces, some further technical descriptions as well as an assignment of the tools to real-time or static computation. This information is collected in the requirement tables below.

Based on this information, the need for a flexible interoperability has been determined, requiring a generic and configurable architecture for the S4RIS. Figure 3 depicts the tools foreseen to be included in the S4RIS platform and a representation of their possible connections within the S4RIS, identifying the complexity of the potential communications between tools both within the S4RIS itself and to external systems. This representation was input into the overall concept architecture presented in the deliverable D2.3 System's specifications and concept architecture (D2.3) and needs to be considered together with this architecture.

In Figure 3, a colour code is used to indicate both the focus of individuals tools functions at a high-level[3] and also the primary layer in which they are foreseen to be placed within the S4RIS platform architecture[4]. These layers are described in more detail in D2.3 and will be implemented in the project later in the "Task 6.2 Technical interoperability and interfaces".

Within the project (as a prototype) it will enable flexibility in developing, testing, fine-tuning and evaluating the platform with its contributory tools, also within the pilot testing with end-users.

Based on this scheme, an end-user could elaborate which components provided by the S4RIS (as a product) are useful for its needs, to use the platform as an extension of its own systems.

[3] Real-time monitoring / infrastructure; simulation; and/or risk assessment / decision support

[4] Source, processing, and decision support / application layer

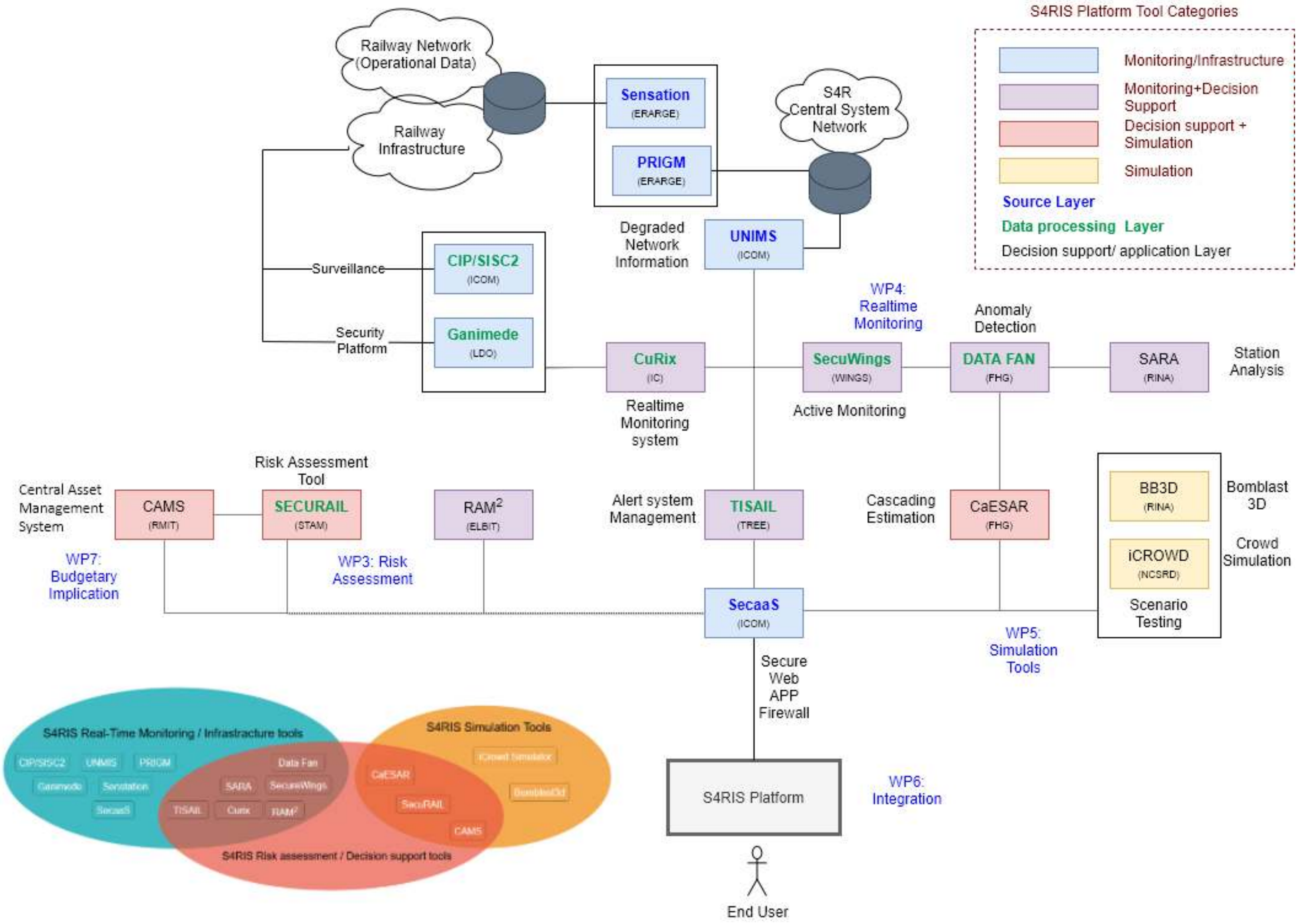


FIGURE 3: SCHEME IDENTIFYING COMPLEXITY OF POSSIBLE COMMUNICATION CONNECTIONS BETWEEN PROVIDED TOOLS AND EXTERNAL SYSTEMS

3.2.1 Overview on the “is” status of the tools foreseen to contribute to the S4RIS platform

In what follows, we provide an overview of the “is” status of each tool foreseen to contribute to the S4RIS platform regarding main functionalities, input and output data and existing interfaces.

The functionalities of the tools describe what the tool brings to the S4RIS, i.e. each tool fulfils one or more functionalities in the proposed system.

The input/output data describe which data is needed to run the tool (input) and what type of result the tool provides (output). Three types of interfaces have been determined and are described:

1. Graphical User Interface (GUI), i.e. either a desktop application or a web application
2. Command Line (CLI), i.e. the input is processed as text in the command line box
3. Application Programming Interface (API), i.e. an interface to receive input from other software systems or to send output (results) to other software systems

As shown in the tables below, the existing interfaces are very heterogenous and need some alignment in terms of operational (i.e. the data exchange and alignment) and technical interoperability. The operational interoperability of the tools will be solved by a JSON interface, where each tool provider defines a JSON structure to receive input from other tools and a JSON structure which provides the output to the S4RIS and other tools. Furthermore, the gathered information serves as basis for a data alignment.

It is foreseen that the technical interoperability of the S4RIS is foreseen to be solved by providing a solution with the help of a Distributed Messaging System (DMS), which is described in D2.3 and D1.4 in more detail and which is foreseen to be implemented in WP6. The DMS combined with the defined

JSON structure will result in a common system, which can be used by each tool provider. Due to this reason, no further information concerning the APIs were gathered.

Tool Name	uniMS: Unified Management Suite
Functionality Number	F-1
Functionality Description	OSS automation platform for the unified management of networks, infrastructure and systems
Set of Requirements	
Operational Requirements (Input/Output)	Input: Integration with network-oriented tools of the railway system
	Output: network management events
Interfaces	APIs (REST/JSON), event import/export possibilities, GUI

Tool Name	Secaas: Security as a Service
Functionality Number	F-2
Functionality Description	Provides cyber-security methods (e.g. VPN, virtual and web-application firewall, network-based intrusion detection) as a service to ensure data privacy following ISO 27001:2013 certification
Set of Requirements	
Operational Requirements (Input/Output)	Input : network and user data from the railway system for the detection of a cyber-threat
	Output : cyber intrusion detection alerts and notifications
Interfaces	APIs (REST/JSON), alert import/export possibilities

Tool Name	CIP/SISC2: CIP & Border Surveillance
Functionality Number	F-3
Functionality Description	Software integration platform for surveillance and physical intrusion detection
Set of Requirements	
Operational Requirements (Input/Output)	Input: Infrastructure surveillance video from sensors or cameras
	Output: physical intrusion detection alerts and notifications
Interfaces	APIs (REST/JSON), alert import/export possibilities, GUI

Tool Name	SARA Securestation Attack Resilience Assessment
Functionality Number	F-6
Functionality Description	Analyse a station and its equipment from a security point of view
Set of Requirements	
Operational Requirements (Input/Output)	Input: description of terminal/underground station places and functional relationships among relevant equipment (xml file)
	Output: svg files. Graphical results then provided in common graphical format
Interfaces	Command line, API

Tool Name	SARA

	Securestation Attack Resilience Assessment
Functionality Number	F-7
Functionality Description	Define and evaluate countermeasures to be applied to the equipment of the station in order to reduce the effects of a terrorist attack, based on the results of the analyses. The effects considered are related to the loss of elements and functioning of different equipment
Set of Requirements	
Operational Requirements (Input/Output)	Input: description of terminal/underground station places and functional relationships among relevant equipment (xml file)
	Output: svg files. Graphical results then provided in common graphical format
Interfaces	Command line, API

Tool Name	SARA Securestation Attack Resilience Assessment
Functionality Number	F-8
Functionality Description	Rank and select possible countermeasures to be applied to the equipment of the station. These activities are performed under constraints that are indicated by the user (e.g., a limited budget, or a determined level of enhancement of the system resilience to be achieved)
Set of Requirements	
Operational Requirements (Input/Output)	Input: description of terminal/underground station places and functional relationships among relevant equipment (xml file)
	Output: svg files. Graphical results then provided in common graphical format
Interfaces	Command line, API

Tool Name	CAMS Central Asset Management System
Functionality Number	F-9
Functionality Description	Provide decision support capabilities for maintenance and rehabilitation activities
Set of Requirements	
Operational Requirements (Input/Output)	Input: user input through web interface, option to upload as an external Excel/csv data upload. Future Dev- API Will be available to be called.
	Output: Excel/csv data export/Reports
Interfaces	GUI

Tool Name	CAMS Central Asset Management System
Functionality Number	F-10
Functionality Description	Probabilistic deterioration predictive model to reflect the stochastic nature of condition degradation to model variety of components of the infrastructure asset

Set of Requirements	
Operational Requirements (Input/Output)	Input: user input through web interface, option to upload as an external Excel/csv data upload. Future Dev- API Will be available to be called.
	Output: Excel/csv data export/Reports
Interfaces	GUI

Tool Name	CAMS Central Asset Management System
Functionality Number	F-11
Functionality Description	Risk and expenditure forecasting based on Markov Chain deterioration prediction
Set of Requirements	
Operational Requirements (Input/Output)	Input: user input through web interface, option to upload as an external Excel/csv data upload. Future Dev- API Will be available to be called.
	Output: Excel/csv data export/Reports
Interfaces	GUI

Tool Name	CuriX Cure Infrastructure in XaaS
Functionality Number	F-12
Functionality Description	Automatic correlation identification of ICT components
Set of Requirements	
Operational Requirements (Input/Output)	Input: any numerical data in a time series
	Output: anomalies detection/deviation/uni-multivariate
Interfaces	GUI- command line - REST - text file as input

Tool Name	CuriX Cure Infrastructure in XaaS
Functionality Number	F-13
Functionality Description	Anomaly detection for the whole IT system based on specific KPIs
Set of Requirements	
Operational Requirements (Input/Output)	Input: any numerical data in a time series
	Output: anomalies detection/deviation/uni-multivariate
Interfaces	GUI- command line - REST - text file as input

Tool Name	CuriX Cure Infrastructure in XaaS
Functionality Number	F-14

Functionality Description	Identification of critical system states for predefined subsystems
Set of Requirements	
Operational Requirements (Input/Output)	Input: any numerical data in a time series
	Output: anomalies detection/deviation/uni-multivariate
Interfaces	GUI- command line - REST - text file as input

Tool Name	CuriX Cure Infrastructure in XaaS
Functionality Number	F-15
Functionality Description	Root cause analysis
Set of Requirements	
Operational Requirements (Input/Output)	Input: any numerical data in a time series
	Output: anomalies detection/deviation/uni-multivariate
Interfaces	GUI- command line - REST - text file as input

Tool Name	DATA FAN
Functionality Number	F-16
Functionality Description	Monitor the active railway system and detect anomalies in the data using machine learning methods
Set of Requirements	
Operational Requirements (Input/Output)	Input: raw data, user data, labelled data (time series data e.g., passengers load/utilization (with the label a) running railway system as well b) during a threat), additional video or image data)
	Output: display (shows the detection of a deviation from the norm and an additional score of the reliability of the detection)
Interfaces	the type of interface is not yet defined, all types are possible (depending on the most benefit for the S4RIS)

Tool Name	DATA FAN
Functionality Number	F-17
Functionality Description	Simulate various what-if scenarios in order to evaluate various scenarios and events, e.g., what is to do if a certain stop cannot be operated due to a cyber or physical threat to avoid panic among the passengers
Set of Requirements	
Operational Requirements (Input/Output)	Input: raw data, user data, labelled data (time series data e.g., passengers load/utilization (with the label a) running railway system as well b) during a threat), additional video or image data)
	Output: display (shows the detection of a deviation from the norm and an additional score of the reliability of the detection)
Interfaces	the type of interface is not yet defined, all types are possible (depending on the most benefit for the S4RIS)

Tool Name	DATA FAN
Functionality Number	F-18
Functionality Description	Results and algorithms reliability assessment
Set of Requirements	
Operational Requirements (Input/Output)	Input: raw data, user data, labelled data (time series data e.g., passengers load/utilization (with the label a) running railway system as well b) during a threat), additional video or image data)
	Output: display (shows the detection of a deviation from the norm and an additional score of the reliability of the detection)
Interfaces	the type of interface is not yet defined, all types are possible (depending on the most benefit for the S4RIS)

Tool Name	PRIGM Hardware Security Module (HSM)
Functionality Number	F-19
Functionality Description	Major cryptography operations such as true random number generation, prime number generation, key generation and management, secure key storage and exchange, symmetric encryption ((AES, 3DES), asymmetric encryption (RSA, ECDSA), and hashing (SHA)
Set of Requirements	
Operational Requirements (Input/Output)	Input: 1-Data that requires encryption/decryption. 2-Authentication tokens
	Output: Raw data like Encryption Keys. Encrypted data. Hashes. Etc
Interfaces	Cryptoki APİ (PKCS #11)

Tool Name	PRIGM Hardware Security Module (HSM)
Functionality Number	F-20
Functionality Description	Tamper-proof enclosure
Set of Requirements	
Operational Requirements (Input/Output)	Input: 1-Data that requires encryption/decryption. 2-Authentication tokens
	Output: Raw data like Encryption Keys. Encrypted data. Hashes. Etc
Interfaces	Cryptoki APİ (PKCS #11)

Tool Name	SenStation Secure sensor station and secure gateway
Functionality Number	F-21
Functionality Description	Combination of secure gateway and sensor interfaces to provide secure data transmission between railway physical and cyber infrastructure. P2P security against any cyber physical attacks
Set of Requirements	
	Input: 1-Sensory data coming from sensors

Operational Requirements (Input/Output)	2-TBD: Data from IoT nodes connected with the railway digital system which are compatible with the supported protocols
	Output: 1-JSON 2-TBD: Raw data like Encrypted data. Hashes. Etc
Interfaces	TCP/IP based API

Tool Name	SenStation Secure sensor station and secure gateway
Functionality Number	F-22
Functionality Description	Synergy with PRIGM tool to update the required one-time passwords and any other secrets
Set of Requirements	
Operational Requirements (Input/Output)	Input: 1-Sensory data coming from sensors 2-TBD: Data from IoT nodes connected with the railway digital system which are compatible with the supported protocols
	Output: 1-JSON 2-TBD: Raw data like Encrypted data. Hashes. Etc
Interfaces	TCP/IP based API

Tool Name	CaESAR Cascading effect simulation to assess and increase resilience
Functionality Number	F-23
Functionality Description	Cascading effects simulation within and across grid borders to assess and enhance the resilience of critical infrastructures in urban areas
Set of Requirements	
Operational Requirements (Input/Output)	Input: description of the modelled grids as text file
	Output: resilience curves, box plot graphs, damage propagation paths
Interfaces	connection with other devices, APIs (REST/JSON), common databases, import/export possibilities GUI, command line

Tool Name	CaESAR Cascading effect simulation to assess and increase resilience
Functionality Number	F-24
Functionality Description	Provide optimized strategies for the mitigation of hazard impact on inter-connected grids.
Set of Requirements	
Operational Requirements (Input/Output)	Input: description of the modelled grids as text file
	Output: resilience curves, box plot graphs, damage propagation paths
Interfaces	connection with other devices, APIs (REST/JSON), common databases, import/export possibilities GUI, command line

Tool Name	Ganimede

Functionality Number	F-25
Functionality Description	Large-scale analysis of live and recorded data streams (audio and video) based on Deep Learning for threat detection
Set of Requirements	
Operational Requirements (Input/Output)	Input: CCTV data
	Output: metadata and processed data as RTSP stream
Interfaces	GUI , REST API

Tool Name	Ganimede
Functionality Number	F-26
Functionality Description	Large-scale analysis of live and recorded data streams (audio and video) based on Deep Learning for threat detection
Set of Requirements	
Operational Requirements (Input/Output)	Input: CCTV data
	Output: metadata and processed data as RTSP stream
Interfaces	GUI , REST API

Tool Name	TISAIL (RAMSES) Threat Intelligence
Functionality Number	F-27
Functionality Description	Crawlers from different sources (social media, darknet, forums)
Set of Requirements	
Operational Requirements (Input/Output)	Input: API, RSS feeds, web scraping
	Output: JSON
Interfaces	API

Tool Name	TISAIL (RAMSES) Threat Intelligence
Functionality Number	F-28
Functionality Description	Identification of vulnerable nodes that suffer cybersecurity attacks
Set of Requirements	
Operational Requirements (Input/Output)	Input: API, RSS feeds, web scraping
	Output: JSON
Interfaces	API

Tool Name	TISAIL (RAMSES) Threat Intelligence

Functionality Number	F-29
Functionality Description	Evaluation/ranking vulnerability
Set of Requirements	
Operational Requirements (Input/Output)	Input: API, RSS feeds, web scraping
	Output: JSON
Interfaces	API

Tool Name	TISAIL (RAMSES) Threat Intelligence
Functionality Number	F-30
Functionality Description	Risk analysis
Set of Requirements	
Operational Requirements (Input/Output)	Input: API, RSS feeds, web scraping
	Output: JSON
Interfaces	API

Tool Name	SECURAIL SECUrity Risk Analysis of raILways infrastructures
Functionality Number	F-31
Functionality Description	Hybrid quantitative/qualitative Risk Analysis of Railway infrastructures and systems
Set of Requirements	
Operational Requirements (Input/Output)	input from user through UI input from surveillance systems for real-time risk-analysis through JSON messages, HTTP requests or other protocols (to be discussed)
	output visualised in the dashboard of the tool possibility to export output as excel file
Interfaces	Web-application with its own GUI

Tool Name	SECURAIL SECUrity Risk Analysis of raILways infrastructures
Functionality Number	F-32
Functionality Description	Infrastructure/system can be modelled by the user
Set of Requirements	
Operational Requirements (Input/Output)	input from user through UI input from surveillance systems for real-time risk-analysis through JSON messages, HTTP requests or other protocols (to be discussed)

	output visualised in the dashboard of the tool possibility to export output as excel file
Interfaces	Web-application with its own GUI

Tool Name	SECURAIL SECUrity Risk Analysis of raILways infrastructures
Functionality Number	F-33
Functionality Description	Generate thousands of attack scenarios
Set of Requirements	
Operational Requirements (Input/Output)	input from user through UI input from surveillance systems for real-time risk-analysis through JSON messages, HTTP requests or other protocols (to be discussed)
	output visualised in the dashboard of the tool possibility to export output as excel file
Interfaces	Web-application with its own GUI

Tool Name	SECURAIL SECUrity Risk Analysis of raILways infrastructures
Functionality Number	F-34
Functionality Description	Simulate evolution of the scenario to understand the set of possible outcomes and compute the related impact, likelihood and risk
Set of Requirements	
Operational Requirements (Input/Output)	input from user through UI input from surveillance systems for real-time risk-analysis through JSON messages, HTTP requests or other protocols (to be discussed)
	output visualised in the dashboard of the tool possibility to export output as excel file
Interfaces	Web-application with its own GUI

Tool Name	BB3D BomBlast3d
Functionality Number	F-35
Functionality Description	Fast calculation of the distribution of main blast wave parameters around and over three-dimensional complex geometries
Set of Requirements	
Operational Requirements (Input/Output)	Input: '3D modelling of infrastructure and surface mesh according to STL format (ASCII and free) model, parameters
	Output: 'Output files: VTK paraview files (ASCII free format) that can be visualised through the open-source software Paraview (https://www.paraview.org/)
Interfaces	Executables running in serial man+M16+M17

Tool Name	BB3D BomBlast3d
Functionality Number	F-36
Functionality Description	Reproduce and analyse bomb explosion consequences to identify potential attractive targets for terrorists
Set of Requirements	
Operational Requirements (Input/Output)	Input: '3D modelling of infrastructure and surface mesh according to STL format (ASCII and free) model, parameters
	Output: 'Output files: VTK paraview files (ASCII free format) that can be visualised through the open-source software Paraview (https://www.paraview.org/)
Interfaces	Executables running in serial man+M16+M17

Tool Name	SECUREWINGS - Big Data and Predictive Analytics Tool
Functionality Number	F-37
Functionality Description	Devices/sensors/actuators, e.g., for air quality, parking availability, health monitoring and many more, as well as device management functionality (activation, cessation, upgrades)
Set of Requirements	
Operational Requirements (Input/Output)	Input: Sensor data and API
	Output: JSON, csv
Interfaces	GUI and command-line

Tool Name	SECUREWINGS - Big Data and Predictive Analytics Tool
Functionality Number	F-38
Functionality Description	Data management functionality (cleansing, imputation, etc.)
Set of Requirements	
Operational Requirements (Input/Output)	Input: Sensor data and API
	Output: JSON, csv
Interfaces	GUI and command-line

Tool Name	SECUREWINGS - Big Data and Predictive Analytics Tool
Functionality Number	F-39
Functionality Description	Artificial intelligence mechanisms (supervised and unsupervised, deep learning, starting from Bayesian statistics, timeseries forecasting, self-organising maps and reaching up to more modern techniques like LSTM) for generating insights and predictions/forecasts and for supporting and conducting decision making

Set of Requirements	
Operational Requirements (Input/Output)	Input: Sensor data and API
	Output: JSON, csv
Interfaces	GUI and command-line

Tool Name	SECUREWINGS - Big Data and Predictive Analytics Tool
Functionality Number	F-40
Functionality Description	Dashboards and applications for visualisation
Set of Requirements	
Operational Requirements (Input/Output)	Input: Sensor data and API
	Output: JSON, csv
Interfaces	GUI and command-line

Tool Name	iCrowd Simulator
Functionality Number	F-41
Functionality Description	Simulate physically independent locations like train and metro stations
Set of Requirements	
Operational Requirements (Input/Output)	Input: 3D model of the infrastructure (.obj) Passenger flow data Monitoring Assets ontology Railway service time plan and processes specification Attack scenarios Evacuation plans and other threat mitigation strategies
	Output: total evacuation time, the average response time, infrastructure and strategies resilience analysis data can be exported in JSON or other formats
Interfaces	GUI

Tool Name	iCrowd Simulator
Functionality Number	F-42
Functionality Description	Abstraction of operating network
Set of Requirements	
Operational Requirements (Input/Output)	Input: 3D model of the infrastructure (.obj) Passenger flow data Monitoring Assets ontology Railway service time plan and processes specification Attack scenarios Evacuation plans and other threat mitigation strategies
	Output: total evacuation time, the average response time, infrastructure and strategies resilience analysis data can be exported in JSON or other formats

Interfaces	GUI

Tool Name	iCrowd Simulator
Functionality Number	F-43
Functionality Description	Define simulation scenarios run by a sophisticated crowd engine with collision avoidance with multiple, different behaviours that can coexist inside the same simulation
Set of Requirements	
Operational Requirements (Input/Output)	Input: 3D model of the infrastructure (.obj) Passenger flow data Monitoring Assets ontology Railway service time plan and processes specification Attack scenarios Evacuation plans and other threat mitigation strategies
	Output: total evacuation time, the average response time, infrastructure and strategies resilience analysis data can be exported in JSON or other formats
Interfaces	GUI

Tool Name	RAM2 DSS (Decision Support System)
Functionality Number	F-44
Functionality Description	Risk prioritization according to operational and busines impact, likelihood and severity
Set of Requirements	
Operational Requirements (Input/Output)	Input: Syslogs, REST API, CSVs, Industrial Project Files, network PCAPs
	Output: assets, alerts and insights using API calls and Syslogs, as well as via PDF and CSV files
Interfaces	Web-based GUI

Tool Name	RAM2 DSS (Decision Support System)
Functionality Number	F-45
Functionality Description	Support multi-site configuration to specifically support multi-site continuous compliance and policy governance
Set of Requirements	
Operational Requirements (Input/Output)	Input: Syslogs, REST API, CSVs, Industrial Project Files, network PCAPs
	Output: assets, alerts and insights using API calls and Syslogs, as well as via PDF and CSV files
Interfaces	Web-based GUI

Tool Name	RAM2 DSS (Decision Support System)

Functionality Number	F-46
Functionality Description	Cyber-physical risk assessment, monitoring and management, detecting gaps and exposures before they become a breach
Set of Requirements	
Operational Requirements (Input/Output)	Input: Syslogs, REST API, CSVs, Industrial Project Files, network PCAPs
	Output: assets, alerts and insights using API calls and Syslogs, as well as via PDF and CSV files
Interfaces	Web-based GUI

Tool Name	RAM2 DSS (Decision Support System
Functionality Number	F-47
Functionality Description	Integration with all IT, OT & IOT assets and systems
Set of Requirements	
Operational Requirements (Input/Output)	Input: Syslogs, REST API, CSVs, Industrial Project Files, network PCAPs
	Output: assets, alerts and insights using API calls and Syslogs, as well as via PDF and CSV files
Interfaces	Web-based GUI

Tool Name	WiBAS
Functionality Number	F-48
Functionality Description	Broadband radio access solution for providing rail network connectivity
Set of Requirements	
Operational Requirements (Input/Output)	Input: Integration in the railway network
	Output: wireless network traffic measurements
Interfaces	uniMS, GUI

3.2.2 Operational interoperability to internal and external systems and technical interoperability

In SAFETY4RAILS, the interoperability also defines a concept for integration in / to existing external systems. Based on workshops with end-users, the integration in external systems was evaluated. Referring to those workshops, the systems operated by the end-users are heterogeneous. Hence, a flexible integration of the S4RIS is necessary to cover all the possibilities. To realise a feasible integration, two approaches were identified: a loose coupling of the S4RIS and an integration of external systems to the S4RIS.

A loose coupling means that the S4RIS does not interact automatically (i.e., without user interaction) with the end-users' systems. This loose coupling can be realized by providing the possibility to import data in the S4RIS mainly manually through the provided GUI, e.g., by an upload button in the S4RIS GUI. For this option, the data input format to be uploaded into the S4RIS and some parsers to read already existing input file formats from end-users' tools must be defined.

The real integration of external tools in the S4RIS can be realized by a Distributed Messaging System (DMS). This means that an external tool would connect to the S4RIS DMS and post data (i.e., push data) to a defined "topic" in the DMS. Another possibility is to connect a member tool of the S4RIS to external tools. The S4RIS tool would receive data and push them to the DMS as a "topic" (i.e., a S4RIS member tool works similarly to a proxy). This mechanism is also planned to be used for the internal interoperability of the S4RIS components (developed in WP6). With this approach, a flexible integration of very heterogenous external systems can be ensured.

If neither a loose coupling nor an integration of external systems in the DMS is feasible during the project, the S4RIS could also work with synthetic data to be uploaded. This is an option to be considered during the project, particularly for the development and possibly pilots.

These options are also described in the requirement tables below.

Req.-ID	*IO-1*
Short name	Data exchange – Between S4RIS tools
Description	The S4RIS platform shall provide a solution(s) whereby contributory tools which need a direct link for a combination of processing can share relevant data.
Priority	*Essential*
Comment	-

Req.-ID	*IO-2*
Short name	Synchronisation
Description	The S4RIS platform shall provide a solution to synchronise the timing of contributory data sources and tools.
Priority	*Essential*
Comment	-

Req.-ID	*IO-3*
Short name	Data exchange with end-users' system
Description	The S4RIS shall provide a solution to connect heterogenous systems at end-users' side without intervention in existing systems
Priority	*Essential*
Comment	Provide a possibility to integrate the S4RIS in existing systems, where data can be uploaded and downloaded by an interface (not GUI). Update February 2022: For clarity, existing systems include multiple access control and intrusion detection subsystems from diverse vendors, including legacy devices and sensors with proprietary protocols/interfaces, plus the novel IoT ones. In the deliverable D1.4 *Specification of the overall technical architecture* (October 2021) this is the "S4RIS platform specific" requirement P-21 (page 25). Its specification is the same as for the requirement P-07 "Data exchange - S4RIS to end-users" in which it is stated (page 19): *"…….In the productive version after the project, with respect to the individual circumstances at end-users infrastructure, data exchange to end-user systems can be addressed over direct communications to APIs or by providing access to S4RIS DMS."*

	Presently, REST APIs would be expected. The D1.4 also includes the further relevant requirement (also on page 19) P-06 “Data exchange – end user sources to S4RIS”: “*The S4RIS platform shall provide a solution(s) whereby physical and cyber sensor data can be communicated from end-users to the S4RIS platform*“. Here the specification includes: *“The real-time monitoring tools (e.g. CuriX, DATA FAN, WINGSPARK) will provide means to observe current values of measured data of physical and cyber sensors within dedicated dashboards. See requirements for the tool CuriX, DATA FAN and WINGSPARK.* *For the productive version, the real-time monitoring tools will be connected via appropriate / proprietary interfaces to data sources (e.g. CuriX will collect relevant data from classical IT-monitoring tools like elastic or PRTG which provide also means to collect SCADA data) in an end-user specific way, i.e. customized connections, because each possible end-user will provide data in a different way…”*

Req.-ID	*IO-4*
Short name	Data exchange – Upload already existing data in the S4RIS
Description	The S4RIS shall provide a possibility to upload existing data based on existing data formats in the S4RIS for the end-user mainly manually
Priority	*Essential*
Comment	Provide a possibility to import data in the S4RIS mainly manually with the provided GUI, e.g. by an upload button in the S4RIS GUI Update February 2022: See IO-3 regarding data from other existing systems.

Req.-ID	*IO-5*
Short name	Data exchange format for the S4RIS
Description	The S4RIS shall provide a data format, where it is indicated which data is optional to use the S4RIS or parts of it and which data is mandatory
Priority	*Essential*
Comment	-

Req.-ID	*IO-6*
Short name	The S4RIS shall provide a possibility to connect to not specified systems
Description	The S4RIS should provide a flexible and generic interface to connect the S4RIS to heterogenous systems, which are not specified at the moment.
Priority	*Essential*
Comment	-

4. Graphical User Interface requirements

4.1 Introduction

S4RIS will enable the end-users to access and use a wide range of tools that will be integrated (where operationally relevant). An important part of S4RIS is the Graphical User Interface (GUI), that the end-users' operators will use to access the tools and to operate the platform. The tools to be integrated in S4RIS are characterized by different types of human-machine interface: some of them have web-based GUIs, accessible through browsers, others are desktop-based applications with their own GUI interface, and for some others their situated use-scenarios do not involve direct human interaction so that the need for a GUI would not arise..

The primary objective of S4RIS GUI is to provide a common access to all the tools and to assist the operators in daily operations. The requirements defined in this section are aimed to drive GUI development, that will be carried out in Work Package 6, T6.2, considering end-user friendly ergonomics to increase S4RIS GUI usability.

The Graphical User Interface requirements section is organised as follows:

- Section 4.1.1 illustrates some of the most commonly adopted GUI design principles.
- Section 4.1.2 describes the methodology followed for defining the GUI requirements.
- Section 4.1.3 reports an assessment on GUIs currently available for each tool to be integrated in S4RIS.
- Section 4.2.1 reports the GUI requirements.
- Section 4.2.2 reports the defined user stories.
- Section 4.2.3 reports a set of examples of the main S4RIS GUI pages.

4.1.1 Principles for GUI design

Graphical User Interface design focuses on anticipating what users might need to do and ensuring that the interface has elements that are easy to access, understand, and use to facilitate those actions. The Jakob Nielsen's general principles for interaction design are some of the most used principles for GUI design. They are called "usability heuristics" or "Nielsen heuristics" because they are broad rules, applicable to any kind of GUI. Nielsen developed the heuristics based on work together with Rolf Molich in 1990.The final set of heuristics that are still used today were released by Nielsen in 1994 (Ref. [43], Ref. [44]). The ten principles are as follows:

#1. **Visibility of system status:** the design should always keep users informed about what is going on, through appropriate feedback within a reasonable amount of time. When users know the current system status, they learn the outcome of their prior interactions and determine next steps.

#2. **Match between system and the real world:** the design should speak the users' language. Use words, phrases, and concepts familiar to the user, rather than internal jargon. Follow real-world conventions, making information appear in a natural and logical order. Terms, concepts, icons, and images that seem perfectly clear to you and your colleagues may be unfamiliar or confusing to your users.

#3. **User control and freedom:** users often perform actions by mistake. They need a clearly marked "emergency exit" to leave the unwanted action without having to go through an extended process.

#4. **Consistency and standards:** users should not have to wonder whether different words, situations, or actions mean the same thing. Follow platform and industry conventions.

#5. **Error prevention:** good error messages are important, but the best designs carefully prevent problems from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.

#6. **Recognition rather than recall:** Minimise the user's memory load by making elements, actions, and options visible. The user should not have to remember information from one part of the interface to another. Information required to use the design (e.g., field labels or menu items) should be visible or easily retrievable when needed.

#7. **Flexibility and efficiency of use: s**hortcuts — hidden from novice users — may speed up the interaction for the expert user such that the design can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.

#8. **Aesthetic and minimalist design:** interfaces should not contain information which is irrelevant or rarely needed. Every extra unit of information in an interface competes with the relevant units of information and diminishes their relative visibility.

#9. **Help users recognize, diagnose, and recover from errors:** error messages should be expressed in plain language (no error codes), precisely indicate the problem, and constructively suggest a solution.

#10. **Help and documentation:** it is best if the system does not need any additional explanation. However, it may be necessary to provide documentation to help users understand how to complete their tasks. Help and documentation content should be easy to search and focused on the user's task. Keep it concise, and list concrete steps that need to be carried out.

These principles should be considered both for the definition of GUI requirements and for its development.

4.1.2 Methodology adopted

This section describes the methodology adopted for the definition of the S4RIS GUI requirements.

The first step for this purpose consisted in collecting and analysing the Tools Providers questionnaires, managed by IC/Fraunhofer at project level, to extract information related to the existing GUI of the tools to be integrated with S4RIS platform.

Based on this analysis, further questionnaires have been prepared within T2.4 and filled-in by the Tool Providers, to have a more comprehensive view on the initial state of the user interface of each tool. The main information to be collected was:

- Type of User Interface (Graphical User Interface, Command Line Interface, other types of interface).
- Type of application (web-based user interface, desktop or mobile interface, etc.).
- Availability of a dashboard.
- User Interface improvements planned in the project.

In parallel, the End-Users questionnaires have been collected and analysed in order to identify end-users' requirements related to GUI, with a focus on three initial aspects:

1) End-users' preference between a single display or a display by main functionality areas of S4RIS
2) The language preference for S4RIS testing later on in the project
3) End-users' preferences when it comes to format of S4RIS results.

Results collected enable to derive the following initial trends:

- An equal share feedback between the willing to gather the entire spectrum of main functionality areas of S4RIS and the need to enable a separation between the main action areas covered by S4RIS. One end-user interestingly highlighted that the separation by main functionality area could be useful, considering that several different units and departments of railways and metro compagnies will use S4RIS.
- Almost all end-users stated that national language would be the best option when it comes to language to be used during S4RIS testing, in order to simplify procedures and improve effectiveness of these tests.
- When it comes to S4RIS results formats, all end-users' answers mentioned dashboard, as a best option or one among others. Yet an end-user also highlights the possibility to adapt S4RIS results format depending on the user profile.

The set of GUI requirements has been subsequently defined, taking into consideration all the information mentioned above. Then, based on the requirements, a set of user stories has been defined, describing the main actions that operators may perform with the software and being an aid to GUI implementation and validation.

Finally, a set of pictures providing examples to be used as a guideline for the development of the GUI interface has been elaborated.

The requirements and the GUI pages examples have been improved and validated during the second end-users' workshop, during a dedicated session on GUI requirements held on 9th March 2021. This end-users' workshop session provided the below key elements:

- Useful feedbacks regarding several aspects of the GUI, including:
  - Displaying of tools in several areas;
  - Displaying of tools based on the role of the operator;
  - Management of tools having no graphical user interface;
  - Access to additional functionalities (such as settings, help, etc.).
- Ranking of GUI requirements, that allowed to confirm or modify the priority rank of several requirements, based on end-users' perspective. The ranks reported in section 4.2.1 reflect the outcome of this activity.

4.1.3 Assessment of the existing GUIs of the tools

In this section, an assessment on the state-of-art regarding GUI of the tools to be integrated in S4RIS is reported. The information reported have been primarily collected through Tool Providers questionnaires and then using additional assessment templates prepared within T2.4 and filled-in by tool providers. The major conclusion that emerges from the analysis of the provided information is the lack of harmonisation regarding the GUI of the tools. Some tools have web-based GUIs, accessible from browsers and sometime from mobiles, some have desktop-based GUIs, while some others have no GUI at all and can be used only through Command Line Interface. Furthermore, each tool is characterized by different graphical appearance.

Figure 4 depicts the types of interfaces actually available in the existing tools. The majority of tools (8) adopt a web-based interface; 4 tools have desktop interfaces, i.e., they are executed as desktop applications with their own graphical user interface; 4 tools have only a command line interface, i.e., they must be executed using a command prompt; finally, 2 tools have no user interface at all and are accessible only through APIs.

Table 5 reports the more relevant collected information and provides an overview of the initial status of the GUI of each tool.

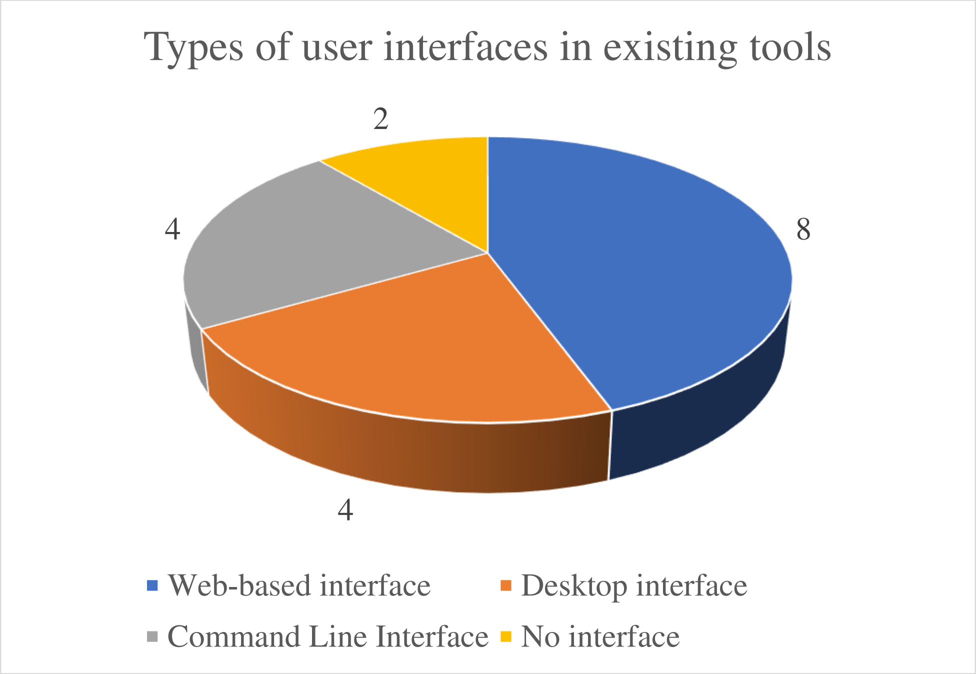


FIGURE 4: TYPES OF INTERFACES IN EXISTING TOOLS

TABLE 5: CHARACTERISTIC OF EXISTING TOOLS

Tool	Partner	Type of User Interface (Yes/No)			Development platform	Type of application		Dashboard (Yes/No)	Other noteworthy features	GUI upgrade currently foreseen
		Command Line Interfaces (CLI)	Text User Interface (TUI)	Graphical User Interfaces (GUI)		Native	Web-based			
-	-	*Only a command line and a prompt*	*TUI between CLI and GUI*	*Usable through operating elements and symbols*	-	*Tool accessible via desktop or mobile application, or another platform*	*Tool accessible / usable via web*	*If the tool has a dashboard*	*List features of your tool that you consider important to the scope of the project from GUI point of view*	*Tool GUI upgrade in S4RIS?*
UMIS	ICOM	No	No	Yes	Linux	Yes, desktop (management console)	No	No	-	No
SecaaS	ICOM	Yes	No	No	Linux	Yes, desktop (management console)	No	No	-	TBC if web-based access will be provided
CIP/SISC2	ICOM	No	No	Yes	Windows/Linux	Yes, desktop (management console)	No	No	-	No
WiBAS	ICOM	No	No	Yes	HW/embedded No (hardware /embedded)	-	No	No		No
SARA	RINA	Yes	No	No	Visual basic, Open SW	Yes, desktop (VM)	No	No	-	Yes, from CLI to GUI
CAMS	RMIT	No	No	Yes	C# (dot net core version 2.1) - Web API, Angular - front end 7.2.6, MongoDB - database 4.4.4	Mobile application (iOS)	Yes	Yes	A mobile application is also available to assign condition data of assets.	No
CuriX	IC	Not only CLI	Yes	Yes	Java, React, JS, (+ Web-Languages)	no	Yes	Yes	REST API, Cloud Service could be provided	Yes
DATA FAN	FHG	No	No	Yes	Python, Pycharm	Yes, desktop application	No	No	-	Yes
PRIGM	ERARGE	No	No	No	Linux	No	No	No	-	No
SenStation	ERARGE	No	No	Yes	Arm IDE	No	Yes	No	Display of sensory data and device settings	No

Tool	Partner	Type of User Interface (Yes/No)			Development platform	Type of application		Dashboard (Yes/No)	Other noteworthy features	GUI upgrade currently foreseen
		Command Line Interfaces (CLI)	Text User Interface (TUI)	Graphical User Interfaces (GUI)		Native	Web-based			
CaESAR	FHG	Yes	No	No	C++	No	No	No	-	Yes
Ganimede	LDO	No	No	Yes	React, Flash	No	Yes	Yes	Voice User Interface (VUI) available. Asynchronous event generation according to the match of specific patterns.	No
TISAIL (RAMSES)	TREE	No	Yes (sends alerts via API)	No	Based on open source project MISP (PHP) with some developments in Python	No	No	No	This tool will provide alerts that can be incorporated in other solutions (Decision Support System, - T5.5), but it does not provide interfaces for the user	No
SECURAIL	STAM	No	No	Yes	Angular	No	Yes	Yes	-	No
BB3D	RINA	Yes	No	No	gcc (FORTRAN)	Yes (currently mainly on Linux)	No	No	Results can be viewed with Paraview (https://www.paraview.org/) that also has a version for the web (https://www.paraview.org/web/)	Possible
SECUREWINGS	WINGS	No	No	Yes	Angular	No	Yes	Yes	-	Upgrades will be done in order to show specific aspects of safety in rail infrastructure
iCrowd Simulator	NCRSD	No	No	Yes	C++	Yes, desktop application	No	No	Crowd flow metrics diagrams	No
RAM2	ELBIT	No	No	Yes	Python, React	No	Yes	Yes	- No	

4.2 GUI definition

4.2.1 GUI requirements list

This section reports the list of S4RIS Graphical User Interface requirements that has been defined.

Requirement ID	GUI-R01
Short name	Web-based interface
Key objectives	- to allow easy access to S4RIS
Priority rank	Essential
Description	S4RIS shall have a web-based interface.
Comments	This simplifies the access to the system and avoid installation issues.

Requirement ID	GUI-R02
Short name	Login page
Key objectives	- to define log-in window
Priority rank	Essential
Description	When S4RIS interface is opened and the user is not already logged-in, only a log-in page shall be displayed. This page shall be coherent with the authentication method adopted for S4RIS.
Comments	For example, if the authentication will be based on username-password only, the username-password fields shall be displayed to the user. If two-factor authentication will be implemented with OTP code (or similar), a page to insert the OTP code (or similar) shall be displayed after the insertion of username-password.

Requirement ID	GUI-R03
Short name	Single point of access to the tools
Key objectives	- to have all tools available for use in a single page
Priority rank	Essential
Description	It shall be possible to launch the tools that need user interaction from a single interface (the home page).
Comments	The entry point to all tools shall be unique to have a complete overview on the available tools.

Requirement ID	GUI-R04
Short name	Grouping of tools
Key objectives	- to group tools based on their area of use
Priority rank	Essential
Description	The tools shall be visually grouped into at least four areas: risk assessment, prevention and mitigation, detection and response, planning and investments.
Comments	This requirement ensures that tools related to an area of use are visually grouped together. This allows the operator to focus more easily on its current task (e.g., when an operator needs to use the "detection" capabilities of S4RIS, all tools related to this capability will be shown grouped and therefore it will be easier for him to focus on these tools).

	Other orders of displaying the tools (e.g., all the tools simply in alphabetic order) are considered less user-friendly and more confuse. Additional areas could be present if needed.

Requirement ID	GUI-R05
Short name	How to launch tools
Key objectives	- to define how each tool will be accessed by the operator
Priority rank	Essential
Description	To launch each tool, an icon button shall be used. The icon button shall include: - the name or acronym of the tool, and; - the icon of the tool. If the tool does not come with an icon from the tool provider, another icon could be defined.
Comments	This requirement ensures that it is easy for the operator to identify the different tools.

Requirement ID	GUI-R06
Short name	Display of tools based on user role
Key objectives	- to guarantee that only authorized users can launch the tools
Priority rank	Essential
Description	The tools shall be displayed on a role-based criterion, so that only authorized users can launch the tools.
Comments	This requirement ensures that only authorized users can launch the tools. For example, an operator dealing with "detection" could be not authorized to access tools dealing with "recovery". In this case, only tools related to "detection" should be shown and clickable by the operator" Note: defining the criteria for granting access to the operators to the tools is out of scope.

Requirement ID	GUI-R07
Short name	Tools keywords and short descriptions
Key objectives	- to help users to easily understand what a tool is used for
Priority rank	Essential
Description	A set of keywords and/or a short description, aimed to describe the tool main functionalities, shall be displayed for each tool.
Comments	Due to large number of tools included in S4RIS, it seems reasonable that for each tool a short description and/or keywords are shown to help the operator to understand what the tools do. Keywords should be provided by the tool providers. Note: other implementations are allowed. Proposed implementation: - near the icon button to launch the tool, a text box with the keywords is displayed; - when the cursor hovers over the icon button to launch the tool and/or the keywords, a tooltip is shown with the short description.

Requirement ID	GUI-R08
Short name	Log-out button
Key objectives	- to defined log-out position
Priority rank	Essential
Description	A log-out button shall be present in the right-top angle of each page (login page is excluded).
Comments	-

Requirement ID	GUI-R09
Short name	Home page button
Key objectives	- to define position of home page button
Priority rank	Conditional
Description	S4RIS logo shall be displayed in the left-top angle of each page and shall work as a "home" button (login page is excluded).
Comments	-

Requirement ID	GUI-R10
Short name	Account management
Key objectives	- to allow the user to manage its account and change its own password
Priority rank	Essential
Description	It shall be possible for the user to manage its account and change its password in a dedicated page, accessible from the home page.
Comments	-

Requirement ID	GUI-R11
Short name	Settings and configuration
Key objectives	- to allow editing of setting and configuration
Priority rank	Essential
Description	If settings will be present for S4RIS, it shall be possible for the user to change settings in a dedicated page, accessible from the home page.
Comments	This requirement shall be implemented only if the users can modify any setting.

Requirement ID	GUI-R12
Short name	Language
Key objectives	- to allow changing of the displayed language
Priority rank	Essential
Description	It shall be possible to change the displayed language. At least the following languages should be supported: - English; - Italian; - Spanish; - Dutch;

	- Turkish.
Comments	Proposed alternative implementations: - change language in a dedicated page accessible from home page; - change language in the setting page, if present; - change language using a drop-down menu in the home page. Note: other implementations are allowed.

Requirement ID	GUI-R13
Short name	Bar with additional functions
Key objectives	- to quickly and easily find additional S4RIS functions and menus.
Priority rank	Conditional
Description	A side-bar (preferred) or a top-bar should be present in the home page and should provide buttons to access the followings: - password management (GUI-R10); - settings and configuration (GUI-R11), if implemented; - language selection (GUI-R12); - help, if implemented (GUI-R21).
Comments	Allowing the user to choose between side-bar or top-bar would be a plus.

Requirement ID	GUI-R14
Short name	Opening web-based tools
Key objectives	- to define how to open tools with web-based interface
Priority rank	Essential
Description	When tools with web-based GUI are launched, they shall be opened in another tab or window of the browser.
Comments	-

Requirement ID	GUI-R15
Short name	Opening desktop tools
Key objectives	- to define how to open tools with desktop application
Priority rank	Essential
Description	When tools with desktop application are launched, the desktop application itself shall be launched.
Comments	-

Requirement ID	GUI-R16
Short name	Opening CLI tools
Key objectives	- to define how to open tools with Command Line Interface only
Priority rank	Conditional
Description	When tools with Command Line Interface only are launched, one (or more) page(s) specific for dealing with that tool should be opened.
Comments	-

Requirement ID	GUI-R16a

Short name	Opening CLI tools - BB3D
Key objectives	- to define how to deal with BB3D
Priority rank	Conditional
Description	When BB3D icon button is pressed, the following features should be displayed (in one or more pages): 1) area for functionalities and parameters' value assignment 2) area for solution progress / warning / errors monitoring 3) area for 3d plot and ASCII results files visualization
Comments	This requirement provides information on how to manage BB3D tool, that does not have a GUI. Guidelines: 1) the first area will allow the user to create/edit input file(s) and to set parameters; 2) the second area will show the solution progress (e.g., with progress bar) and will display warnings and errors; 3) the third area will allow to show 3D plots and ASCII results (maybe using external viewer)

Requirement ID	GUI-R16b
Short name	Opening CLI tools - CaESAR
Key objectives	- to define how to deal with CaESAR
Priority rank	Conditional
Description	When CaESAR icon button is pressed, the following features should be displayed (in one or more pages): 1) area for creation/selection/editing of input file(s) and parameters 2) area for launching and monitoring the processing / showing warnings and errors 3) area to view the generated outputs and open already generated results
Comments	This requirement provides information on how to manage CaESAR tool, that does not have a GUI. Guidelines: 1) the first area will allow the user to create/edit input file(s) and to set parameters; 2) the second area will show the processing progress (e.g., with progress bar) and will display warnings and errors; 3) the third area (or page) will allow to show the generated plots and outputs

Requirement ID	GUI-R16c
Short name	Opening CLI tools - SARA
Key objectives	- to define how to deal with SARA
Priority rank	Conditional
Description	When SARA icon button is pressed, the following features should be displayed (in one or more pages): 1) area for creation/selection/editing of input file(s) and parameters 2) area for launching and monitoring the processing / showing warnings and errors

	3) area to view the generated outputs and open already generated results
Comments	This requirement provides information on how to manage CaESAR tool, that does not have a GUI. Guidelines: 1) the first area will allow the user to create/edit input file(s) and to set parameters; 2) the second area will show the processing progress (e.g., with progress bar) and will display warnings and errors; 3) the third area (or page) will allow to show the generated plots and outputs

Requirement ID	GUI-R17
Short name	User confirmation on certain actions
Key objectives	- to let the user correct some unwanted actions
Priority rank	Essential
Description	When the button to launch a tool or the log-out button are pressed, a confirmation pop-up shall be displayed to let the user confirm or cancel the action.
Comments	This requirement allow the user to cancel actions when a button is pressed by error

Requirement ID	GUI-R18
Short name	Font type and size
Key objectives	- to ensure readability
Priority rank	Conditional
Description	The used font shall be clearly readable (e.g., Arial, Helvetica, Calibri, etc.). The font size shall never be smaller than 12pt.
Comments	This requirement ensure that used font is readable and not too small.

Requirement ID	GUI-R19
Short name	Error display
Key objectives	- to inform the user of errors
Priority rank	Essential
Description	When an error occurs, a pop-up to inform the user shall be displayed.
Comments	The pop-up should contain a description of the error, not only a code.

Requirement ID	GUI-R20
Short name	S4RIS account creation
Key objectives	- to allow operators to request the creation of an account
Priority rank	Optional
Description	A button to request the creation a new account could be present in the login page. Pressing this button, a form should be displayed to collect user information (such as name, surname, email, ID, qualification, etc.). Then, the user should be able to cancel the process or to submit the form for the creation of the account.

Comments	This feature would allow new operators to request the creation of a new account. Depending on the provided information, the administrator can decide the level of access that the user might have.

Requirement ID	GUI-R21
Short name	Help and documentation
Key objectives	- to provide access to provide tutorials and/or documentation
Priority rank	Conditional
Description	A button should be present in the home page to provide access to tutorials and user manuals.
Comments	This feature allows the operators to get information on S4RIS and on the tools

Requirement ID	GUI-R22
Short name	Frequently/recently used tools
Key objectives	- to collect the tools frequently/recently used
Priority rank	Optional
Description	The homepage could include an area where the most frequently/recently used tools are displayed, to simplify the access to those tools
Comments	This feature allows to have in a single place the most frequently/recently used tools, so that the operator can access them easily.

Requirement ID	GUI-R23
Short name	Dashboard
Key objectives	- to display information to the user
Priority rank	Conditional
Description	A dashboard displaying relevant and useful information to the user should be present in the home page.
Comments	If possible, a dashboard should be present in the home page. The type of displayed information will depend on the actual implementation of the tools

Requirement ID	GUI-R24
Short name	Mobile interface
Key objectives	- to allow usage of S4RIS from mobile devices
Priority rank	Conditional
Description	S4RIS GUI should be compatible for displaying on mobile devices such as tablets or phones. In this case, it should be possible to launch only the tools compatible with usage from mobile devices.
Comments	In the long run, the support for using S4RIS from mobile devices will be a plus.

4.2.2 User stories

This section contains a set of user stories for S4RIS Graphical User Interface, defined within Task 2.4.

A user story is an informal, natural language description of one or more features of a software system (Ref. [54]). It is usually written from the perspective of a user of the system and its purpose is to articulate how a software feature will provide value to the customer. The user stories describe:

- the user involved;
- the need to be satisfied;
- the reason why the need has to be satisfied.

They typically follow a simple template such as (Ref. [55]):

As a < type of user >, I want < the objective of the user > so that < the reason >.

User stories are typically accompanied by acceptance criteria that specifies the conditions under which a user story is fulfilled. In particular, the scenario-oriented approach is very popular: it comes in the form of scenarios that illustrate each criterion. The common template for describing acceptance criteria using a scenario-oriented approach is the Given/When/Then format that is derived from behaviour-driven development. The Given/When/Then format is used for writing acceptance tests that ensure that all the specification requirements are met.

Table 6 reports the user stories derived from the requirements defined in 4.2.1. Acceptance criteria following the scenario-oriented approach are also included within the same table. These user stories will be useful both to drive the development and validation of S4RIS GUI.

TABLE 6: S4RIS GUI USER STORIES

Req. ID	Short name	User Story			Acceptance criteria		
		As a…	I want…	so that…	Given…	When…	Then…
GUI-R01	Web-based interface	S4RIS user	to have a web-based interface	I am not required to install an application on my PC, as well as I can access it from any device connected to the Internet	That I prefer to not install any application into my PC	I enter the URL of S4RIS on a web-browser	I shall access the login page of S4RIS
GUI-R02	Login page	S4RIS user	to visualise a very simple login page	I can easily access S4RIS with my own credentials	That I already have S4RIS credentials	I enter username and password into the login page	I shall enter into S4RIS Home page
GUI-R03	Single point of access to the tools	S4RIS user	to have a home page providing access to all the S4RIS tools	I can easily select and launch the tool I wish to use	That I want to launch one of the S4RIS tool	I am on the S4RIS Home page	I shall easily identify and launch the one I want
GUI-R04	Grouping of tools	S4RIS user	to have tools grouped according to resilience phases	I can easily identify which are the tools available for each task/purpose	That I need to perform a certain task or achieve a goal	I am on the S4RIS Home page	I will select the group containing the tools with the capability needed (e.g., detection)
GUI-R05	How to launch tools	S4RIS user	to have a customised icon button to launch each tool containing its name or acronym	I can easily identify the tool that I am looking for	That I want to launch one of the S4RIS tool	I am on the S4RIS Home page	I will launch the chosen one by simply clicking on the corresponding icon containing its name and acronym
GUI-R06	Display of tools based on user role	S4RIS user	to clearly visualise only the tools to whom I am authorized to access	I can avoid wasting of time caused by launching tools which I am not authorised to use	that I am not authorized to use all the S4RIS tools because of my role	I am on the S4RIS Home page	I will clearly visualise the tools which I am authorized to access
GUI-R07	Tools keywords and short descriptions	S4RIS user	to visualise a short description and a set of keywords for each tool	I can understand quickly which functionalities each tool can perform	That every S4RIS tool is characterised by a short description and keywords	I move my mouse on the icon button of the different tools	I will visualise that information

Req. ID	Short name	User Story			Acceptance criteria		
		As a…	I want…	so that…	Given…	When…	Then…
GUI-R08	Log-out button	S4RIS user	to have a log-out button visible in each page	I can disconnect S4RIS after use and avoid improper access to sensitive data	That I am logged-in to S4RIS	I click on the log-out button present in each page	I will immediately log-out from S4RIS
GUI-R09	Home page button	S4RIS user	to have a button to come back to home whenever I want	I can select another tool	That I am currently using one of the S4RIS tools	I click on the "Home page" button	I am immediately be redirected to the home page
GUI-R10	Password managemen t	S4RIS user	to change my password from the login page	I can increase the security level of my account	That I want to change my password	I click on a dedicated button on the login page	I shall set a new password
GUI-R11	Settings and configuration	S4RIS user	to change settings on a dedicated page, accessible from the home page	I can tailor the usage of S4RIS on my preferences	That I am logged-in to S4RIS and I need to change settings	I click on the "Setting" button of the home page	I can change every option
GUI-R12	Language	S4RIS user	to choose my native language	I can easily understand S4RIS instructions	That different languages are available for S4RIS	I click on the "Language" button on the S4RIS home page	I can select my language from a list
GUI-R13	Bar with additional functions	S4RIS user	to have a simple shortcut to access the followings: - password management; - settings and configuration, if implemented; - language selection.	I can quickly and easily find “enter into S4RIS settings”	That there is a toolbar to access different S4RIS functions	I click on an icon of the toolbar	I can access the related function
GUI-R14	Opening web-based tools	S4RIS user	that tools with web-based GUI are opened in another tab or window of the browser when they are launched	I can simultaneously open different tools and I can still have the S4RIS home page open	I need to work contemporarily with different S4RIS tools	I launch tools with web-based GUI	They are opened in another tab or window of the web browser

Req. ID	Short name	User Story			Acceptance criteria		
		As a…	I want…	so that…	Given…	When…	Then…
GUI-R15	Opening desktop tools	S4RIS user	to launch a desktop application from the S4RIS home page	I can avoid searching for it on my PC	That some S4RIS tools are desktop application	I click on the related icons on the S4RIS home page	The desktop application is automatically launched
GUI-R17	User confirmation on certain actions	S4RIS user	to visualise a confirmation pop-up when I press on log-out	I can avoid unintentional actions which can cause the loss of data	That some S4RIS tools require input from the user to be saved before exiting from the application	I click the log-out button	I shall visualise a confirmation pop-up
GUI-R18	Font type and size	S4RIS user	that S4RIS text is clear and not too small	I can easily read all the instructions	That the S4RIS platform contains text	I use the S4RIS platform	I should be able to read the text without any effort
GUI-R19	Error display	S4RIS user	to visualise a pop-up with a description in human language when an error occurs	I can understand the error and react accordingly	That I could mistakenly enter wrong inputs or perform bad commands	An error occurs	I should visualise a pop-up with the error description in human language
GUI-R20	S4RIS account creation	S4RIS user	to create a user account	I can access S4RIS	That I do not have a S4RIS account yet	I need to access S4RIS for the first time	I should fill in a form starting from login page and request an account
GUI-R21	Help and documentation	S4RIS user	to get some information on the functioning of a certain tool	I can use that tool properly	That I need some clarification/information on a specific tool	I click the help button	The tutorials or documentation on the tools is displayed and can be opened
GUI-R22	Frequently/recently used tools	S4RIS user	to have all the most frequently/recently used tool easily available	I can access them very easily	That I have already used one or more tools	I am on the S4RIS Home page	The most frequently/recently used tools are shown in a dedicated area
GUI-R23	Dashboard	S4RIS user	to have an overview of relevant and useful information	I can take actions if needed	That at least some tools can show information to the user without his/her interaction (e.g., detection tools)	I am on the S4RIS Home page	A dashboard with that information is displayed

Req. ID	Short name	User Story			Acceptance criteria		
		As a…	I want…	so that…	Given…	When…	Then…
GUI-R24	Mobile interface	S4RIS user	to access S4RIS from a mobile device, such as a tablet	I can access S4RIS functionalities when I am in the field	That S4RIS tools are compatible with usage from mobile devices	I access S4RIS from a mobile device	The GUI is shown in a mobile version and only functions compatible with mobile usage are shown

4.2.3 GUI examples

This section reports a set of examples of the main pages of S4RIS GUI. The following images have been elaborated based on the requirements listed in section 4.2.1 and on the user stories listed in section 4.2.2. They are intended as examples and guidelines for the development of the S4RIS GUI. The characteristics (type, colour, position, number, etc.) of each portrayed object are purely indicative.

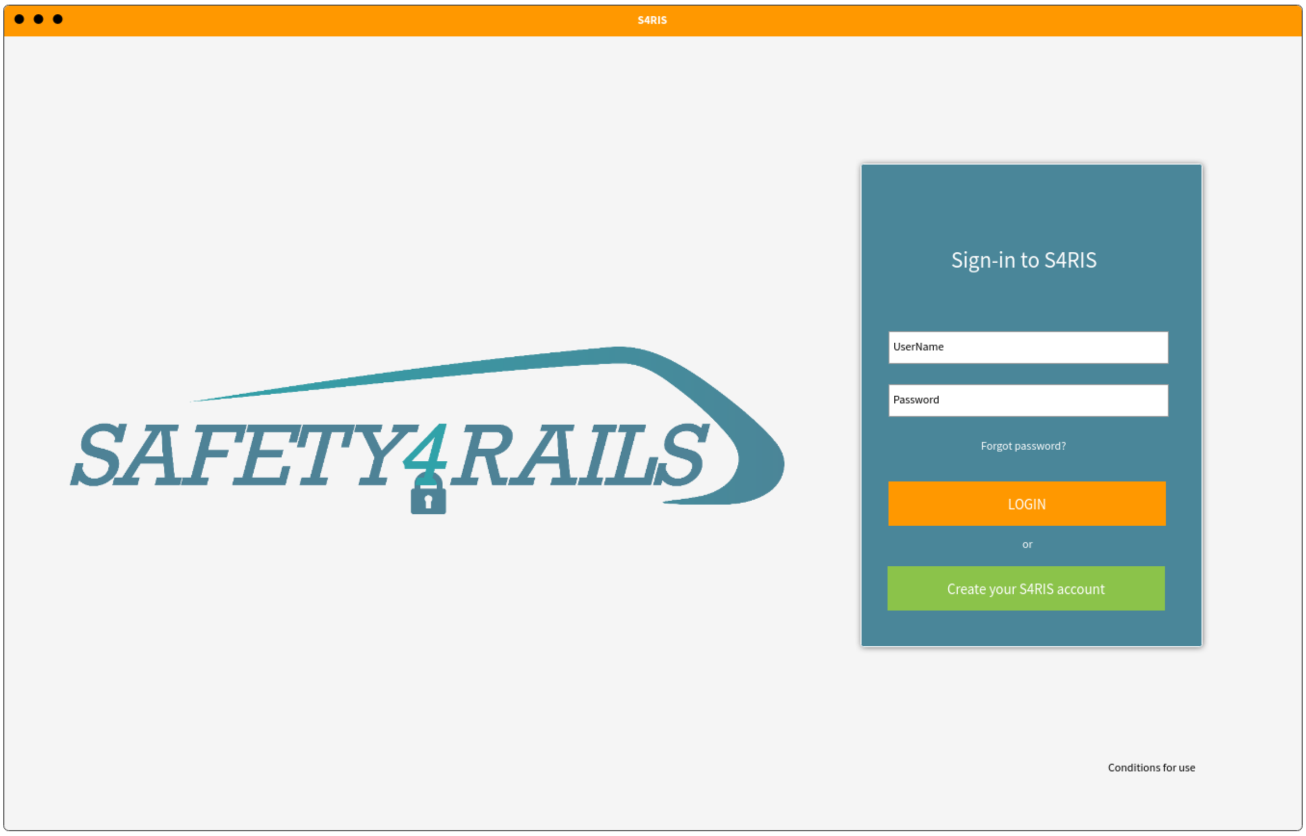


FIGURE 5: SIGN-IN PAGE

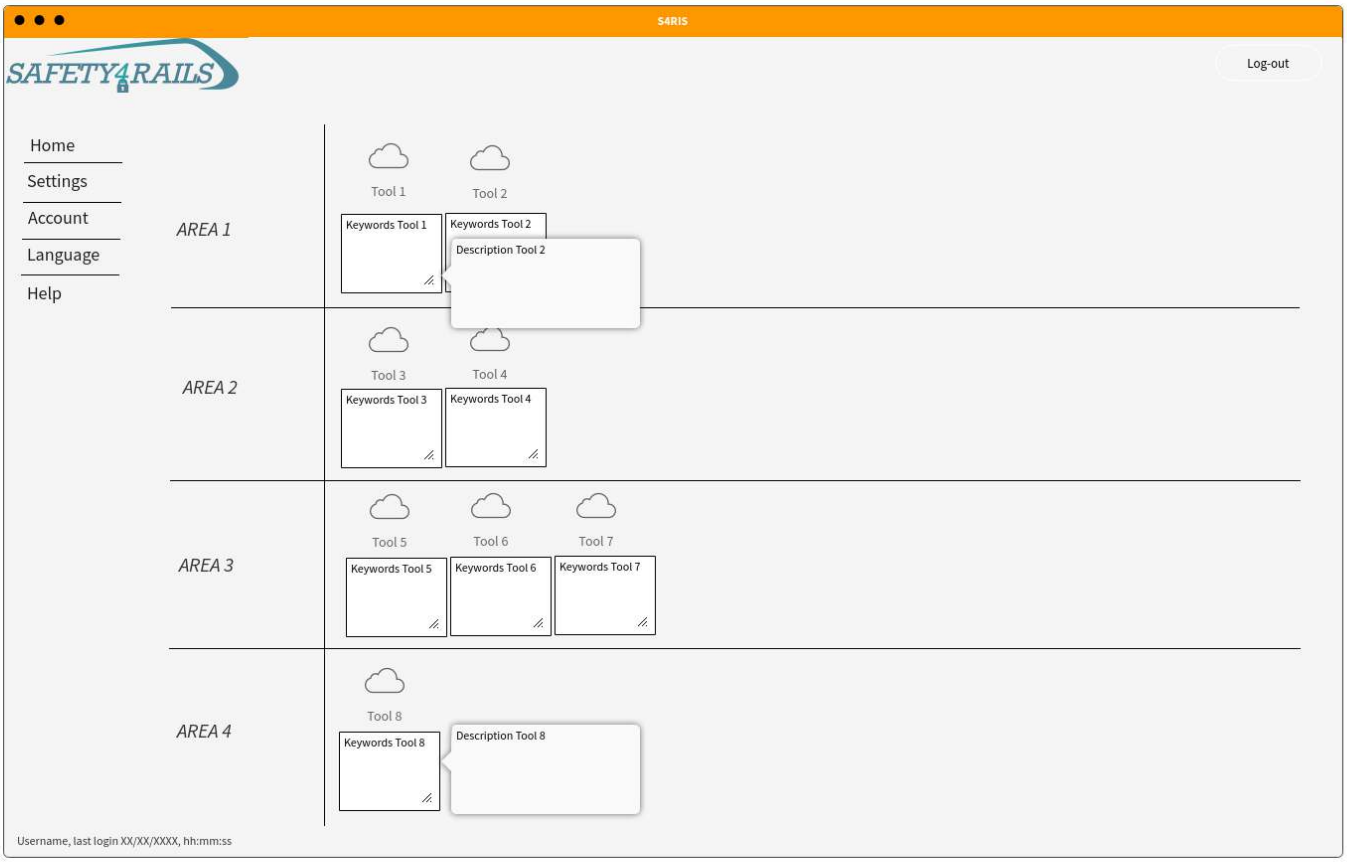


FIGURE 6: HOME-PAGE LAYOUT PROPOSAL #1

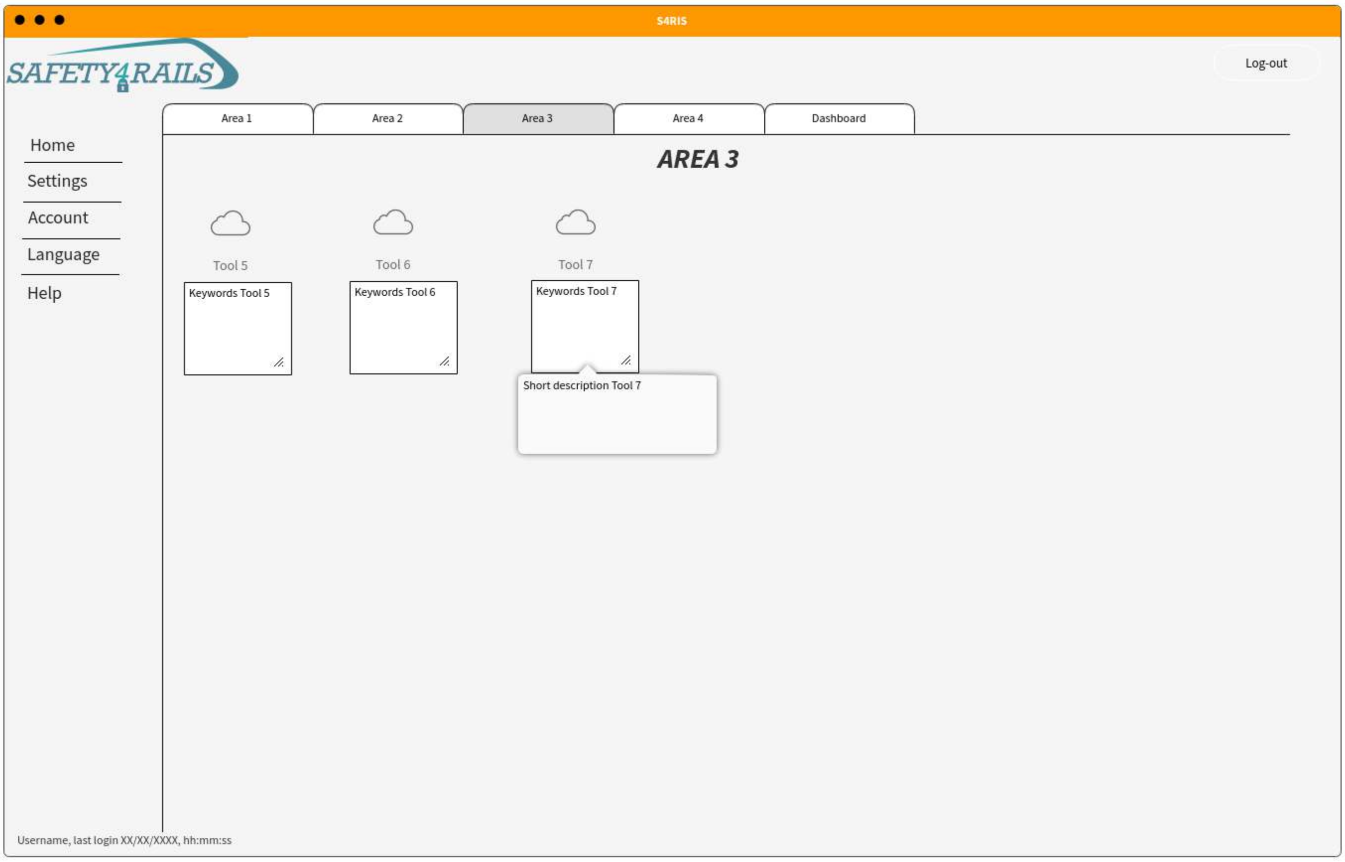
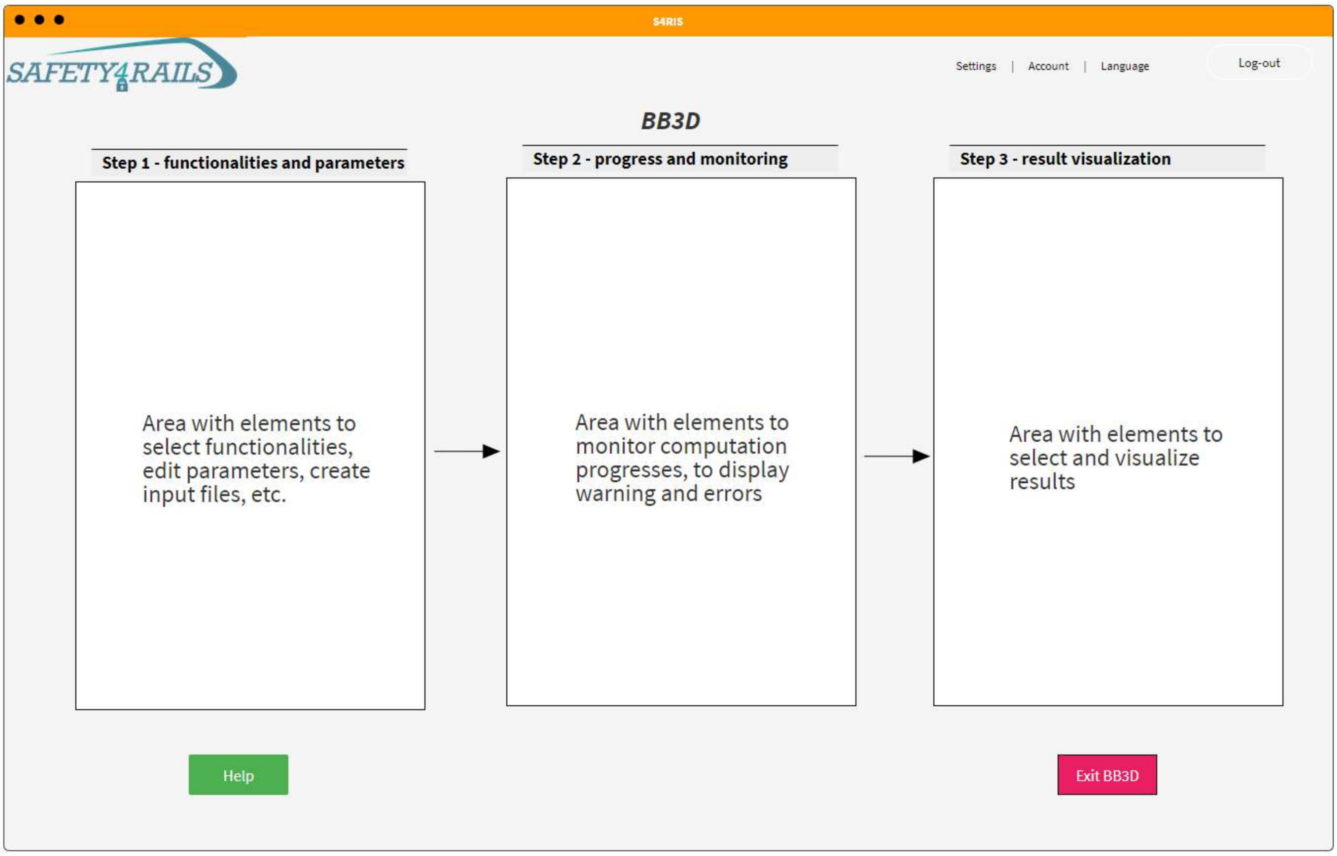


FIGURE 7: HOME-PAGE LAYOUT PROPOSAL #2



BB3D

Step 1 - functionalities and parameters

Area with elements to select functionalities, edit parameters, create input files, etc.

Step 2 - progress and monitoring

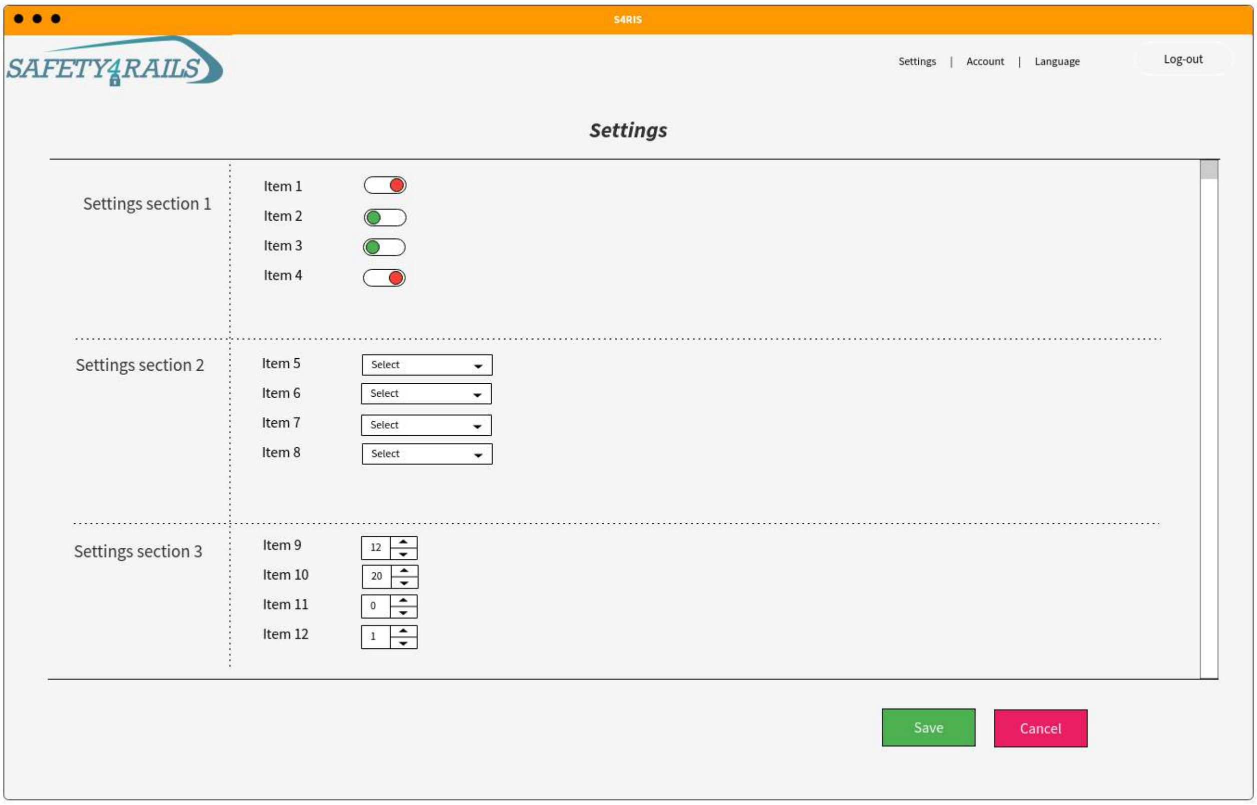
Area with elements to monitor computation progresses, to display warning and errors

Step 3 - result visualization

Area with elements to select and visualize results

FIGURE 8: EXAMPLE OF INTERFACE FOR INTERACTION WITH CLI TOOLS (E.G., BB3D)

Note: the three areas to deal with BB3D could be placed in more than one page, this layout is a concept proposal.



Settings

Settings section 1

Item 1

Item 2

Item 3

Item 4

Settings section 2

Item 5 Select

Item 6 Select

Item 7 Select

Item 8 Select

Settings section 3

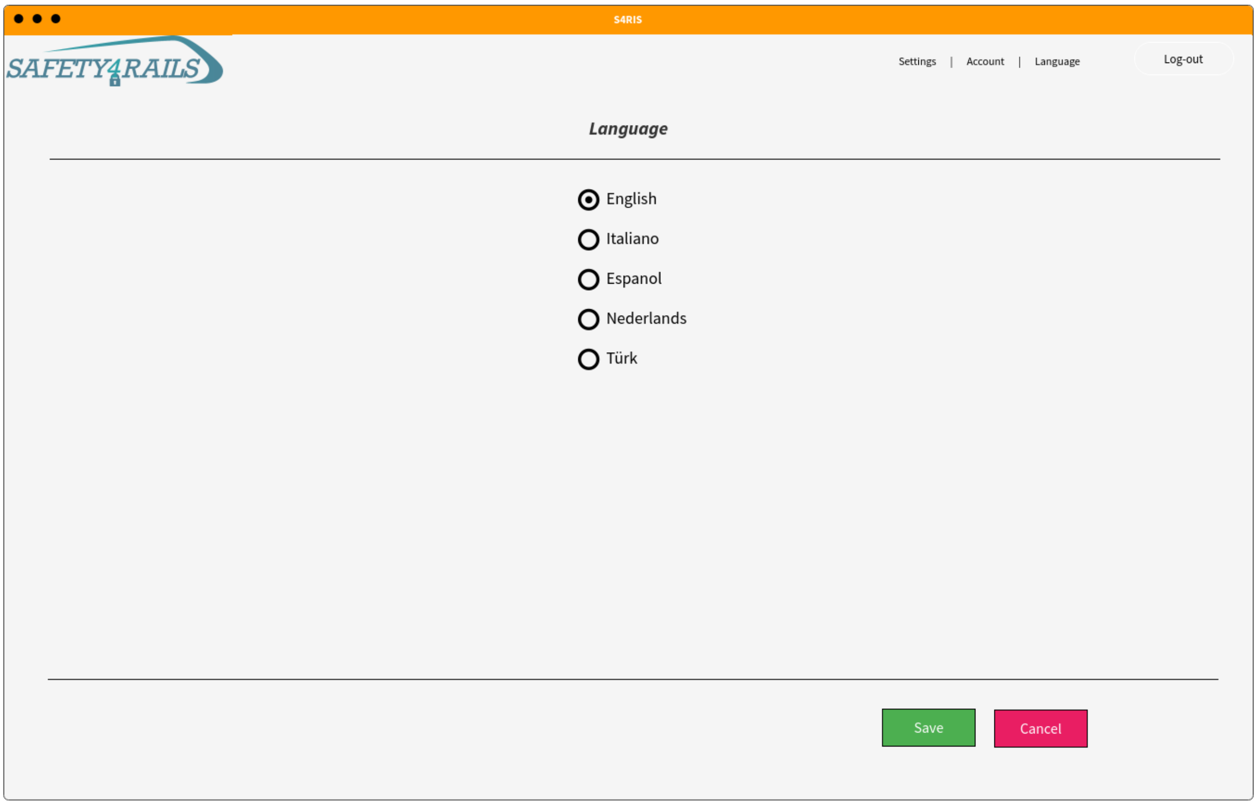
Item 9 12

Item 10 20

Item 11 0

Item 12 1

FIGURE 9: SETTINGS PAGE



● English
○ Italiano
○ Espanol
○ Nederlands
○ Türk

FIGURE 10: LANGUAGE SELECTION PAGE

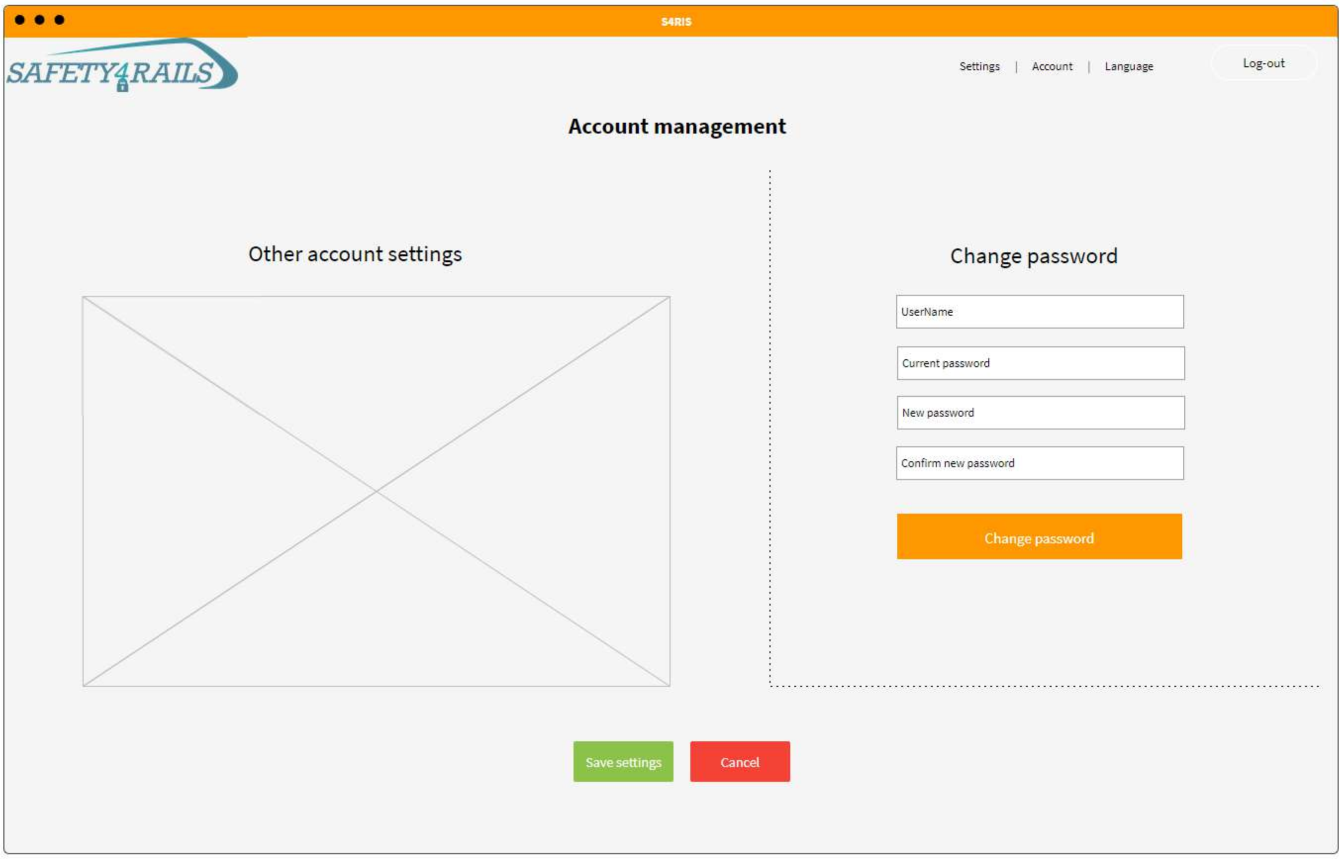
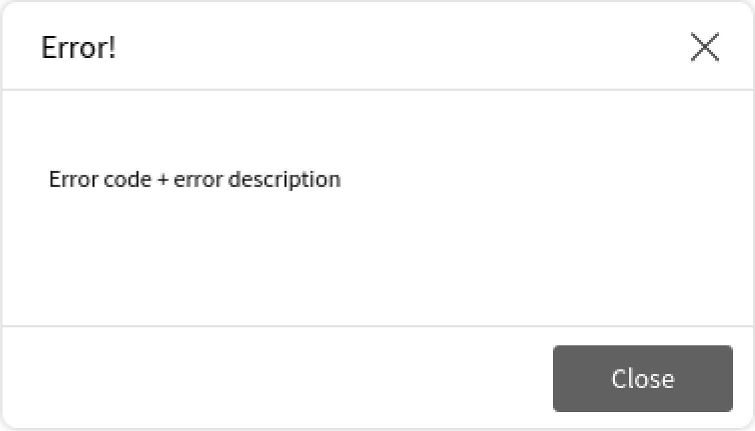


FIGURE 11: ACCOUNT MANAGEMENT



Error!

Error code + error description

FIGURE 12: ERROR POP-UP

5. Conclusions

This report deals with the definition of standardisation, interoperability and graphical user interface requirements. These activities have been carried out in the scope of Task 2.4. The report contains three main sections (§2, §3 and §4), each dealing with one of the three topics of the document.

Concerning standardisation requirements definition, the EU legal framework, standards and best practices in the field of security have been investigated. The NIS Directive (EU) 2016/1148 (Ref. [2]), has been identified as the major legal text regulating security aspects for the railway sector relevant to the S4RIS platform. The proposal for the NIS2 Directive (Ref. [13]) has also been taken into consideration. Both include the Infrastructure Managers, for whom S4RIS is being designed and will be developed, among the Operators of Essential Services. An analysis of the most adopted security standards has been carried out to identify the requirements relevant to S4RIS, in order to meet the OES security requirements, additionally taking into consideration also recommendations provided by the ENISA. The most used standards adopted for requirements definition are ISO 27001, ISO 27002 and IEC 62443. The full list of the defined standardisation requirements is available in section 2.2. Furthermore, additional recommendations and guidelines are provided in section 2.3. The outcome of this activity will enable products based upon S4RIS platform to be as much as possible in line with EU legislation and will also constitute an important input for the activities to be carried out within the Task 9.3 of the project, also led by RINA.

Concerning interoperability requirements definition, information gathered from tool providers and during end-user workshops has been analysed to define an interoperability framework defining the data exchange and alignment within the tools that will be integrated within S4RIS, as well as a concept for the interoperability between the S4RIS and external systems at end-users' premises. The operational interoperability requirements were defined for the S4RIS as well as for external systems. This is input into the architecture of S4RIS and for integration in/with external systems. The foreseen architecture should be flexible and generic, to ensure a working integration of the heterogenous systems and to provide possibilities for adapting the S4RIS prototypes to the end-users' needs. The outcome of this activity will be precious for Tasks 6.1 and 6.2, dealing with operational and technical interoperability, respectively.

Concerning graphical user interface requirements definition, the characteristics of the tools that will be integrated within S4RIS have initially been assessed through questionnaires to the tool providers. Based on this information, on common GUI design principles and on inputs received from the end-users, a list of requirements and a set of user stories have been defined, as respectively reported in sections 4.2.1 and 4.2.2. Finally, a set of examples of S4RIS GUI pages is provided in section 4.2.3 for the main pages, as a guideline for actual development of the GUI. From the activity carried out it emerged that the S4RIS GUI will be a web-based interface aiming to provide a single point of access to the tools integrated into the platform and to support the end-users' operators. The outcome of the activity will constitute an important input for the GUI development that will be carried out in Task 6.2.

6. Bibliography

Ref. [1] https://ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en

Ref. [2] 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. [3] 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. [4] ENISA, Railway Cybersecurity report, Security Measures in the Railway Transport Sector, November 2020

Ref. [5] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems COM/2019/546 final

Ref. [6] NIS Coordination Group, Reference document on security measures for Operators of Essential Services, CG Publication 01/2018, February 2018

Ref. [7] ENISA, Mapping of OES Security Requirements to Specific Sectors, December 2017

Ref. [8] ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

Ref. [9] ISA/IEC 62443-3-3:2013 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

Ref. [10] UK Department of Transport, UK Rail Cyber Security Guidance to Industry, February 2016

Ref. [11] https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

Ref. [12] ENISA, Guidelines on assessing DSP and OES compliance to the NISD security requirements, Information Security Audit and Self – Assessment/ Management Frameworks, NOVEMBER 2018

Ref. [13] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (Text with EEA relevance) {SEC(2020) 430 final} - {SWD(2020) 344 final} - {SWD(2020) 345 final}

Ref. [14] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Ref. [15] COMMISSION EVALUATION of COUNCIL DIRECTIVE 2008/114 ON THE IDENTIFICATION AND DESIGNATION OF EUROPEAN CRITICAL INFRASTRUCTURES AND THE ASSESSMENT OF THE NEED TO IMPROVE THEIR PROTECTION

Ref. [16] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities {SEC(2020)433final} - {SWD(2020)358final} - {SWD(2020)359 final Brussels, 16.12.2020

Ref. [17] Directive (EU) 2016/797 of the European Parliament and of the Council of 11 May 2016 on the interoperability of the rail system within the European Union

Ref. [18] Directive (EU) 2016/798 of the European Parliament and of the Council of 11 May 2016 on railway safety

Ref. [19] Regulation (EU) 2016/796 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Railways and repealing Regulation (EC) No 881/2004

Ref. [20] https://www.era.europa.eu/activities/technical-specifications-interoperability_en

Ref. [21] https://www.era.europa.eu/activities/common-safety-methods_en

Ref. [22] Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009

Ref. [23] EN 50126-1 Railway applications —The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 1: Generic RAMS Process

Ref. [24] EN 50126-2 Railway Applications — The specification and demonstration of reliability, availability, maintainability and safety (RAMS) – Part 2: Systems Approach to Safety

Ref. [25] EN 50128 Railway applications — Communication, signalling and processing systems — Software for railway control and protection systems

Ref. [26] EN 50129 Railway applications — Communication, signalling and processing systems — Safety related electronic systems for signalling

Ref. [27] EN 50159 Railway applications — Communication, signalling and processing systems

Ref. [28] COMMISSION REGULATION (EU) 2016/919 of 27 May 2016 on the technical specification for interoperability relating to the 'control-command and signalling' subsystems of the rail system in the European Union

Ref. [29] COMMISSION IMPLEMENTING REGULATION (EU) 2019/776 of 16 May 2019 amending Commission Regulations (EU) No 321/2013, (EU) No 1299/2014, (EU) No 1301/2014, (EU) No 1302/2014, (EU) No 1303/2014 and (EU) 2016/919 and Commission Implementing Decision 2011/665/EU as regards the alignment with Directive (EU) 2016/797 of the European Parliament and of the Council and the implementation of specific objectives set out in Commission Delegated Decision (EU) 2017/1474

Ref. [30] https://www.era.europa.eu/activities/european-rail-traffic-management-system-ertms_en

Ref. [31] CENELEC prTS 50701 Railway applications – Cybersecurity

Ref. [32] European Commission, HORIZON 2020 – WORK PROGRAMME 2014-2015 General Annexes, G. Technology readiness levels (TRL), available at: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

Ref. [33] OASIS CAP: Common Alerting Protocol, specification version 1.2, 2010. (http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.html)

Ref. [34] OWASP (Open Web Application Security Project) CODE REVIEW GUIDE 2.0 (https://owasp.org/www-pdf-archive/OWASP_Code_Review_Guide_v2.pdf)

Ref. [35] NIST SP 800-63-3 Annex A (https://pages.nist.gov/800-63-3/)

Ref. [36] https://us-cert.cisa.gov/sites/default/files/publications/infosheet_SoftwareAssurance.pdf

Ref. [37] https://owasp.org/

Ref. [38] https://owasp.org/www-project-top-ten/

Ref. [39] https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards

Ref. [40] https://cwe.mitre.org/index.html

Ref. [41] https://cve.mitre.org/

Ref. [42] https://nvd.nist.gov/

Ref. [43] Nielsen, J.. Heuristic evaluation. In Nielsen, J., and Mack, R.L. (Eds.), Usability Inspection Methods, John Wiley & Sons, New York, NY.

Ref. [44] https://www.nngroup.com/articles/ten-usability-heuristics/

Ref. [45] FIRST, CSIRT Services Framework, Version 2.1, November 2019 (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1)

Ref. [46] https://www.first.org/resources/guides/

Ref. [47] NIST SP 800-61 rev. 2, Computer Security Incident Handling Guide (http://dx.doi.org/10.6028/NIST.SP.800-61r2)

Ref. [48] Guédria W., Naudet Y., Chen D. 2008. Interoperability Maturity Models – Survey and Comparison. Meersman R., Tari Z., Herrero P. (eds) On the Move to Meaningful Internet Systems: OTM 2008 Workshops. OTM 2008. Lecture Notes in Computer Science, vol 5333. Springer, Berlin, Heidelberg. 2008.

Ref. [49] IEEE. 1990. "A Compilation of IEEE Standard Computer. New York, Standard 1990. . 1990.

Ref. [50] —. 11 Dec. 2000. The Authoritative Dictionary of IEEE Standards Terms, Seventh Edition. in IEEE Std 100-2000 , vol., no., pp.1-1362. 11 Dec. 2000.

Ref. [51] ISO/IEC. 2003. International Technology for Learning, Education,. International Standard, Geneva: ISO, 2003. 2003.

Ref. [52] Morris, Edwin & Levine, Linda & Meyers, Craig & Plakosh, Daniel. 2004. System of Systems Interoperability (SOSI): Final Report. . 2004.

Ref. [53] Saikou Y. Diallo, Heber Herencia-Zapana, Jose J. Padilla, Andreas Tolk. 2011. Understanding interoperability. In: Proceedings of the 2011 Emerging M&S Applications in Industry and Academia Symposium. Boston, Massachusetts: Society for Computer Simulation International; 2011, p. 84–91. 2011.

Ref. [54] Cohn, Mike (2004). User Stories Applied: For Agile Software Development. Addison-Wesley. ISBN 0321205685. OCLC 54365622.

Ref. [55] Lucassen G, Dalpiaz F, van der Werf JM, Brinkkemper S (2016) The use and effectiveness of user stories in practice. In: Proceedings of the international conference on requirements engineering: foundation for software quality (REFSQ), LNCS, vol 9619. Springer, pp 205–222.

Ref. [56] SAFETY4RAILS, Deliverable D1.4 Specification of the overall technical architecture, October 2021.

Ref. [57] SAFETY4RAILS, Deliverable D2.3 System's specifications and concept architecture, September 2021.

ANNEXES

ANNEX I. GLOSSARY AND ACRONYMS

TABLE 7: 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
REST	Representational State Transfer

Term	Definition/description
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

Partners:

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