SAFETY4RAILS

SYSTEM SPECIFICATIONS AND CONCEPT ARCHITECTURE

Deliverable D2.3

Lead Author: NCSRD

Contributors: Fraunhofer, MDM, EGO, PRO, RFI, LDO, CEIS, STAM, IC, RMIT, RINA, WINGS, INNO, ERARGE, ICOM, UMH, AC, TREE

Dissemination level: PU – Public

Security Assessment Control: passed

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

D2.3 System Specifications and Concept Architecture		
Deliverable number:	D2.3	
Version:	V1.6	
Delivery date:	27/09/2021	
Dissemination level:	PU – Public	
Nature:	Report	
Main author(s)	Konstantinos Panou, Lemonia Argyriou	NCSRD
Contributor(s)	Uli Siebold, Stephen Crabbe	IC, Fraunhofer
Internal reviewer(s)	Atta Badii Stephen Crabbe	UREAD Fraunhofer
External reviewer(s)	Andre Samberg	n/a

Document control			
Version	Date	Author(s)	Change(s)
0.1	13/1/2021	NCSRD	Initial Version TOC
0.2	10/2/2021	NCSRD	Initial Content for Section 2
0.3	5/3/2021	NCSRD, STAM, IC, Fraunhofer, ERARGE, LDO, WINGS, ICOM, TREE, RINA, RMIT	Contribution to System Specifications by tool providers
0.4	25/3/2021	NCSRD	Added content for Section 3
1.0	23/4/2021	NCSRD, IC	First consolidated version
1.1	18/5/2021	NCSRD, UMH, Fraunhofer	Updated after first review, added contribution from UMH to Section 3
1.2	4/6/2021	NCSRD, Fraunhofer	Updates from internal review
1.3	25/6/2021	NCSRD	Updates from internal review
1.4	8/7/2021	NCSRD	Final version for external review
1.5	27/9/2021	NCSRD	Final version after external review
1.6	27/9/2021	Fraunhofer	Minimal updates to front cover, footers, this page and back cover and formatting.

DISCLAIMER AND COPYRIGHT

ABOUT SAFETY4RAILS

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

SAFETY4RAILS concentrates on rush hour rail transport scenarios where many passengers are using metros and railways to commute to work or attend mass events (e.g. large multi-venue sporting events such as the Olympics). When an incident occurs during heavy usage, metro and railway operators 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 CONTENT

List of tables

List of figures

Executive summary

This document is Deliverable D2.3 – System's specifications and concept architecture – of SAFETY4RAILS. The objective of this document is to provide a report on the overall SAFETY4RAILS concept system architecture and sub-system specifications. The layered approach followed in the architectural design of the SAFETY4RAILS is based on the analysis of the user and system needs reported in other deliverable reports "D2.1-Grid analysis of end-users needs and workshop minutes", "D2.2-Report on past failure analysis and past lessons learned" and D1.4-Specification of the overal technical architecture which depicts the complete set of processing modules and interfaces required, their relation and interconnections. D2.3 aims to serve as a reference document for all technical developments in the project and for validating achievement of technical objectives by subsequent WPs prior to release of relevant technologies for trials involving end-users.

The deliverable provides a concrete specification of all the tools integrated as sub-system solutions in the final integrated SAFETY4RAILS platform. Those sub-systems aim to contribute to risk assessment, real-time monitoring, simulation and decision-making support services that are offered by the SAFETY4RAILS platform. Through the architecture specification, the different data source needs are being presented along with the storage solutions, the information exchange framework, the data processing and the decision-support services.

Finally, directions for the real deployment of the SAFETY4RAILS integrated platform are detailed followed by a statement on the conditions required for its configuration as a product.

1. Introduction

1.1 Overview

The goal of the SAFETY4RAILS project is to design, develop and integrate a suite of software systems providing a range of capabilities into a comprehensive platform solution aiming to increase the security and resilience of the railway sector. The SAFEYT4RAILS Information System (S4RIS) platform will provide a real-time monitoring solution able to constantly process incoming streams of data which further trigger risk assessment processes to detect threat events. Moreover, the platform will offer decision support tools that provide guidance and further insights for mitigating security threats and incidents by simulating what-if-scenarios tailored to the railway sector.

In this context, the purpose of this document is to present the work carried out under Task 2.3 - Specifications and modelling concept architecture which is comprised of the formulation of system specifications for the S4RIS platform tools followed by an analysis and presentation of the Safety4Rails concept architecture.

1.2 Structure of the deliverable

The document contains the following sections:

- Section 1: Introduction
- Section 2: System Specifications
- Section 3: Concept System Architecture
- Section 4: Conclusion

1.3 Methodology

The methodology followed in Task 2.3 started with the analysis of the end-user needs and requirements from “T2.1- Specifications and modelling concept architecture”, “T2.2- Requirements from past failure analysis and lessons learnt”, “T2.4- Requirements based on standardization and interoperability framework” and “T2.5- Specific requirements for inter-city and intra-city railway and metro systems” in order to formulate the S4RIS platform tool specifications that can address them. An analysis of modular approaches that enable individual sub-system development and interfacing of each platform component is set out. The core outcome of this analysis is the specification of the conceptual S4RIS architecture and the definition of the required physical and logical components of the solution as well as the intercommunication protocols to support secure information and data transfer.

The main actions that took place in T2.3 and are reported in this deliverable were the following:

Analysis of each of the S4RIS platform tools by gathering information from tool providers with regards to the tool functionalities and their overall role in the S4RIS platform (also from D1.4).

Analysis of requirements gathered as part of Tasks 2.1, 2.2, 2.4 and 2.5. In order to effectively define the system specifications for S4RIS platform tools it was important to thoroughly review and analyze all requirements collected from other tasks. System specifications were formulated as needed to address the elicited requirements.

Formulation of tool specifications based on requirements review and derive new system specifications and functionalities to be implemented and fulfilled by the S4RIS platform tools.

Analysis of modular architecture approaches suited to the S4RIS platform involved researching and reviewing state of the art approaches in large scale software systems design and tailoring the approach to be followed in the SAFETY4RAILS project.

Design of the S4RIS concept architecture by applying a tailored architecture approach based on the aforementioned analysis. The goal of the S4RIS concept architecture is to present in a clear and concise manner information flow in the S4RIS platform by modularizing the architecture in different layers and defining

the interactions between them. The concept architecture should further clarify and provide insights with regards to the purpose of different tools in the platform while assisting in the identification of data needs and their sources, the definition of functional needs per pilot use-case and the intended interaction between the end-users and the platform.

2. System Specifications

2.1 S4RIS Platform overview

The S4RIS platform aims to provide real-time monitoring, risk assessment and decision support services by applying methods that constantly collect, process and analyze incoming data streams from sensors and other sources relevant to the railway sector. Real-time monitoring tools will process the data further and attempt to detect threats and anomalies through the application of threat intelligence utilizing techniques such as machine learning. Information from monitoring tools can be forwarded to decision support tools to further process the incoming data in order to present end-users with useful information and suggested mitigation options with regards to threats. Moreover, the platform will make use of several simulation tools in an attempt to further enhance the decision support capabilities of its end-users applying methods such as infrastructure asset simulation and agent-based crowd simulation. In the SAFETY4RAILS project lifecycle, a set of different work packages address the specific functionality domains of the S4RIS platform, in summary:

- Work Package 3 is concerned with Risk Assessment tools and the corresponding techniques employed in the platform.
- Work Package 4 deals with Real-Time Monitoring Methods from various sources such as sensors, infrastructure, databases, APIs or raw data.
- Work Package 5 is responsible for the provision of various Simulation services from different tools in the platform in order to provide end-users with enhanced decision support capabilities.
- Work Package 6 deals with the integration of all those different components, methods and services in the final S4RIS platform.

The diagram shown in Figure 1 outlines the processes described above and their interaction between them.

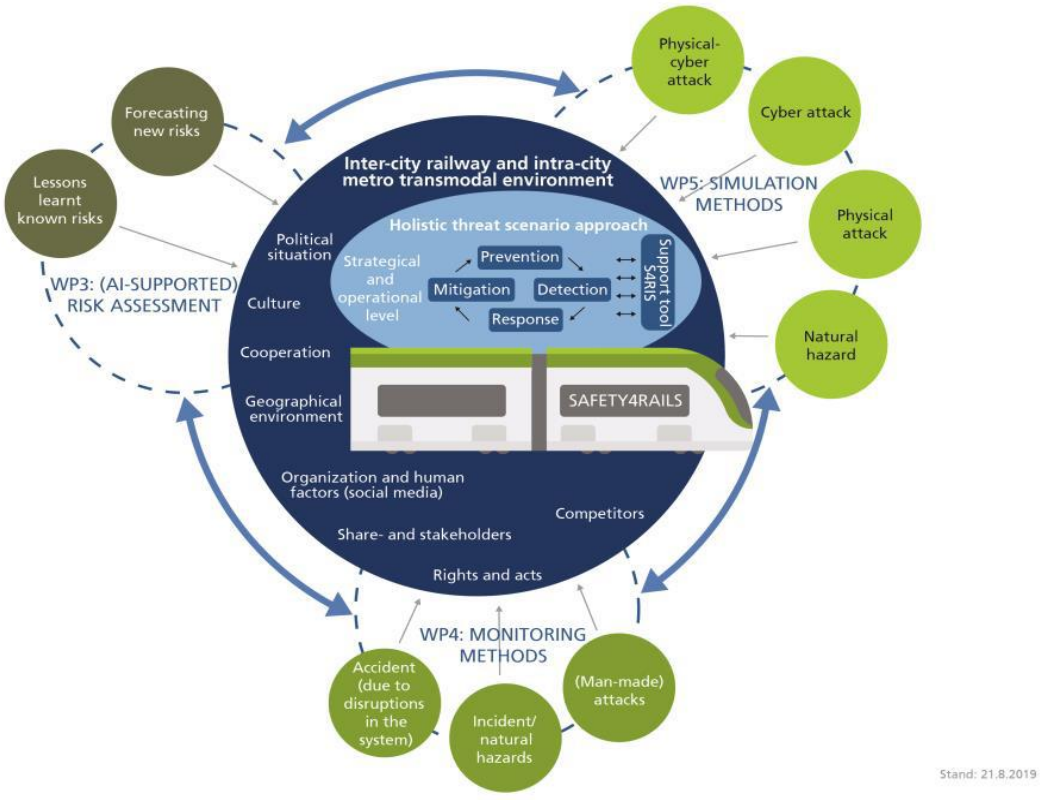

FIGURE 1 - WORK PACKAGE INTERACTION IN SAFETY4RAILS [1]

At a high-level, tools in the S4RIS platform are foreseen to be able to provide functionality under three main domains:

- Real-Time Monitoring / Infrastructure tools
- Simulation tools
- Risk assessment / Decision support tools

The tools inside the platform are able to offer functionalities under one of those domains although it is more often the case that a tool will provide an intersection of functionalities across these domains. The following Venn diagram shown in Figure 2 depicts this concept by visualizing the intersection of tools across the different domains in the S4RIS platform. The diagram presented aims to provide a broad understanding with regards to the domains in which the tools provide their main functionalities.

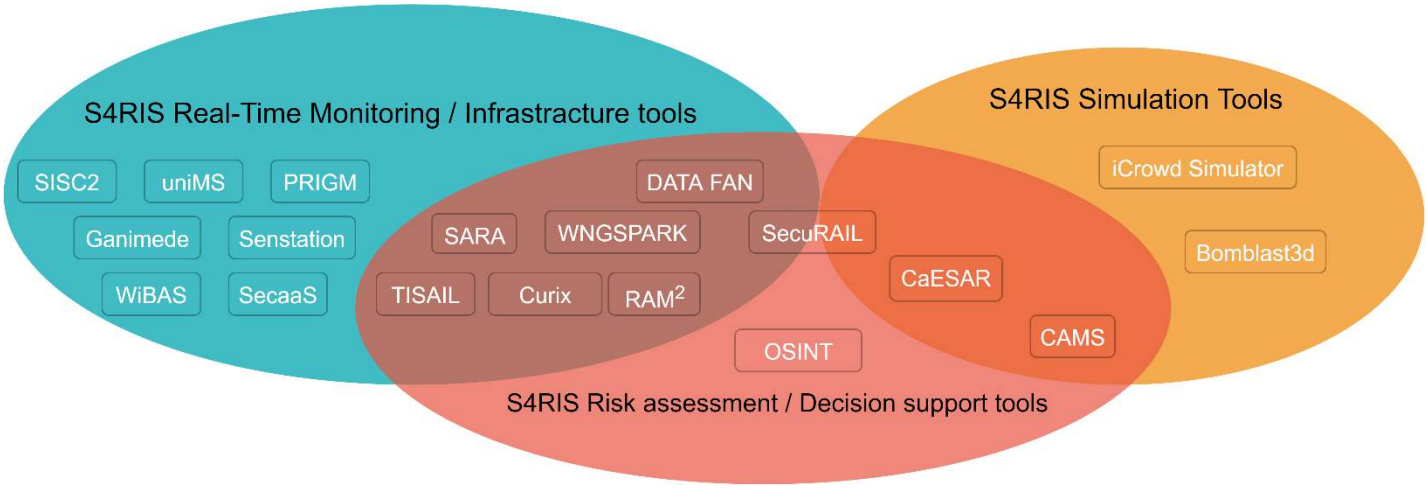

FIGURE 2 - DOMAIN INTERSECTION OF TOOLS IN THE S4RIS PLATFORM

There are 19 distinct software tools in total in the S4RIS platform, from these:

- 7 tools (unIMS, SISC2, Senstation, PRIGM, Ganimede, WiBAS and SecaaS) provide monitoring and infrastructure services related to security, network infrastructure and CCTV data stream analysis.
- 8 tools (DATA FAN, SARA, TISAIL, Curix, RAM², CAMS and SecuRAIL) provide an intersection of monitoring, simulation and decision support services that are made possible through the use of intelligent risk assessment mechanisms and provide further mitigation insights through decision support functionality.
- 4 tools (iCrowd Simulator, Bomblast3d, CAMS and CaESAR) provide simulation services such as agent-based crowd simulation and bomb blast simulation scenarios enabling the security and resilience assessment of a station.

In the next section a thorough specification of all the tools that are part of the S4RIS platform, their data needs, functionality and requirements that they address is presented.

2.2 System Specifications for the S4RIS platform

This section presents the various tools in the S4RIS platform followed by the corresponding system specifications for each tool. The tool specifications provided in this section refer to functionalities that are either provided already by the tool or will be implemented as part of the development of the tool for the S4RIS platform. It is also important to note that, as tools in the S4RIS platform will need various forms of data input, a number of the specifications are dependent on the data provision from end-users as well as the integration with other tools in the platform. Below, the specification of each tool in the S4RIS platform is defined in the form of a table providing:

- A description of the tool and its objectives with regards to the S4RIS platform

- Pre-condition / Input definition describing mandatory data needed for the main functionality of the tool along with specific hardware needs (e.g.: integration with sensors).
- Post-condition / Output definition which is a description on the different forms of output for the tool.
- Operational Specifications, a sub-table containing a list of System Specifications of the tool mapped to a specific S4RIS domain defining also corresponding data needs. Each specification will be grouped under a specific domain: Risk Assessment, Infrastructure, Monitoring, Simulation and Decision Support.
- Component dependencies specification, defining the interconnection and data exchange needs and conditions for each tool.

The tool operational specifications were derived based on thorough analysis of the functional and non-functional requirements gathered in Task 2.1, 2.2, 2.4 and 2.5 followed by a concrete analysis of the tool requirements derived from Task 1.2. The system specifications presented indicate the functionality to be provided by the S4RIS platform in a clear manner and should act as a point of reference in terms of validating technical achievements [6].

2.2.1 SECURAIL

Component Name	**SECURAIL**
Responsible	STAM
Description and Objectives	
SECURAIL is a risk assessment web-based application for Railway infrastructures and networks which allows to perform both quantitative and qualitative analysis, therefore it could be considered as a hybrid evaluation. Moreover, it is classified as dynamic because it allows to conduct analysis with real-time data coming from sensors, monitoring and surveillance systems. It is a web-based application characterized by a powerful computation engine capable to generate, simulate and analyze thousands of risk scenarios according to the topology of the infrastructure and the threats considered. It is a general-purpose application; therefore, the end-user can customize its own railway infrastructure by using an intuitive graphic user interface. Moreover, it has a dashboard to study the results of the analysis and visualize them through charts and indicators. The engine of the tool, starting from the components of the infrastructure/system (e.g., assets, areas, security measures) modelled by the user and its own knowledge base, is capable to generate thousands of attack scenarios. For each scenario, the evolution is simulated to understand the set of possible outcomes and computes the related impact, likelihood and risk. SECURAIL will be used mainly for prevention, so it will develop a risk analysis before an attack, but it could be exploited for early warning when it performs real time analysis. This last peculiarity will allow to identify a threat when it occurs giving the possibility to protect the infrastructure in time. Finally, with the purpose of developing the SECURAIL tool within SAFETY4RAILS, it is necessary to build an extensive database to collect and organize all the data required by the risk analysis algorithms. In this manner, the tool will take into account the connections and interdependences between different components of the infrastructures making the model very realistic and providing reliable results.	
Pre-condition / Input	
• Detailed modelling of the components of the infrastructure (areas, assets, security measures, services) and their relationships	

• Database of threats against the railway infrastructure (cyber, physical, cyber-physical attacks, natural hazard), e.g., GTD and RAND for terrorism, to define likelihood of occurrence and potential impact • Economic figures of assets and services • Real-time alerts from monitoring/surveillance systems to run real-time targeted risk analysis for rapid impact assessment • Distribution of people within the infrastructure/network
Post-condition / Output
• Cost-benefit analysis in order to compare risk reduction with cost of security measures implementation • Risk assessment of the defined infrastructure considering several scenarios, with results expressed through diagrams, tables, charts and pictures • Modelling of the connections and interdependences between different components of the infrastructures to assess cascading effects consequences
Operational Specification

S4RIS Domain	**Operation/Function Description**	**Data Needs**
Risk Assessment	The tool will be the main one with the aim of implementing the risk assessment process. Input will be requested to the user through GUI, while results will be depicted in dashboards and reports	Components of the infrastructure, economic value of the assets, likelihood of an attack, distribution of people within infrastructure/network
Monitoring	SECURAIL enables the analysis in real-time of an emerging threat and react accordingly	Sensors and an alarm system in real-time
Decision Support	The tool will provide cost-benefit analysis functionality to support the user in comparing the reduction of risk with the cost of protection in order to find a trade-off	Results obtained by the running of the SECURAIL tool, CAPEX and OPEX of security measures and procedures

Component Dependencies

Component Name	**Needs and data description**
CuriX	Alerts containing relevant information (e.g., type of threat occurring, target affected) in order to define a risk scenario and analyze it with real-time risk assessment for rapidly assess potential impact on the whole infrastructure/network

2.2.2 SARA

Component Name	**SARA**	
Responsible	RINA-C	
Description and Objectives		
SARA (SECURESTATION Attack Resilience Assessment) aims to analyze a station and its equipment from a security point of view. The results of the analyses will enable the user to define, evaluate, rank and select possible countermeasures to be applied to the equipment of the station in order to reduce the effects of a terrorist attack. The effects considered are related to the loss of elements and functioning of the different equipment. The activities of ranking and selecting the countermeasures 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) [11].		
Pre-condition / Input		
Station/terminal functional model, equipment location, passenger density, timetables.		
Post-condition / Output		
Station security and resilience assessment results and mitigation countermeasures.		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Risk Assessment	Physical and functional resilience and security assesment of the station and relevant equipment.	Station and Terminal structural model along with asset information.
Simulation	Simulate accidents in order to assess the security of the station and quantify the impact of hazards by applying relevant analytical and numerical methodologies.	Structural model of the station along with equipment model.
Decision Support	Provide cost-effective countermeasures that could potentially improve the overall security of the station based on the accidents simulated.	
Component Dependencies		
N/A		

2.2.3 DATA FAN

Component Name	**DATA FAN**	
Responsible	Fraunhofer	
Description and Objectives		
DATA FAN is used as a monitoring and detection tool. It monitors the active railway system to detect anomalies in the data using machine learning methods. Furthermore, the DATA FAN can simulate various what-if-scenarios in order to evaluate various scenarios and events, e.g., what is to be done if a certain stop cannot be operated due to a cyber or physical threat to avoid panic among the passengers. Moreover, the DATA FAN will provide a reliability assessment for its results and applied algorithms.		
Pre-condition / Input		
Raw data, user data, labelled data (time series data e.g., passenger load/utilization (with the label a) running railway system as well b) during a threat), additional video or image data)		
Post-condition / Output		
Display the detection of a deviation from the norm and an additional score of the reliability of the detection		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Monitoring	Real-time monitoring from incoming data streams.	Time series data from sensors and raw Data to process,
Risk Assessment	Apply anomaly detection techniques and prediction algorithm to the incoming data streams.	
Decision Support	Visualize results of prediction algorithms in a friendly user interface for assisting domain experts with decision making.	
Component Dependencies		
CuriX, CEASAR, SECURAIL, TISAIL, GANIMEDE		

2.2.4 CAMS

Component Name	**CAMS**
Responsible	RMIT
Description and Objectives	
A web-based software tool enabling asset managers to make informed decisions for maintenance and rehabilitation activities. The software tool uses a probabilistic deterioration prediction model to reflect the stochastic nature of condition degradation to model variety of components of the infrastructure asset. Risk and expenditure forecasting based on Markov Chain deterioration prediction are generated within the tool [12].	
Pre-condition / Input	
• Asset inventory • Condition inspection data • Repair records • Maintenance, repair and rehabilitation costs	
Post-condition / Output	
Risk/cost evaluation, damage condition forecasting, expenditure prediction, budget allocation, budget optimization.	
Operational Specification	

S4RIS Domain	**Operation/Function Description**	**Data Needs**
Simulation	Prediction of normal deterioration due to aging and degradation of assets	Condition rating from regular inspections of assets. At least data from two consecutive inspections is required to train the data-based model. Further, repair records of the inspected assets is needed to clean the data and remove outliers.
Simulation	Maintenance and repair budget calculation	It requires maintenance, repair, and rehabilitation costs, unit cost of the component. Further, it requires investment policies, budgeting, as well as intervention criteria (threshold of the maintenance activities)
Simulation	Risk / Cost Evaluation	The data required to perform risk/cost evaluations is the cost of a component being in a given condition

		and the managing authority's policy on intervention.
Decision Support	Analysis of compromise between maintenance, repair, rehabilitation and resilience enhancement efforts	This specification requires the data of previous requirements such as the budget, the definition of budgetary scenarios as well as the available budget for maintenance, repair, rehabilitation and response.

Component Dependencies	
Component Name	**Needs and data description**
CaESAR, SECURAIL	Common definition of the infrastructure model.

2.2.5 CaESAR

Component Name	**CaESAR**
Responsible	Fraunhofer

Description and Objectives

CaESAR is a coupled grid simulation tool which computes cascading effects within grids and across grid borders to assess and enhance the resilience of critical infrastructures in urban areas. The overall aim is to find optimized strategies for the mitigation of hazard impact on inter-connected grids [14].

Pre-condition / Input

- Model of the railway infrastructure should exist including system components and their links to other components as well as system functions
- Need Input for Model adaption in relation to
  - System functionalities
  - Mitigation/recovery strategies
  - Infrastructure vulnerabilities
  - Infrastructure performance measures

Post-condition / Output

- Resilience curves
  - Graphical representation of resilience over time including applied mitigation measures
- Resilience indicators
  - Box plot graphs (real-time: if several simulation runs are possible)
- CaESAR will show the output as a colored network scheme containing the following information:

- Results of the impact analysis are visualized as a graph consisting of nodes and edges
- Graph shows where the propagation started and which further nodes are impacted in the following time steps, i.e., the result graph represents the time-dependent impact
- Graph will be provided as gif
- Graph gives also an overview on remaining nodes and their remaining functionalities after the impact.

Operational Specification

S4RIS Domain	Operation/Function Description	Data Needs
Simulation	Estimate the propagation of disruptive events through the railway network and from/to interdependent infrastructures including the impact on the infrastructure, its components and their functionalities.	Network Model for the impacted infrastructure (see input defined above) Interdependencies to other relevant critical infrastructures should be available
Simulation	Identify weak points in the railway/metro system, i.e., estimate which components contribute most to the impact propagation	Network Model for the impacted infrastructure (see input defined above)
Simulation	Provide several strategies to recover from disruptive events and evaluate their impact on the infrastructure resilience.	Network Model for the impacted infrastructure (see input defined above) Data regarding • recovery strategies, • infrastructure performance measures should be available.
Simulation	Provide possible and rated mitigation measures to weaken the impact of a disruptive event to/from interdependent infrastructures	Network Model for the impacted infrastructure (see input defined above) Data regarding • mitigation strategies, • rating of mitigation strategies • infrastructure performance measures should be available.

Component Dependencies

N/A

2.2.6 CuriX

Component Name	**CuriX**
Responsible	IC
Description and Objectives	
CuriX is an microservice based software tool to accurately predict failure occurrences in IT, IoT environments. CuriX is deployable to infrastructure e.g., computers or VMs, platforms e.g., databases or applications e.g., monitoring applications. The main objective is to precisely locate the sources of potential failures or critical systems' states in advance. Operators can perform mitigations before the business is impacted by complex outages; this can have a huge impact on security, non-availability of critical infrastructure for safe and secure transportation as well as costs (e.g., Service Level Agreements) and generally on the risk management. CuriX covers the entire process of data analysis using state of the art artificial intelligence operations and machine learning techniques. The process of outage prevention can be divided into four consecutive phases. Initially sensor data is collected in a data collection phase, followed by an anomaly detection phase and a failure prediction phase in which faults are localized. Finally, there is the fault correction phase in which fixes are implemented [13].	
Pre-condition / Input	
CuriX can be integrated in existing control/monitoring environments/infrastructure either by adapting to existing monitoring tools or by implementing customized connectors to collect numerical Key Performance Indicator (KPI) data. Data collection and aggregated KPI data can be processed on infrastructure, platform, and application level. Collected KPIs are transferred to CuriX using standardized APIs. The performance data gets analyzed and as a result information about anomalies, health scores, and a failure indication is provided. The more extensive the KPIs are the more precise the outage prevention will be. Input from • Source Layer (refer to D2.4; Figure 3); Monitoring/Infrastructure Tools (e.g. Sensation, PRIGM, UNIMS) • Railway Network (Operation Data) • IT Operation Monitoring (ITOM) • Security Information and Event Management (SIEM) • Industrial Control Systems (ICS) • Supervisory Control and Data Acquisition (SCADA) • Configuration Management Database (CMDB) Input of: • Numerical Key Performance Indicators (KPI) • Log data • Sensor data • Railway infrastructure hierarchy • Integration using standardized APIs (e.g., JSON)	

- Follow the rules of interoperability (following the interoperability concept described in D2.4)
- Accessibility from S4RIS (Web link) from S4RIS Web application to CuriX Web application.

Post-condition / Output

As an output, CuriX provides information on system status (e.g., in form of anomalies, health scores of system elements, correlations, etc.) and if there will be a system failure, the location of potential faulty resources. Based on this information the railway operator can proactively intervene. Furthermore, a semi-automated or full automated fix execution process can be implemented. The results of the different CuriX phases (data collection, anomaly detection, failure prediction, fault localization) are summarized in CuriX Web dashboard as well as forwarded to existing monitoring tools. Failure prediction and alarms of fault correction phase can be integrated using REST API.

Operational Specification

S4RIS Domain	Operation/Function Description	Data Needs
Risk Assessment	Topological/hierarchical view on services / contracts / dependencies	System topology model
Risk Assessment	Risk score of system assets. E.g., based on anomalies per asset the risk score can be defined.	System topology mode, real time numerical performance indicators
Monitoring	Failure Prediction and Fault Correction Advice (Healing recommendations)	System topology mode, real time numerical performance indicators
Monitoring	Proactive Infrastructure Monitoring	System topology mode, real time numerical performance indicators
Monitoring	System Resource Optimization for the Railway IT infrastructure	System topology mode, real time numerical performance indicators
Monitoring	CuriX Connectors (integration) to other S4RIS tools	Arbitrary numerical indicators
Monitoring	Anomaly Detection for not constant time series	System topology mode, real time numerical performance indicators
Simulation	Catalogue based attack simulation	Attack simulation parameters need to be provided
Decision Support	Catalogue based mitigation advices	System topology mode, real time numerical performance indicators

Component Dependencies

Component Name	Needs and data description
S4RIS	S4RIS user can access CuriX Dashboard (GUI); so that CuriX opens in another tab or window of the browser when it is launched from S4RIS GUI.

2.2.7 PRIGM

Component Name	PRIGM	
Responsible	ERARGE	
Description and Objectives		
PRIGM is a Hardware Security Module (HSM), a device that is capable of performing 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). HSM connects to a host device (server, PC, etc.) using PCIe interface. It is enclosed in a tamper-proof enclosure. PRIGM will operate at the server side.		
Pre-condition / Input		
Encrypted sensory data that comes from field to the Operation Control Centre (OCC)		
Post-condition / Output		
Decrypted sensory data in a required format. (e.g., json, csv, xml, SQL) Output can be streaming data or output data can be stored in a database		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Monitoring	PRIGM gets sensory data from field and decrypts them. PRIGM is connected to a PC via PCIe connector. Sensory data can be stored in the PC or sent through the network.	N/A
Simulation	PRIGM will work as a utility for the management of certification and IoT device authentication	N/A
Decision Support	In case of PRIGM has an open channel sensory data or previous sensory data statistics. PRIGM can detect anomalies between open and secure sensory data.	Sensory data of Railway/metro as raw, anonymized,

		or statistical analysis.
Component Dependencies		
Component Name	**Needs and data description**	
Senstation	PRIGM needs encrypted sensory data that comes from field.	

2.2.8 Senstation

Component Name	**Senstation**	
Responsible	ERARGE	
Description and Objectives		
The purpose of Senstation is to provide secure data transmission between the railway physical infrastructure and S4RIS. Senstation is planned to be realized as the combination of a secure gateway and sensor interface. Senstation will be installed at the client side aiming to encrypt critical data where data is generated and assure the security of data on transit. Senstation and PRIGM will work in coherence to update the required one-time passwords or any other secrets.		
Pre-condition / Input		
• Integration of sensors with Senstation. • Existence of communication channel between Sensation and PRIGM		
Post-condition / Output		
Encrypted sensory data with timestamp		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Monitoring	Senstation is connected railway/metro sensors on field. Sensory data is encrypted by Senstation and is sent to OCC over a secure channel. In OCC encrypted sensory data is receipted by PRIGM. As a result, a sensor data flow channel that cannot be manipulated, is established	N/A
Monitoring	Communicate with sensors through appropriate hardware interfaces.	Sensors to be integrated

Component Dependencies	
Component Name	**Needs and data description**
PRIGM	Senstation integrates with PRIGM to create end-to-end secure communication channel.

2.2.9 WINGSPARK

Component Name	**WINGSPARK**
Responsible	WINGS

Description and Objectives

In WINGS there is the area of "Networks and Infrastructures" and a part of it is Transportation-Land based. Therein the first focus was parking, and the platform was called WINGSPARK. This platform will be the basis for covering the rails case as well. We will accomplish certain reuse and economies, while we will extend with the capabilities needed in the main use-cases of SAFETY4RAILS project. The platform foundation comprises:

- Devices/sensors/actuators, e.g., for air quality, parking availability, health monitoring and many more, as well as device management functionality (activation, cessation, upgrades).
- Data management functionality (cleansing, imputation, etc.).
- Artificial intelligence mechanisms for generating insights and predictions/forecasts and for supporting and conducting decision making.
- Dashboards and applications for visualization.

Pre-condition / Input

- Data from sensors in cameras concerning rail infrastructure (e.g. tracks, station, surroundings)

Post-condition / Output

- Detected anomalies
- Recommendations for increased security
- Infrastructure resilience analysis

Operational Specification

S4RIS Domain	**Operation/Function Description**	**Data Needs**
Risk Assessment and Monitoring	Data management and analysis is an important aspect of 'Monitoring' and includes e.g., cleansing,	Data from available sensors in the station, rail infrastructure, train (e.g., open/close gates,

	imputation, etc. of data in order to feed the prediction and anomaly detection algorithms accordingly.	doors), camera footage (with hidden faces).
Risk Assessment	Definition and development of machine learning functionality/algorithm for incident prediction/ anomaly detection.	Ingested data from sources previously mentioned will be used for feeding the algorithm.
Decision Support	This operation mainly includes decisions for effective handling of incidents and recommendations for potential increase of security level based on analyzed data and predictions.	Analyzed data will be used for decision making and recommendations.
Decision Support	Provide a user-friendly interface for end users to access visualization data and mitigation strategies	
Component Dependencies		
N/A		

2.2.10 TISAIL

Component Name	**TISAIL**
Responsible	**TREE**
Description and Objectives	
A platform for gathering, analyzing and sharing potential threats that might be relevant for the railway industry, such as active malware campaigns targeting Critical Infrastructures or vulnerabilities that might be exploited by threat actors [16].	
Pre-condition / Input	
• Input of use-cases and attacks scenarios. • List of IT/OT software/devices and providers that are widely used on the railway sector.	
Post-condition / Output	
TISAIL will look for cyberthreats that might be relevant for the railway industry, such as active malware campaigns targeting Critical Infrastructures or vulnerabilities that might be exploited by threat actors.	
Operational Specification	

S4RIS Domain	Operation/Function Description	Data Needs
Decision support	Malware families that might be relevant for the railway industry or for Critical Infrastructures.	Input of use cases and attack scenarios.
Decision Support	Detection of credential leaks and IT/OT exposed assets on the Internet.	List of IT/OT software/devices and providers widely used within the railway industry.
Decision Support	Information Sharing of the latest threats gathered from Threat Intelligence feeds and social media.	Input of use cases and attack scenarios.
Decision Support	Detection of new vulnerabilities that might affect one or more components within the railway industry.	List of IT/OT software/devices and providers widely used within the railway industry.
Decision Support	Detection of domain names supplanting railway providers and companies for spear-phishing attacks.	List of the most relevant providers in the railway sector.
Decision Support	Threat Taxonomy for the railway sector based on MISP taxonomy format for allowing rapid identification of threats.	Threat Taxonomy
Component Dependencies		
N/A		

2.2.11 OSINT

Component Name	OSINT
Responsible	**INNO & T4.2 partners**
Description and Objectives	
A platform for gathering, analysing and sharing potential threats to railway infrastructure for cyber, physical and combined cyber-physical threats. The main objective of the platform is to channel relevant threats to operators as soon as information becomes available in open sources in order to enable operators to prevent continuing exposure to those threats.	
Pre-condition / Input	

- Inventory of device types and deployment parameters for the relevant railway operator(s)
- Description of target use-cases and attack vectors of concern

Post-condition / Output

OSINT will employ TISAIL to search for cyber threats and augment TISAIL capabilities both in the cyber as well as in the physical and cyber-physical OSINT domain.

Operational Specification

S4RIS Domain	Operation/Function Description	Data Needs
Decision support	Malware families that might be relevant for the railway industry or for Critical Infrastructures	Input of use-cases and attack scenarios
Decision Support	Detection of credential leaks and IT/OT exposed assets on the Internet	List of IT/OT software/devices and providers widely used within the railway industry
Decision Support	Information Sharing of the latest threats gathered from threat intelligence feeds and social media	Input of use-cases and attack scenarios
Decision Support	Detection of new vulnerabilities that might affect one or more components within the railway industry	List of IT/OT software/devices and providers widely used within the railway industry
Decision Support	Detection of domain names supplanting railway providers and companies for spear-phishing attacks	List of the most relevant providers in the railway sector
Decision Support	Threat taxonomy for the railway sector based on MISP taxonomy format for allowing rapid identification of threats	Threat taxonomy
Decision Support	Detection of potentially relevant real-world events based on OSINT sources	Description of event types of concern

Component Dependencies

N/A

2.2.12 uni|MS

Component Name	**uni|MS**	
Responsible	ICOM	
Description and Objectives		
The uni|MS (Unified Management Suite) serves the concept of simple and unified management for networks, infrastructure and systems. uni|MS. The platform automates management and monitoring tasks to eliminate error-prone and time-consuming manual efforts. uni|MS platform automates decision-making and augments operators' responsiveness, throughout all phases of the network lifecycle [7].		
Pre-condition / Input		
Real-time network data and network infrastructure configuration.		
Post-condition / Output		
Analytics concerning network activity and alerts with regards to network infrastructure issues. User interface for managing network infrastructure and configuration.		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Monitoring	Real-time monitoring of network activity for detecting malicious activity or problems with network infrastructure.	Real-time network data and network infrastructure configuration.
Monitoring	Unified management of network infrastructure from a web-based interface.	
Monitoring	Provide configurable auditing capabilities to end-users.	
Decision Support	Intuitive user-interface for network infrastructure management and alert previewing.	
Component Dependencies		
WIBAS		

2.2.13 WIBAS

Component Name	**WIBAS**	
Responsible	ICOM	
Description and Objectives		
WIBAS is a state-of-the-art Point-to-MultiPoint (PtMP) native Ethernet microwave product line, perfectly fits demanding operator needs. It provides access to broadband fixed wireless access. It is especially designed for high-speed multi-service applications, WiBAS offers a wide service area footprint reaching distant underserved areas and locations lacking telecommunications infrastructure.		
Pre-condition / Input		
Broadband access configuration.		
Post-condition / Output		
N/A		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Monitoring	WIBAS will monitor broadband connection access in real time and issue alerts whenever there are issues with connectivity.	
Decision Support	WIBAS integrated with uniMS in order to proactively inform operators with regards to degrading network conditions and avoid service-affecting problems.	
Component Dependencies		
uniMS		

2.2.14 SISC2

Component Name	**SISC2**	
Responsible	ICOM	
Description and Objectives		
SISC2 platform maximizes detection efficiency and operational effectiveness and timely produces situational awareness. It augments and expedites the operators' decision-making process by offering decision support and optimizing operation and back-office and mission plans managing available resources and tasks [8].		
Pre-condition / Input		
Integrated sensors and relevant data for human resources and organization assets.		
Post-condition / Output		
Incident management, alarm detection and customizable reports.		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Monitoring	Resource management including humans and assets.	Input of relevant assets to the platform
Monitoring	Multi-Sensor data fusion and track management system to integrate a wide variety of sensors and technologies such as CCTV to enhance real-time situational awareness.	Integration with relevant sensors
Decision Support	Provide incident management tailored to the railway domain.	Railway incident management standard operations specification
Decision Support	Customized reports with regards to incidents.	
Decision Support	Intuitive user interface for end-users providing analytics and access to alerts and mitigation strategies.	
Component Dependencies		

N/A

2.2.15 iCrowd

Component Name	**iCrowd**	
Responsible	NCSRD	
Description and Objectives		
Agent-based human crowd simulation platform capable of efficiently simulating crowds in any internal or external area. Realistic simulation solution regarding physical motion, behavior and interactions among agents or between agent(s) and the simulated environment (such as sensors, doors) [18,19].		
Pre-condition / Input		
• 3D model of the infrastructure (.obj file) • Passenger flow data • Monitoring Assets ontology • Railway service time plan and processes specification • Attack scenarios • Evacuation plans and other threat mitigation strategies		
Post-condition / Output		
Total evacuation time, the average response time, infrastructure and strategies resilience analysis data		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Simulation	Simulate realistic crowd congestion levels to detect crowd flow bottlenecks	The trains' schedule, passenger arrival rates, passenger behavioral model
Simulation	Interaction with other S4R systems	None - The other systems must be able to interface with iCrowd via a TCP/UDP connection and conform to the simulator's JSON-based protocol
Simulation	Detect blind-spots and unattended areas	Guards' movement patterns, cameras' positions and fields of view

Decision Support	Simulate an evacuation because of terrorism (bomb, gas release) or natural disaster (fire/flood), in order to assess the performance of safety measures/resilience strategies	Guards' behavioral model, guards' movement patterns, crisis management strategies
Simulation	Simulate crowd behavior considering cyber agents.	Passengers' behavioral model, areas affect by information presented by cyber agents as well as radius of agent in which knowledge can be transferred to another agent.
Simulation	Simulate access to a restricted area by cyber-attack or physical attack.	Behavior of guard and malicious agents.
Component Dependencies		
N/A		

2.2.16 RAM²

Component Name	**RAM²**
Responsible	ELBIT
Description and Objectives	
RAM² is a cyber-physical risk assessment, monitoring and management platform, integrating with all IT, OT & IoT assets and systems. RAM2 Decision Support System platform is a next-generation solution that enables a proactive cyber defense strategy (detecting gaps & exposures before they become a breach), using a holistic, orchestrated approach and providing the business operational context for all digital assets and systems. The risks are prioritized according to operational and business impact, likelihood and severity. RAM² supports a multi-site configuration to specifically support multi-site continuous compliance and policy governance [10].	
Pre-condition / Input	
Syslogs, REST API, CSVs, Industrial Project Files, network PCAPs	
Post-condition / Output	

Assets, alerts and insights using API calls and Syslogs, as well as via PDF and CSV files		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Risk Assessment	RAM² will generate correlated insights based on the identification of patterns that indicate potential risk.	Data collected from sensors and/or end user input.
Decision Support	RAM² will provide alerts and insight mitigation steps.	Definition of the operational hierarchy of the railway system in RAM² in order to provide mitigation strategies.
Decision Support	RAM² will provide a dashboard presenting end users with detailed information with regards to system status, pending alerts and mitigation options.	N/A
Monitoring	RAM² will integrate with other platform tools such as CuriX in order to receive syslog output data for processing and generation of alerts.	N/A
Component Dependencies		
CuriX		

2.2.17 BB3d

Component Name	**BB3d**
Responsible	RINA
Description and Objectives	
A predictive tool based on the literature empirical data to develop analyses of blast loading consequent to a bomb explosion. Enables the fast calculation of the distribution of the main blast wave parameters around and over three-dimensional complex geometries virtually reproducing potential attractive targets for terrorists.	
Pre-condition / Input	

• 3D modelling of infrastructure and surface mesh according to STL format model (ASCII and free) • Parameters such as bomb blast data (explosion point, mass charge, type of explosive).
Post-condition / Output
• VTK paraview files (ASCII free format) that can be visualized through the open-source software Paraview (https://www.paraview.org/) • Visual analysis of blast-induced adverse consequences to assist the design of protective strategies and countermeasures
Operational Specification

S4RIS Domain	**Operation/Function Description**	**Data Needs**
Simulation	Simulate Bomb explosion scenario for railway station.	Railway station model along with parameters such as the bomb explosion radius and other blast wave parameters.
Simulation	Computing time for bomb explosion simulations should last less than 20 minutes.	
Decision Support	Provide analysis of results from bomb explosion simulation offering insights to end users with regards to increasing railway station security.	

Component Dependencies
Results of blast simulation will need to be embedded in the S4RIS platform.

2.2.18 SecaaS

Component Name	**SecaaS**
Responsible	ICOM
Description and Objectives	
SecaaS is a software platform that allows for monitoring of network traffic for signs of abnormality. The platform also provides Security as a Service though virtual firewalls and web application firewalls enhancing the security of the network [9].	

Pre-condition / Input		
• Access to signalling network traffic • Firewall configuration		
Post-condition / Output		
Mitigation countermeasures for detected threats.		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Monitoring	Monitoring of network traffic for signs of abnormality and correlation with known cyber attract profiles.	Network traffic activity
Decision Support	Provide mitigation strategies for detected threats in the network.	
Component Dependencies		
N/A		

2.2.19 Ganimede

Component Name	**Ganimede**
Responsible	LDO
Description and Objectives	
Ganimede is a platform for the large-scale analysis of live and recorded data streams based on Deep Learning. Ganimede is implemented exploiting Video Analysis techniques, in IT platforms and security, supported by competence centers specialized in artificial vision and deep learning. Ganimede Video Content Analysis platform enhances situational awareness and transforms threat detections from a manual, resource-intensive operations into an efficient and automated process [15].	
Pre-condition / Input	
CCTV data	
Post-condition / Output	

Metadata and processed data as RTSP stream		
Operational Specification		
S4RIS Domain	**Operation/Function Description**	**Data Needs**
Monitoring	Audio pattern detection	Audio recorded with microphones integrated in CCTV cameras
Monitoring	Enhanced abandoned baggage detection	CCTV data - hall of the station or railway platform:
Monitoring	People re-identification	CCTV data - Due to the difficulties in obtaining identifiable faces, the appearance of clothing becomes the main clue for identification purposes.
Monitoring	Man down detection	CCTV data - hall of the station or railway platform
Monitoring	Event visualization	Events described above visualized in a cartographic view
Component Dependencies		
N/A		

2.3 S4RIS integrated platform interfacing components specification

In the previous section there was the presentation of the tools that are part of the S4RIS platform as provided by technical partners primarily as initial input into the project. This section will present the specifications of tools that are complimentary to the functionality of the S4RIS platform through storage, communication and graphical user interfaces.

2.3.1 Distributed Messaging System (DMS)

Component Name	**DMS**
Responsible	NCSRD
Description and Objectives	
The DMS is an implementation of a Message Broker that can be used by all tools to exchange information. The implementation used in the S4RIS platform will be Apache Kafka, a well-known high-performance messaging system which is based on the publish-subscribe design pattern [4, 5]. Parties can publish data in specific topics and parties that are interested in the data can consume	

data from topics that they are interested in. In Apache Kafka parties can create topics which contain data, each topic has a specific name and purpose. There can be any number of topics depending on the data exchange needs. Publishers are the parties interested in publishing data to a topic for others to consume. Consumers are the parties that are interested in consuming data from topics. Whenever a new message is published on a topic by a publisher, consumers are notified and can immediately consume the new message. The concept outlined can be shown below in Figure 3. One of the main advantages of using a Message Broker implementation as a means of communication between multiple systems is that whenever a system is needs to share information with two or more other systems then they can share this information through the message broker to be available for all other systems interested in the information instead of integrating with each of the interested tools separately.

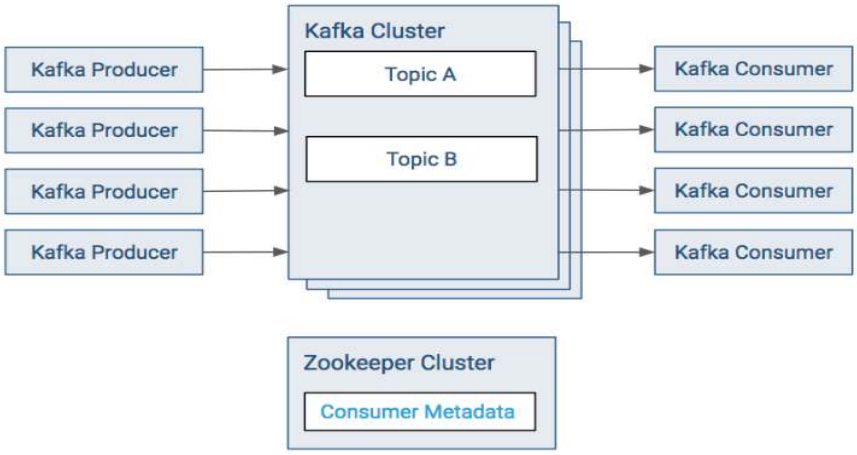

FIGURE 3 - APACHE KAFKA COMMUNICATION OVERVIEW

Pre-condition / Input	
JSON REST API	
Post-condition / Output	
JSON REST API	
Operational Specification	
Operation/Function Description	**Data Needs**
Provide secure channel for communication between S4RIS platform tools.	N/A
Provide authentication capabilities to the platform for ensuring that only allowed parties are allowed to use DMS.	N/A
Allow the exchange of messages in JSON format between parties in DMS.	Specification of the Data Model for each topic in the DMS.

Component Dependencies
All components in S4RIS that will integrate through DMS

2.3.2 S4RIS GUI

Component Name	**S4RIS GUI**
Responsible	UNEW
Description and Objectives	
The S4RIS GUI will be a web application that will act as an intermediate layer to the user interfaces provided by other tools in the S4RIS platform. The primary objective of the S4RIS GUI is to provide a unified GUI for end-users to access information and different tools in the S4RIS platform. S4RIS GUI will integrate with S4RIS platform tools in order to provide relevant links to the specific GUI of each tool. Moreover, the S4RIS GUI aims to provide an intuitive interface to end-users for accessing and displaying and updating information.	
Pre-condition / Input	
Actions from end-users in the GUI.	
Post-condition / Output	
Depending on user actions this may vary. Results may be displayed or other tools may be opened.	
Operational Specification	
Operation/Function Description	**Data Needs**
Authentication and Authorization capabilities for users	N/A
Providing links to access other web-based, desktop and CLI S4RIS platform tools	Information required from each tool that needs to be accessed through S4RIS GUI.
Account management	Specification of the Data Model for each topic in the DMS.
Settings and configuration	N/A

Choice of Interface Languages	Relevant translations for interface elements.
Help and Documentation	N/A
Component Dependencies	
All components in S4RIS that will be available for access through S4RIS GUI.	

2.3.3 Blockchain

Component Name	**Blockchain**
Responsible	Alpha Cyber
Description and Objectives	
The use of Blockchain technology will be investigated and elaborated as part of the SAFETY4RAILS project. The motivation behind the adoption of Blockchain is to enhance the monitoring and detection of cyber and cyber-physical threats. The performance for sharing and accessing real-time data for the monitoring and detection tools will also be investigated. Blockchain technology can prove beneficial in any system/platform where information integrity is of significance. SAFETY4RAILS will attempt to provide a novel solution that harnesses the benefits of the technology and further increases the overall safety of the platform.	
Pre-condition / Input	
Data to be stored on the Blockchain	
Post-condition / Output	
Access to data on the Blockchain. Facilities to verify events/transactions are valid.	
Operational Specification	
Operation/Function Description	**Data Needs**
Access to the Blockchain for entities which have a defined identity and role in the network	Entities and roles to be defined.
Determine open-source blockchain platform solution to be employed.	N/A
Use of permissioned Blockchain.	N/A

Data acquisition and storage of data such as audit trails and alerts.	N/A
Detecting attempts of manipulation with ingested data and provide functionality for verifying events/transactions.	Relevant translations for interface elements.
Component Dependencies	
All components in S4RIS that will store data on the Blockchain and/or will need to verify events/transactions.	

3. Concept System Architecture

3.1 Concept System Architecture approach

The S4RIS platform is comprised of 19 tools many of which are platforms themselves, focused on specific domains providing certain functionalities. One of the main challenges of designing the architecture for the S4RIS platform is defining a clear separation of concerns between different tools/modules, which is of great significance as a lot of the tools used in SAFETY4RAILS might be used as standalone tools after project completion. In light of this challenge, the approach followed employs a combination of a multilayered architecture and the N-tier architecture style which separates the architecture in multiple layers attempting to achieve clarity with regards to layer functionality and interoperability.

The architecture approach employed is an open N-tier/N-layer architecture approach [2] which enables any layer to communicate with any other layer in the architecture. The reasoning behind choosing an open architecture is that some of the layers that will be part of the S4RIS platform provide services/functionalities that can be used from many other layers, a prime example of this being the Information Exchange layer providing communication facilities to all tools in the S4RIS platform. In an N-tier architecture services are not only logically separated but also physically which points to the fact that various services run on different infrastructures and hardware which is the case for the S4RIS platform. This is especially useful since it might not always be possible to deploy certain tools on premises due to various reasons.

Some of the benefits of N-tier architecture design in relevance to the S4RIS platform:

- Portability between cloud and on-premises deployment
- Open to heterogenous software environments
- Flexibility when integrating existing software systems
- Enables iterative development work and early testing between components

Some of the challenges of N-tier architecture design in relevance to the S4RIS platform:

- Independent deployment of features will need good coordination between parties involved to avoid issues.
- More work is involved since there is physical separation between systems and they run on different environments.
- Avoiding unnecessary development of middle tier software.

Figure 4 shows an example of an architecture with multiple services and layer separation between them.

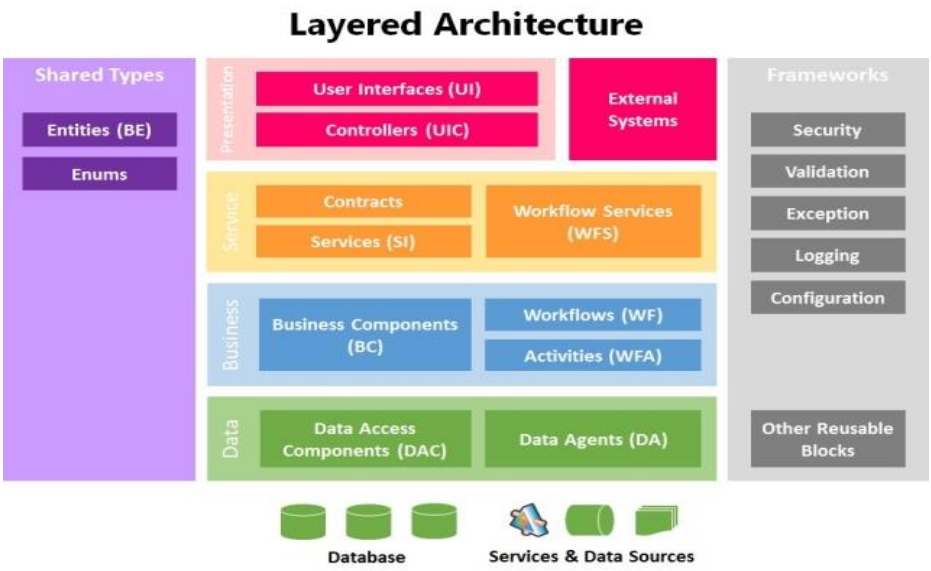

FIGURE 4 - LAYERED ARCHITECTURE EXAMPLE [3]

3.2 SAFETY4RAILS Concept System architecture

The SAFETY4RAILS platform is comprised of a number of tools where each tool provides a set of capabilities to the platform. The goal of the concept architecture is to present a high-level architecture diagram that outlines how all the different components/tools interconnect and how information flows through the different layers of the S4RIS platform. It is important to note that layers in the context of the Concept Architecture are aimed more towards modelling an abstract grouping of the tools in S4RIS and interactions between them instead of layers representing realized software. Tools can coexist in multiple layers as well as interact with other layers depending on their nature and the features they provide, for instance a tool can perform data processing and at the same time provide decision support capabilities to the platform. The S4RIS platform concept architecture is presented as an open N-tier architecture consisting of 5 different layers:

- Source Layer
- Information Exchange Layer
- Storage Layer
- Data Processing Layer
- Decision Support Layer

In Figure 5 below the S4RIS platform Concept System architecture is presented. Arrows in the diagram represent the direction of information flow in the platform, the presence of bidirectional arrows represents constant exchange of information between layers. Following there will be an analysis of each layer's function and interactions with other layers.

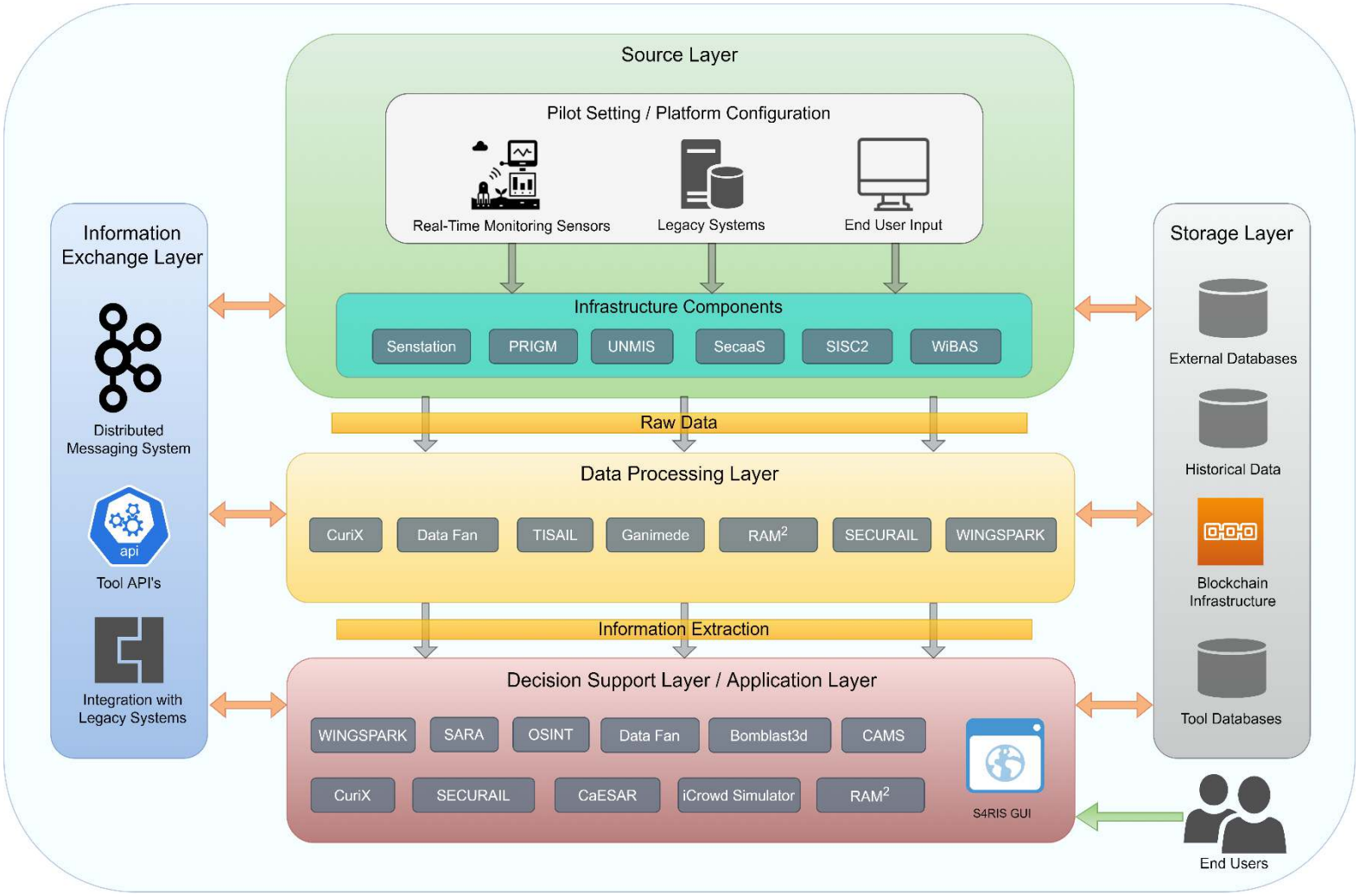

Figure 5 – The concept of S4RIS Platform Concept System Architecture

3.3 Source layer specification

The Source layer is the layer where information flow starts in the SAFETY4RAILS platform. Initially, the configuration of the platform under a specific pilot setting should take place. The platform configuration entails the following:

- Real-Time monitoring Sensors (Temperature sensors, Wind sensors, Network monitoring infrastructure)
- Integration with Legacy Systems and definition of what information will be made available to the platform and how it will be exploited by the platform
- Railway station 3D model, railway grid plan, Equipment specification
- End-User Input.

Real-time monitoring sensors for a specific Pilot Setting refers to the set of the sensors available from end-users along with the sensors that are part of the SAFETY4RAILS platform. Coordination with end-users at this level is important as there should be a clear specification of the information available to the SAFETY4RAIL platform tools from the sensors as it is of great significance to exploit available information for further data

processing. It is also possible that data from sensors can be fed through 3rd party tools used by end-users which can integrate with one or more tools in the S4RIS platform thus providing further flexibility and minimizing integration effort with distinct sensors.

Integration with legacy systems concentrates on the integration of the SAFETY4RAILS platform with external systems for data exchange. Depending on the nature of external systems to be integrated a detailed functional approach will be formulated regarding how these systems will interface with the platform. This will be defined in close cooperation with end-users.

End User input can include a few different options ranging from configuration of the platform's tools from the end users to the preparation and uploading of offline real or synthetic data for usage within the system. This can act as an alternative or additional to the Real-time monitoring sensors in case it is not possible to integrate with end users' sensors, if access is forbidden for instance due to security reasons or to include information that is not detected by sensors but by direct observation of people or communication with third parties or employees. The human sources of information that can be used by the end user to provide different inputs can be divided into two broad categories: information from people inside the organization and information from people outside the organization.

Within the organization: Employees are a source of information that can provide a wide variety of information. The main types of information they can provide are listed below:

- Condition of components and threats to their integrity, functioning and access: Those in charge of the maintenance of different components can identify the presence of mold, damp, rust, limescale, vibrations, overheating, deteriorated locks, forced doors, etc., or confirm the malfunctioning of components.

- Errors and accidents: Any worker can report the loss of keys, devices, documents, accreditations, or any other type of material or information that could trigger a threat.

- Security-related information from direct observation: Workers can also provide information about the level of occupancy, conflict situations, status of access control elements such as doors, locks, status of signs, etc.

- Staffing information: Finally, workers can provide relevant information about their own functioning, such as changes in surveillance, control and monitoring patterns, available personnel, delays of key personnel or they geographical location, unattended locations, etc.

Outside the organization: There are different external actors that can provide valuable information in different domains. The main sources of information and the type of information they can provide are listed below:

- Security forces, civil protection services, fire and emergency services, local administrations, other transportation services and media: They can issue alerts on a wide variety of threats to the end-user (e.g. terrorist alert level, major events, weather forecasts, fires, risk of earthquakes, pollution level, traffic congestion, regulations affecting transportation).

- Metro and railway users: Through intercoms or other means of communication, passengers can issue alerts for incidents, emergencies, conflicts, the status of certain components, etc., based on their direct observation.

- Subcontractors: Surveillance, maintenance, cleaning, etc., may be subcontracted to external personnel. In this sense, external workers can provide the same information as mentioned above for internal organization workers (component status, errors, staffing information and other information obtained from direct observation).

All data made available from the Pilot Setting / Platform Configuration and end-users will go through the Infrastructure Components. Tools in this layer are focused on the network infrastructure and security of the platform providing functionality such as:

- Network Infrastructure Management
- Network Firewalls
- Security of IoT devices
- Encryption of data at transit

Tools that have an important role in the Source Layer are:

PRIGM and **Senstation** are tools that are concerned with the security of data streams from sensors and user data that will flow down to the other layers of the S4RIS platform.

uniMS is a unified network infrastructure management solution concerned with the security and reliability of network infrastructure.

SecaaS provides virtual firewall and web application firewall technologies to the platform and enables real-time monitoring of network traffic for detecting potential threats aiming to increase the security and reliability of the network.

Tools such as SISC2, SecaaS and uniMS will act as sensors for constantly monitoring network activity and any risks and threats detected should be further communicated to the Data Processing and Decision Support Layer through the Information Exchange Layer.

3.4 Storage layer specification

The storage layer is associated with the interfacing of tools in the S4RIS platform to various storage systems for reading or writing data. The various storage systems include:

Tool databases refer to the specific database(s) that each tool in the S4RIS platform provides. A number of tools in the S4RIS platform make use of multimodal database technologies ranging from traditional relational databases such as PostgreSQL and MySQL, document databases such as MongoDB and Elasticsearch as well as time series databases such as InfluxDB. Most tools use a combination of database technologies that is suited to the nature of data processed by the tool. Whenever a tool in the S4RIS platform needs to access data stored by another tool then the process of retrieving the data would be enabled through the Information Exchange Layer.

Historical Data refers to all the trace and log data kept by the different tools in the S4RIS platform. This data will be useful for analysis and debugging of the systems in the platform as well as for the accountability of actions from different users and tools in the platform.

External Databases deal with the integration of tools in the S4RIS platform with various external databases. These include databases provided by end-users as part of a pilot as well as public databases containing useful data that assists information processing in the S4RIS platform. An external database that will be used is the OSINT database which will be integrated in the platform as part of WP4. External Databases will be integrated with specific tools in the S4RIS platform that either use the data directly for processing and/or share data with other tools in the platform through the Information Exchange Layer.

Blockchain Infrastructure is concerned with the provision of a storage solution that utilizes blockchain technology. In the S4RIS platform this will provide a tamper proof storage for various tools and will greatly increase the security and integrity of the S4RIS platform. Blockchain can be utilized for storing data such as audit trails of user actions, sensor reading and generated alerts allowing for verifiable tracing of information in the platform.

3.5 Information exchange layer specification

The information exchange layer is an omnipresent layer in the architecture of the SAFETY4RAILS platform with its main purpose being to enable all the different software components to communicate in a seamless manner. In the SAFETY4RAILS platform the integration options regarding information exchange are:

- Distributed Messaging System
- Tool API integration
- Integration with Legacy systems

Distributed Messaging System (DMS): The Distributed Messaging System is a broker implementation that will be deployed as part of the S4RIS platform. It will be the main integration tool for intercommunication between the different components in the platform allowing heterogenous systems to plug-in to a unified approach for the integration of the platform. Furthermore, it enables parties to easily publish information to all other interested parties preventing the unneeded replication of data while improving network performance in a real-time setting.

Tool API integration is concerned with the provision of specific APIs from tools in the S4RIS platform that will be used to communicate with other tools. Tool providers will be mainly encouraged to integrate through DMS although in some specific cases where there is already an API and there may be specific performance or functional requirements API integration might be a better option.

Integration with Legacy systems encompasses all integrations from S4RIS platform to external systems. These systems can be APIs provided by a specific platform used by the end users. In cases where such an integration happens then one of the tools in the S4RIS platform will integrate with the legacy API which will enable information to be shared with other tools through DMS.

3.6 Data Processing layer specification

The Data Processing layer can receive data from the Source Layer or the Information Exchange Layer. The data received will be processed by the relevant tools in the SAFETY4RAILS platform. During the data processing phase various tools will apply intelligence techniques for risk analysis. Tools in the S4RIS platform that will play a central role in the data processing layer are:

Curix will be one of the main real-time monitoring tools in the S4RIS platform constantly receiving multiple data streams from various sensors and analyzing the respective time series data for applying anomaly detection techniques. CuriX has a multitude of functionalities that intersect with Decision Support / Application layer by providing decision support functionality through outage prevention and prediction.

DATA FAN will contribute to anomaly detection through the analysis of real-time data streams and reliability assessment.

Ganimede is the main tool in the S4RIS platform for real-time monitoring and analysis of CCTV data streams. Ganimede will utilize deep learning techniques for offering intelligence to the platform and will communicate alerts, results and important information to tools in the Decision Support Layer.

WINGSPARK is a monitoring platform that can receive data from multiple sensors and apply anomaly detection techniques along with infrastructure and resilience analysis. WINGSPARK uses Big Data technologies to store and process sensor data enabling long-term analysis of datasets for further insights.

The tools discussed above are mostly focused in real-time monitoring and data processing. In S4RIS platform there are also other tools that provide offline data processing capabilities such as through the functionality of simulating various risk scenarios provided by **SecuRail.**

Tools in the Data Processing Layer will continuously make use of the Information Exchange Layer for information exchange between other tools in the same or other layers. Information flow in the S4RIS platform will then propagate to the Decision Support / Application Layer.

3.7 Decision support / Application layer specification

The Decision Support / Application Layer involves tools that provide decision support capabilities to end-users through the respective tool interfaces. More specifically responsibilities in this layer include:

- Retrieval of the data from Data Processing layer
- Further processing of that data for generating decision support suggestions
- Provision of offline Simulation Tools for decision support
- User Interfaces for tools in the S4RIS platform along with a unified S4RIS GUI tool for easily accessing the different tool interfaces

Tools in the S4RIS platform with an important role in the Decision Support / Application layer are:

RAM² is a decision support platform that will be constantly consuming data from real-time monitoring tools such as CuriX. RAM² is able to analyze data and provide mitigation options to end-users through the tools' web interface.

SecuRail is a risk assessment platform for the railway sector able to perform quantitative and qualitative analysis on real-time data coming from sensors. SecuRail is able to generate attack scenarios and execute them providing useful analysis and insights with regards to risks concerning railway infrastructure.

Simulation tools in the S4RIS platform will also play an important role in the Decision Support Layer, more specifically:

iCrowd Simulator supports the simulation of scenarios in relation with human crowd behavioral modelling, such as railway station evacuations, and provides end-users with insights with regards to optimizing evacuation routes and important performance metrics related to safety measures assessment.

CaESAR provides cascading effects simulation within grids and across grid borders to assess and enhance the resilience of critical infrastructures in urban areas**.** It will assist end-users to find optimized strategies for the mitigation of hazard impact on inter-connected grids.

Bomblast3d supports simulation of explosions in order to assist end-users by simulating the effects of blasts and providing relevant metrics thereby allowing end users to further increase railway station security.

CAMS is a tool that analyzes assets which can include materials and equipment. CAMS is able to apply asset degradation simulation techniques in an attempt to notify end-users with regards to components that might fail thus preventing failures and possibly avoiding accidents.

An important part of the S4RIS platform is interaction with end users. Most of the tools in the platform already provide an interface through a Web browser or standalone application. In order to alleviate the need for users to open each tool GUI separately the S4RIS platform will provide means to allow users access to the various tool interfaces. The **S4RIS GUI** is a tool that links all the different user interfaces by providing a central point for end-users to access most tool interfaces in the form of links. This provides end-users a unified way to access functionality and information in the S4RIS platform.

3.8 SAFETY4RAILS Platform Security and Deployment

SAFETY4RAILS will employ a concrete approach with regards to security based on certain principles as outlined below. Primarily specific network infrastructure and security tools in the platform will provide security and monitoring functionalities for the S4RIS platform network. These include tools such as SecaaS, uniMS and RAM2 which provide real-time monitoring capabilities for detecting malicious threats. With regards to information that is received from external sources such as sensors or raw user data, PRIGM and Senstation are components that will be responsible for ensuring security of information in transit from sensors to the S4RIS platform. Finally, all tools in the SAFET4RAILS platform will apply industry security best-practices for the development and deployment of applications. As part of the definition for a concrete security framework for the S4RIS platform it is important that for all tools/components the following apply:

- Encrypted communication of information during transit
- Authentication and authorization capabilities where applicable
- Ethical compliance with regards to data exchange and storage
- Detailed logs allowing tracing of events and debugging

- Appropriately configured environments and network infrastructure
- Software configuration according to latest security best practices

It is crucial to ensure that the above criteria are addressed in the course of all the development and testing processes of the tools supporting the platform. This will further ensure the reliability and security of the platform. Moreover, as specific S4RIS platform prototypes will be deployed for each pilot/use-case this will allow further practical assessment of the security of the platform during the project aiming to reach TRL of 7 by the end of the project [17].

3.9 SAFETY4RAILS Platform Prototypes

The Concept Architecture approach presented in this document takes a flexible perspective with regards to platform components and different data providers from real-time monitoring sensors to legacy system integration and external databases. During the project, the aspiration is the development of the S4RIS platform as a product that can adapt to specific use-case needs. Throughout the pilots different S4RIS prototype versions will be deployed. In practice this means that for each pilot the platform will be configured differently, to support a set of diverse needs and scenarios, with regards to:

Sensors / **Input Data:** For each pilot/use case there needs to be a definition of the exact data available to be exploited by the different tools in the platform. This includes the definition of hardware sensors that provide input but also the use of synthetic data that resembles realistic sensor output. In cases where real data is not available or cannot be provided then the usage of synthetic data that resembles the real data format and structure will be implemented.

Integration with external systems: For some use cases there might be systems available from end users that can provide further useful information to the S4RIS platform increasing risk assessment and decision support capabilities. These systems include API's, applications and external databases which will have to be integrated to the platform. Depending on the nature of the external system an appropriate method of integrating will be followed. In the case of external databases this could be a direct connection to the database whereas in the case of applications there could be API integration if the application does provide one.

Tools / **Components:** Depending on the data available from Sensors, Synthetic Data and Integration with External Systems the subset of the S4RIS platform tools in use per pilot may differ. Different tools or components will be enabled at each specific pilot / use case depending on specific data availability, systems integrated and needs to be addressed.

4. Conclusion

4.1 Key conclusions and outcomes

This deliverable deals with the presentation of the System Specifications and the definition of the Concept System Architecture for the S4RIS platform. SAFETY4RAILS is a project aiming to integrate a large number of software systems providing a seamless experience to end-users (railway/metro control room staff, security/crisis management operators) with regards to risk assessment and decision support functionality.

There are a number of challenges involved in the process of defining a Concept System architecture ranging from modest challenges such as the heterogenous nature of systems to challenges that require sophisticated solutions. A prime example being the definition of how different end-users will configure the S4RIS platform in a diverse manner according to their needs and provide different sets of data as input. These challenges were the driving force behind the approach of defining a flexible and modular Concept System Architecture for the S4RIS platform that outlines how tools interact with each other. The S4RIS architecture specification follows an abstraction layer approach allowing for a clear separation of concerns and a simpler reasoning of the overall system while enabling flexible platform configuration for different use cases.

Following such a flexible approach is of great importance for the SAFETY4RAILS project and the S4RIS platform as it enables the platform to dynamically adapt in different pilots/use cases with regards to:

- S4RIS platform tools used
- Integration with third-party systems
- Different sensors and user input data
- User Interface

All of the above were made possible by the careful examination of the user requirements gathered from other tasks and by information made available from the various tool providers with regards to the functionality and system specifications of the software systems provided. Work carried under this deliverable also helped various tool providers further define changes and new system specifications that need to be developed in the SAFETY4RAILS project.

4.2 Future work

Since the S4RIS platform Concept System Architecture provides a flexible approach, it is of great importance that future work in other tasks and work packages will take this into consideration and make decisions accordingly. More specifically work that will be carried out in “WP6-Implementation of SAFETY4RAILS Information System” and “WP8-Simulation Exercises and Evaluations in Operational Environments” which is concerned with integration, pilot design and execution will need to clearly define for each use-case the configuration and the setting for the S4RIS platform. This entails clear communication between technical partners and end-users for each specific use-case. It is important to identify at an early stage the need for specific third-party integration with end-user systems or specific user input and sensor data.

This deliverable should be used by technical partners and end-users as a reference for the Concept System Architecture of the S4RIS platform providing information into how different components interact and their specific role in the platform. Moreover, it should act as a reference in terms of the functionalities, input and output capabilities provided by the different tools in the platform.

BIBLIOGRAPHY

[1] European Commission, *SAFETY4RAILS Grant Agreement*, version 1.0, dated 21 April 2020.

[2] Microsoft Application Architecture guide on "N-tier architecture style", [Online]. Available: https://docs.microsoft.com/en-us/azure/architecture/guide/architecture-styles/n-tier [Accessed 27 04 2021]

[3] Layered Architecture Sample for .NET, [Online]. Available: https://archive.codeplex.com/?p=layersample [Accessed 27 04 2021]

[4] Intro to Apache Kafka, [Online]. Available: https://kafka.apache.org/intro [Accessed 27 04 2021]

[5] Dobbelaere, Philippe, and Kyumars Sheykh Esmaili. "Kafka versus RabbitMQ: A comparative study of two industry reference publish/subscribe implementations: Industry Paper." In Proceedings of the 11th ACM international conference on distributed and event-based systems, pp. 227-238. 2017.

[6] "IEEE Guide for Developing System Requirements Specifications," in IEEE Std 1233, 1998 Edition, vol., no., pp.1-36, 29 Dec. 1998, doi: 10.1109/IEEESTD.1998.88826.

[7] Intracom-Telecom uni|MS™ Wireless Network System, [Online]. Available: http://www.intracom-telecom.com/en/products/wireless_network_systems/netw_manag_systems/unimsNetwork.htm [Accessed 22 05 2021]

[8] Intracom-Telecom SISC2 solution, [Online]. Available: http://www.intracom-telecom.com/en/products/ict_services_solutions/sis/cip.htm [Accessed 22 05 2021]

[9] Intracom-Telecom SecaaS solution, [Online]. Available: http://www.intracom-telecom.com/en/products/ict_services_solutions/cloud/SecaaS.htm [Accessed 22 05 2021]

[10] RAM² tool by Elbit Systems, [Online]. Available: https://www.otorio.com/platform [Accessed 18 05 2021]

[11] CORDIS | European Commission (europa.eu), "Passenger station and terminal design for safety, security and resilience to terrorist attack | SECURESTATION Project," [Online]. Available: https://cordis.europa.eu/project/id/266202. [Accessed 22 05 2021]

[12] CAMS Central Asset Management System by RMIT, [Online]. Available: http://www.assethub.com.au/Default.aspx [Accessed 18 05 2021]

[13] CuriX Cure Infrastructure in XaaS by IC-Information, [Online]. Available: https://www.curix.ch [Accessed 18 05 2021]

[14] CaESAR Cascading effect simulation to assess and increase resilience by Fraunhofer EMI, [Online]. Available: https://www.emi.fraunhofer.de/de/geschaeftsfelder/sicherheit/forschung/analyse-von-kaskadeneffekten-in-versorgungs--netzen--softwaretoo.html [Accessed 18 05 2021]

[15] Ganimede platform by Leonardo, [Online]. Available: https://www.leonardocompany.com/documents/20142/119826/GANIMEDE+platform+LQ+%28mm09022%29_set19.pdf?t=1572444983962 [Accessed 18 05 2021]

[16] CORDIS | European Commission (europa.eu), "Internet Forensic platform for tracking the money flow of financially-motivated malware | RAMSES Project," [Online]. Available: https://cordis.europa.eu/project/id/700326. [Accessed 22 05 2021]

[17] European Commission, "HORIZON 2020 – WORK PROGRAMME 2014-2015 General Annexes, G. Technology readiness levels (TRL)," [Online]. Available: https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf [Accessed 18 05 2021]

[18] Kountouriotis, Vassilios I., Manolis Paterakis, and Stelios CA Thomopoulos. "iCrowd: agent-based behavior modeling and crowd simulator." In Signal Processing, Sensor/Information Fusion, and Target Recognition XXV, vol. 9842, p. 98420Q. International Society for Optics and Photonics, 2016.

[19] Kountouriotis, Vassilios, Stelios CA Thomopoulos, and Yiannis Papelis. "An agent-based crowd behaviour model for real time crowd behaviour simulation." Pattern Recognition Letters 44 (2014): 30-38.

ANNEXES

ANNEX I. GLOSSARY AND ACRONYMS

TABLE 1 GLOSSARY AND ACRONYMS

Term	Definition/description
S4RIS	SAFETY4RAILS Information System
API	Application Programming Interface
GTD	Global Terrorism Database
RAND	Database of Worldwide Terrorism Incidents
CAPEX	Capital Expenditure
OPEX	Operational Expenditure
HSM	Hardware Security Module
AES	Advanced Encryption Standard
3DES	Triple Data Encryption Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
RSA	Rivest–Shamir–Adleman public-key cryptosystem
SHA	Secure Hash Algorithm
OCC	Operation Control Centre
JSON	JavaScript Object Notation
XML	Extensible Markup Language
SQL	Structured Query Language
CSV	Comma Separated Values
GUI	Graphical User Interface
REST	Representational State Transfer

VM	Virtual Machine
IT	Information Technology
OT	Operational Technology
IoT	Internet of Things
TCP	Transmission Control Protocol
IP	Internet Protocol
UDP	User Datagram Protocol
CCTV	Closed-circuit Television
DMS	Distributed Messaging System
CLI	Command Line Interface
RTSP	Real Time Streaming Protocol
TRL	Technology Readiness Level
MISP	Malware Information Sharing Platform

SAFETY4RAILS

Partners:

Fraunhofer EMI
UIC
Metro de Madrid
EGO Genel Müdürlüğü
RFI Rete Ferroviaria Italiana – Gruppo Ferrovie dello Stato Italiane
Leonardo
ceis avisa partners
STAM Mastering Excellence
TCDD
information company
RMIT University
University of Reading
etra I+D
Demokritos National Centre for Scientific Research
RINA
WINGS ICT Solutions
Newcastle University
EOS European Organisation for Security
Innova Integra
LAUREA Ammattikorkeakoulu University of Applied Sciences
CybeServices Made in Europe
erGE
FGC Ferrocarrils de la Generalitat de Catalunya
MTRS
INTRACOM TELECOM
Universitas Fernández
TREE Technology
Elbit Systems C4I and Cyber
ProRail
Comune di Milano

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