SAFETY4RAILS

Final developmental validation and evaluation of the S4RIS system

Deliverable D6.4

Lead Author: LDO

Contributors: LDO, RINA-C, RMIT, NCSRD, STAM, CuriX, WINGS, Fraunhofer, TREE, ELBIT, ICOM, ERARGE, UNEW

Dissemination level: PU - Public

Security Assessment Control: passed

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

D6.4 Final developmental validation and evaluation of the S4RIS system	
Deliverable number:	6.4
Version:	1.8
Delivery date:	23/09/2022
Dissemination level:	PU - Public
Nature:	Report
Main author(s)	LDO
Contributor(s) to main deliverable production	Fraunhofer LDO STAM RMIT RINA-C NCSRD WINGS UNEW ERARGE ICOM TREE ELBIT CuriX
Internal reviewer(s)	Fraunhofer (including security assessment)
External reviewer(s)	*Input to future work*

Document control			
Version	Date	Author(s)	Change(s)
1.0	30/09/2021	LDO	Document structure and test schema.
1,1	09/07/2022	LDO, RINA-C, RMIT, NCSRD, STAM, Fraunhofer	Inclusion of sections related to BB3d, CAMS, Ganimede, iCrowd, SARA, DATAFAN and SECURAIL
1.2	13/07/2022	CuriX, WINGS, Fraunhofer; TREE	Inclusion of sections related to Wingspark, CAESAR, TSAIL, and CuriX.
1.3	15/07/2022	Elbit, ICOM	Inclusion of sections related to RAM2, SecaaS, SISC2, uni|MS™, WIBAS.
1.4	25/07/2022	ERARGE, LDO	Inclusion of sections related to PRIGM and Senstation. Review related to Project Coordinator comments.
1.5	29/08/2022	LDO, all tool providers + UNEW	Contributions related to data used for tests. New section “S4RIS Platform”
1.6	14/09/2022	Fraunhofer, LDO, UNEW, RINA.	Updates from UNEW on GUI test details. Acceptance of all tracked changes (in V1.5.1) provided to project coordinator. Review, editing and drafting of further text by Fraunhofer as coordinator. Addition of SARA test data details.
1.7	15/09/2022	Fraunhofer	Creation of 1.7 from 1.6 with acceptance of all earlier tracked changes, insertion of deliverable details page (page 2) and abstract page (page 3), in Annex IV addition of OSINT and Blockchain testing under WP4, reordering of Annexes, minor edits, removal of comments and formatting.
1.8	23/09/2022	Fraunhofer	Updates: Front cover, this table, Figure 8 reference, Annex II redaction, CAMS comments in Annex IV.

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 2004) and combined cyber-physical attacks, which are important emerging scenarios given increasing IoT infrastructure integration.

SAFETY4RAILS concentrates on rush hour rail transport scenarios where many passengers are using metros and railways to commute to work or attend mass events (e.g. large multi-venue sporting events such as the Olympics). When an incident occurs during heavy usage, metro and railway operators have to consider many aspects to ensure passenger safety and security, e.g. carry out a threat analysis, maintain situation awareness, establish crisis communication and response, and they must 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 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 figures

List of tables

Executive summary

This document represents a report for laboratory tests on the functionalities of the main components and contributory tools that form the S4RIS platform.

The aim is to validate the S4RIS platform and contributory tool functions respect to the specifications derived from the requirements described in deliverable D1.4

For each main component and tool will be provided a short description, the indication of Development and Quality standards and the list of tests done using the test methodology described in section 1.2.

1. Introduction

1.1 Purpose

This Deliverable provides the description of the test carried out on the S4RIS platform and its contributory tools.

The scope was to perform a technical evaluation and validation of the S4RIS platform that has a different meaning with respect to the evaluations that were done in WP8.

The evaluation in task T6.4 was only with the technical developmental partner participation (not end-users) and served as input (and documentation) for the targeted end-user evaluation and validation in WP8 and following the project.

In task T6.4 the S4RIS platform and each of its contributory tools have been evaluated and as far as possible validated (in laboratory) against the specifications derived from the requirements listed in the deliverable D1.4 sections 2.2 and 2.3.

1.2 Test methodology

The S4RIS platform validation of tool requirements will be based on a schema (Test Data Report) that reports test activities made for each tool in relation to requirements described in D1.4 sections 2.2 and 2.3.

The schema includes the following elements:

- ***Unique Test Id*** (Tool-Id + Test Number)
- ***Addressed Requirement and accordingly derived specifications***: the requirement(s) and the specification(s) derived from them addressed in the test (from D1.4)
- ***Hardware preparation****:* needed procedures to prepare hardware for the test (if applicable)
- ***Software Preparation****:* needed procedures to prepare item under test and any related software (if applicable)
- ***Test Inputs****:* input data for the test
- ***Test Procedure****:* defined test procedure for the test case. The test procedure is defined as a series of individually numbered steps listed sequentially in the order in which the steps are to be performed, containing (if applicable) information about
  test operator actions and equipment operation required for each step
- ***Expected Test Result****:* list of all expected test results
- ***Pass/fails****:* This field reports the test evaluation:
  PASSED = all results as expected
  PASSED WITH DEVIATIONS = In case of Passed with deviations it's necessary to provide information about the deviation.
- ***Encountered Problems****:* problems encountered which have caused test failure and their severity

2. S4RIS Core Platform

2.1.1 Overview

The S4RIS core platform is an online platform for cyber-physical security implemented in the SAFETY4RAILS project. It is designed to integrate software tools into a single platform by enhancing the usability through ensuring that (a) the data exchange includes data protection for sensitive information and (b) interoperability enables seamless links between software providers and end users.

The S4RIS core platform main components includes:

- an Activation portal based on Graphical User Interface (GUI) to enable end users adapt the platform to their own needs to provide protection for critical infrastructure in real time.
- a data exchange Distributed Message System (DMS) designed to allow efficient and secure data sharing among different software providers and stakeholders, thereby facilitating the best user experience.
- the following tools to be considered as initial contributory tools (not all software):

TABLE 1 S4RIS PLATFORM TOOLS

Tool Nr.	Tool short name	Tool provider
1	BB3d	RINA-C
2	CaESAR	Fraunhofer
3	CAMS	RMIT
4	CuriX	CuriX
5	DATA FAN	Fraunhofer
6	Ganimede	LDO
7	iCrowd	NCSRD
8	PRIGM	ERARGE
9	RAM²	ELBIT
10	SARA	RINA-C
11	SecaaS	ICOM
12	SECURAIL	STAM
13	Senstation	ERARGE
14	SISC2	ICOM
15	TISAIL	TREE
16	uni|MS™	ICOM
17	WIBAS	ICOM
18	WINGSPARK	WINGS

S4RIS was developed to enhance the end user experience using multiple tools in the same environment. In its development, two phases were required to achieve software integrations.

Firstly, user requirements were identified aiming at creating a user-customised platform experience. Secondly, application interfaces were created connecting each third-party tool connected within the project.

The S4RIS has been tested with a number of different configurations scenarios with end users to ensure that the right features, functionality, and performance are in place.

2.1.2 Development and Quality Standards

No specific software development and/or quality standard adopted. However, the main S4RIS specific platform components are implemented with well-established technologies, namely for the GUI Wordpress[1] and for DMS Apache Kafka[2] as described in D6.5.[3]

2.1.3 S4RIS core platform Test Data report (focused on activation portal)

This section reports the tests executed for S4RIS core platform, based on a sub-set of requirements/specifications described in D1.4 par. 2.2.3 (Graphical User Interface – GUI).

Test - ID	S4RIS_TR_01
Addressed Requirement	GUI-R01 S4RIS shall have a web-based interface.
HW/SW preparation	1 - An initial local installation of the S4RIS platform was developed offline as a version to ensure the profile creation and integration was operational. 2- Private domain with S4RIS platform online version 3- Testing with different web browsers: Firefox, Chrome, Opera, Brave, Explorer, Safari
Test inputs	Time response
Test procedure	Step 1: Access the S4RIS platform address Step 2: Check the time response and main functionalities
Expected Results	Fully operational with different web browsers.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test - ID	S4RIS_TR_02
Addressed Requirement	GUI-R02 When S4RIS interface is opened and the user is not already logged-in, only a log-in page shall be displayed.
HW/SW preparation	1- Initial version of S4RIS with only the log-in page displayed. 2- Second version of the platform with the private area log-in required and (S4RIS) and with public interface with information about the project
Test inputs	Access without logging in
Test procedure	Step 1: Creation of profiles with password Step 2: Try to connect without the passwords from different machines
Expected Results	Block the users to access s4ris / private are of s4ris without logging
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test - ID	S4RIS_TR_03
Addressed Requirement	GUI-R03 Single point of access to the tools. It shall be possible to launch the tools that need user interaction from a single interface (the home page). "One page of the S4RIS GUI shall provide an overview of all available tools in form of a list or table. Each tool should be depicted by an icon or an example screenshot. "

[1] https://wordpress.org/
[2] https://kafka.apache.org/
[3] D6.5 S4RIS system with an online platform dedicated to training and what-if scenarios, including GUI

HW/SW preparation	Description of tools and icon are requested from took providers Buttons with the description and icons are created Redirection or connection were implemented
Test inputs	Redirection / Connection
Test procedure	Step 1: Creation of buttons and redirection scripts Step 2: Access the tools/ database Step 3: Retrieve and visualize data in the GUI or in new tab the tools
Expected Results	Access to the tools within S4RIS or in a new tab
Pass/Fail	Pass for those tools tested.
Deviation Encountered	Not all tools listed in Table 1 presently connected/accessible
Problems	
Comments	

Test - ID	S4RIS_TR_04
Addressed Requirement	GUI-R04 "The tools shall be visually grouped into at least four areas: risk assessment, prevention and mitigation, detection and response, planning and investments. "
HW/SW preparation	Used the alternative solution / variant allowing the user to configure the groups according to their own needs
Test inputs	Group configurations/ creation
Test procedure	Step 1: Creation of group Step 2: Connect the required tools into the specific group / database Step 3: Access the group and visualise data in the GUI
Expected Results	Allow user to create, delete and edit existing group
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	Demonstrated for tools used in SEs.

Test - ID	S4RIS_TR_05
Addressed Requirement	GUI-R05 How to launch tools. "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. " Detailed specification: *“For each tool there should be a clickable link that opens the tool in one of the following possibilities:* • *Navigate to the web GUI of the selected tool (within the S4RIS GUI or open another tab / browser window)* • *Open the respective tool on the client machine via an executable file* • *Open a web page that provides access to a remote machine in which the tool can be executed* *Tools that are used in a one-shot manner and are not meant to run permanently need to assure that required data is available. One of the following three possibilities can be followed by each tool:* • *request manual input of required data (via upload possibilities or forms)* • *retrieve data over parameters provided via the open link within S4RIS* • *having a permanently running program that observes KAFKA and stores relevant files in an accessible folder of the respective tool* *Results of stand-alone tools shall be sent over KAFKA if those results will be processed by other tools within S4RIS; if results are meant to be directly communicated to the user they will be provided by standard means (e.g. own GUI of tool, result file, email, etc.)”*

HW/SW preparation	Button with icons were created and tested in different browsers
Test inputs	Readability
Test procedure	Step 1: Creation of icons for the buttons Step 2: Readability test
Expected Results	Able to be read from different browsers and with different contrast levels
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	Full specification test(s) not reported on here.

Test - ID	S4RIS_TR_06
Addressed Requirement	GUI-R06 Display of tools based on user role. "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. "
HW/SW preparation	1 Group profiles were created with different authorization levels requirements 2 Multiple user profiles with different authorization levels
Test inputs	Access
Test procedure	Step 1: Creation of profiles with different authorisation Step 2: Profile approvals Step 3: Testing if were possible access groups with different authorization permissions
Expected Results	Deny access for non-authorised profiles.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test - ID	S4RIS_TR_07
Addressed Requirement	GUI-R07 "A set of keywords and/or a short description, aimed to describe the tool main functionalities, shall be displayed for each tool. "
HW/SW preparation	Functionalities and tools description were created
Test inputs	Creation, deletion and editing on tool description
Test procedure	Step 1: Creation of data, directly using WordPress Step 2: Editing and deleting the descriptions
Expected Results	The user should be able in the GUI to create and edit the description created
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	Actual descriptions subject to update.

Test - ID	S4RIS_TR_08
Addressed Requirement	GUI-R08 A log-out button shall be present in the right-top angle of each page (login page is excluded).

HW/SW preparation	Login buttons were created and saved as a template for all the pages
Test inputs	Pages
Test procedure	Visit all the pages in the platform to check the existence of the login button
Expected Results	Login button in all pages
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test - ID	S4RIS_TR_09
Addressed Requirement	GUI-R09 "S4RIS logo shall be displayed in the left-top angle of each page and shall work as a ""home"" button (Login page is excluded). "
HW/SW preparation	S4RIS logo s were created and saved as a template for all the pages
Test inputs	Pages
Test procedure	Visit all the pages in the platform to check the existence of S4RIS logo
Expected Results	S4RIS logo in all the pages
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test - ID	S4RIS_TR_10
Addressed Requirement	GUI-R10 "It shall be possible for the user to manage its account and change its password in a dedicated page, accessible from the home page. "
HW/SW preparation	Profile page were created
Test inputs	
Test procedure	Step 1: Creation of profiles Step 2: Visit the profiles page Step 3: Change password
Expected Results	The used should be able to change their password directly from S4RIS user profile page.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test - ID	S4RIS_TR_11
Addressed Requirement	GUI-R11 "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. "
HW/SW preparation	Setting dedicated page creation
Test inputs	
Test procedure	Access the setting page and change the configuration
Expected Results	Be able to change the setting configurations

Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	As it stands the end-user does not see the settings page.

Test - ID	S4RIS_TR_12
Addressed Requirement	GUI-R12 "It shall be possible to change the displayed language. At least the following languages should be supported: • English. • Italian. • Spanish. • Dutch. • Turkish."
HW/SW preparation	Multilingual alternative solutions were created
Test inputs	
Test procedure	Step 1: Creation of alternative version of the page/ group with different language option Step 2: Redirect to translated version of the tool Step 3: Retrieve and visualize data in the GUI or for analytics purposes
Expected Results	Be able to redirect to a translated version of the tool in the database.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	Compared to D1.4 comments on requirement: not each individual tool demonstrated for at least two different languages.

Test - ID	S4RIS_TR_13
Addressed Requirement	GUI-R13 A sidebar (preferred) or a top bar should be present in the home page and should provide buttons to access the following: - password management (GUI-R10); - settings and configuration (GUI-R11), if implemented; - language selection (GUI-R12); - help, if implemented (GUI-R21).
HW/SW preparation	Used the alternative solution
Test inputs	Data acquisition for a day and extrapolation to fit a duration of approximately a month for each position
Test procedure	Creation of top bar with different groups and within each group the required tools
Expected Results	The users should be able to access the tools in the different groups created.
Pass/Fail	Pass
Deviation Encountered	Test demonstrated possibility to access tools grouped under a specific heading e.g. a Simulation exercise location. Full specification not tested.
Problems	
Comments	

Test - ID	S4RIS_TR_14
Addressed Requirement	GUI-R14 When tools with web-based GUI are launched, they shall be opened in another tab or window of the browser.
HW/SW preparation	Iframa option and new tab options were created for the different tools
Test inputs	
Test procedure	Step 1: Creation of group with different tools opening in the new tab Step 2: Create iFramed option inside S4RIS Step 3: Check each tool if the readability inside the tool and user interface is compromised
Expected Results	The users should be able to config the opening preferences according to their own needs.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	Demonstrated for tools with web application.

Test - ID	S4RIS_TR_15
Addressed Requirement	GUI-R15 When tools with desktop application are launched, the desktop application itself shall be launched.
HW/SW preparation	Virtual Machine with the desktop tool installed were investigated
Test inputs	
Test procedure	Step 1: Creation of virtual machine with the tool Step 2: Access to the virtual machine from S4RIS
Expected Results	Connecting to the virtual machine directly from S4RIS
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

2.1.4 Test Results Consideration

S4RIS activation portal tests focussed on the profile creation, interconnection of the tools into the platform, and creation of a user specific experience. It was tested and demonstrated in 4 scenarios listed below:

- Madrid – Integration of RAM2, Curix, SecuRail and CAMS
- Ankara - Integration of RAM2, Curix, SecuRail, CAMS, TISAIL, GANIMEDE and DATAFAN (DMS only)
- Rome - Integration of RAM2, Curix, SecuRail, CAMS, TISAIL, WINGSPARK, CAESAR, GANIMEDE/SC2 +DATAFAN (DMS)
- Milano - Integration of Ram2, Curix, SecuRail, CAMS, TISAIL, WINGSPARK, CAESAR, +DATAFAN (DMS)

Feedback provided by end users in the 4 scenarios helped improve the interface and the integration of the tools in accordance with the end user needs and preferences.

3. S4RIS Tools Test Data Report

3.1 BB3d

3.1.1 Overview

BomBlast3d (BB3d) computes the loading due to a blast wave impact over structures such as buildings, and supplies the main physical quantities of interest both over the wall surface of three-dimensional models (e.g.), virtually reproducing potential attractive targets for terrorists, and in air.

These results can be visualised and used to support blast analysists' assessment and decision makers.

3.1.2 Development and Quality standards adopted

RINA adopts the following Quality Standards:

- ISO 31000 - The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome).
- ISO Guide 73:2009 - Risk can be defined as the combination of the probability of an event and its consequences.
- NFPA 130 - Standard for Fixed Guideway Transit and Passenger Rail Systems.

No specific software development and/or quality standard adopted.

3.1.3 Data used for tests

The description of types, sources, amount and number of time test performed dealing with BB3d follows:

- **Types**: main data consists of 3D Computer-Aided Design (CAD) models of urban areas to study and information on the explosive charge (i.e. type of high-detonation explosive, mass of the charge and location of the explosion).
- **Sources**: the 3D CAD models of urban areas, needed to analyse blast scenarios, were generated from scratch using Computer-Aided Engineering (CAE) commercial software of the ANSYS suite and exploiting the features of the Google Maps application. To assign the data concerning high-detonation explosives, online and literature data were considered.
- **Amount**: two complex 3D CAD models were created. The first refers to an area in Madrid (Spain) which includes a sporting stadium whilst the second to an area in Rome (Italy), including an important train station.
- **Number of time test performed**: 6 fully blast scenarios (5 for the Spanish use case and 1 for the Termini station test case) were fully analysed and described in different deliverables that were issued. Hundreds of tests were performed for developing, debugging and testing (e.g. computing performance) all the features and capabilities of BB3d implemented during the project.

3.1.4 Test Data Report

This section reports the tests executed for BB3d, based on requirements described in D1.4 par. 2.3.1. An extensive description of the features and enhancements implemented during the project is present in Deliverable 5.4.

Test.-ID	BB3d_TR_01
Addressed Requirement	BB3d_01 **Bomb blast loading** •Predict the blast loads and the main blast quantities due to a high-explosive bomb attack (i.e. physical attack) in a wide range of possible scenarios, taking

	into account areas with an extension of a small neighborhood or a big crucial infrastructure. The code was developed to properly predict the structural damages on buildings, taking into account a wide range of charge possible dimensions, from a suitcase to a full explosive van. Such data are provided over the solid surfaces of interest (e.g. buildings' facades) and in a predefined volume around them (virtually filled by air). •Support blast designers and safety experts for carrying out studies of outdoor non-confined blast scenarios due to a bomb attack.
HW / SW preparation	BB3d executable available.
Test inputs	Madrid Use Case model (STL format) and BB3d input file.
Test procedure	Step 1: Perform a set of BB3d analyses. Step 2: Assessment of the ASCII output files generated. Step 3: Visualization of blast results using Paraview.
Expected Results	Depending on the settings of the BB3d's input file, generation of ASCII output files and VTK files to be visualized using Paraview.
Pass/Fail	Pass
Deviation Encountered	No
Problems	No
Comments	-

Test.-ID	BB3d_TR_02
Addressed Requirement	BB3d_02 **Bomb blast usability** • Ease the usability of the tool for the user • Stability in computing • Robustness in data processing
HW / SW preparation	BB3d executable available.
Test inputs	Madrid Use Case model (STL format) and BB3d input files.
Test procedure	Step 1: Perform a set of BB3d analyses. Step 2: Assessment of the ASCII output files generated.
Expected Results	To ease the usability of the tool for the user, one single input file and one single computing stage were suitably designed and implemented. To make more user-friendly the interaction with BB3d, the generation of a set of supporting files was implemented while the external data of blast was hardcoded. The stability in computing is guarantee by the use and processing of experimental data.
Pass/Fail	Pass
Deviation Encountered	No
Problems	No
Comments	-

Test.-ID	BB3d_TR_03
Addressed Requirement	BB3d_03 **Bomb blast damage and casualties** Predict the physical damage for the asset and casualties

HW / SW preparation	BB3d executable available.
Test inputs	Madrid Use Case model (STL format) and BB3d input file for the different blast scenarios.
Test procedure	Step 1: Perform a set of BB3d analyses. Step 2: Assessment of the ASCII output files generated concerning both indoor and outdoor damage model. Step 3: Visualization of blast results using Paraview (structural damage level for indoor damage model and survival probability for outdoor damage model).
Expected Results	For each blast scenario calculation of: • number of casualties and people injured for persons near the location of explosion (outdoor damage model) • number of casualties and people injured for persons present in building(s) when the bomb attack occurs (indoor damage model) • structural damage level
Pass/Fail	Pass
Deviation Encountered	No
Problems	No
Comments	-

Test.-ID	BB3d_TR_04
Addressed Requirement	BB3d_04 **Bomb blast computing performance** • Enable an efficient management of large dataset (e.g. whole train station) to ease the analysis of different blast scenarios in function of bomb explosion location • Time needed to accomplish a single analysis
HW / SW preparation	BB3d executable available.
Test inputs	Italian Station model (STL format) and BB3d input file for the different analysed scenarios (sensitivity study).
Test procedure	Step 1: Perform a set of BB3d analyses increasing the value of the processing distance. Step 2: Assessment of the ASCII output files to evaluate the computing performance (advantage provided by the implementation of the cropping feature). Step 3: Run an analysis enabling all features of BB3d and using an adequate value for the processing distance.
Expected Results	The cropping feature is supposed to decrease the computing demand when different blast scenarios have to be analysed using one single large model (e.g. urban area, sensitive infrastructure). The time needed to perform a complete analysis is requested to be lower than 20 minutes.
Pass/Fail	Pass
Deviation Encountered	No
Problems	No
Comments	-

3.2 CaESAR

3.2.1 Overview

CaESAR is a tool to model Critical Infrastructures ((CI) and simulate single/multi-point failures in them to assess resilience of the infrastructure against a combination of physical and cyber-physical threats. As an output, the tool produces the following:

1. Graph based visualization of the network/networks, color coded by their type.
2. Comma separated file with list of nodes in the network, their state (working /failed/percentage operational) and criticality (properties of network graph).
3. In order to visualize the impact, the tool produces resilience curves, representing average state of the components in the network, in the form of graphs, for different threats/scenarios.
4. For different mitigation measures, a meta data file is generated containing rating of these measures using area below the curve.
5. Graphics interchange format visualization displaying propagation of the impact in the network.

The tool is developed as a framework and hence has further capability to consider different impact propagation algorithms to simulate cascades in the network. For further details on the capability of the tool, SAFETY4RAILS project deliverable D5.3 can be referred.

3.2.2 Development and Quality standards adopted

The code for CaESAR is written with an object-oriented approach and uses modern libraries wherever appropriate. For example, all geometric- and projection-related calculations are done using Geo-pandas, network-related interactions such as path finding use NetworkX, matplotlib for GIF generation and Bokeh for all the web-based visualizations.

Furthermore, the code uses a modular structure with following modules:

1. Pre-processor
2. Simulator
3. DMS communicator
4. Post-processor

This type of formatting ensures that input-data is reused, preventing unnecessary pre-processing of the same data and saving the raw simulation-output in order to allow processing them without need to re-run the simulations.

3.2.3 Data used for tests

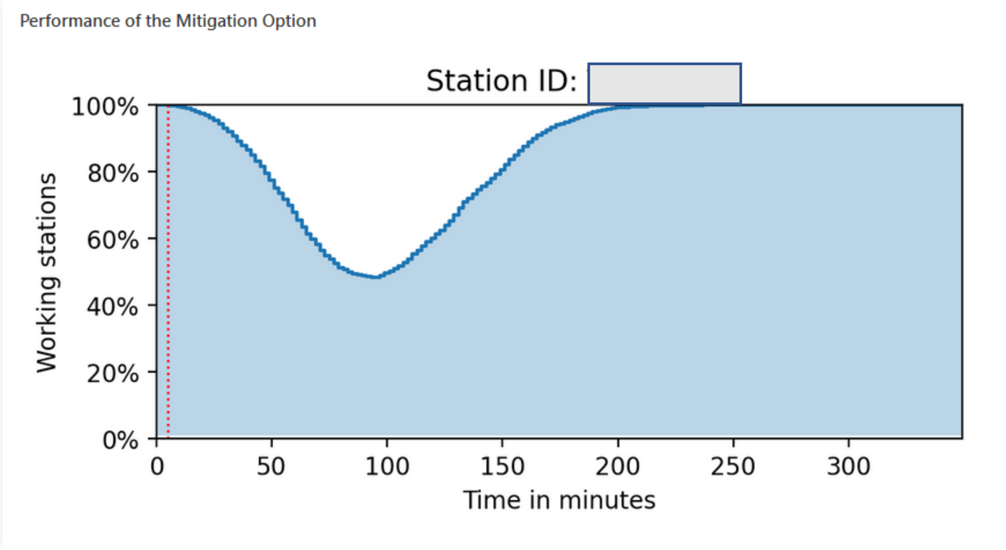
As CaESAR has been developed over the course of different projects, the developments under SAFETY4RAILS project were tested directly with data from the project's simulation exercises. The data used is open-source data available at OpenMobilityData. It is based on The General Transit Feed Specification (GTFS), which is a common format for public transport networks, including schedules and geographic information. This data was filtered to generate input files, which are summarized in ANNEX II Input test data for CaESAR

To further summarize, the input data is in the form of comma separated files (csv) for nodes and edges together forming the grid for the graph network. Configuration for the tool is provided with the help of JSON config file. The tool was tested across the development cycle and tested and demonstrated live in simulation exercises. All the test cases were performed multiple times on different systems to confirm the results.

3.2.4 Test Data Report

This section reports the tests executed for CaESAR, based on requirements described in D1.4 par. 2.3.2. Please note that, since the tool requires inputs in the form of network files, they are not added to the test case descriptions.

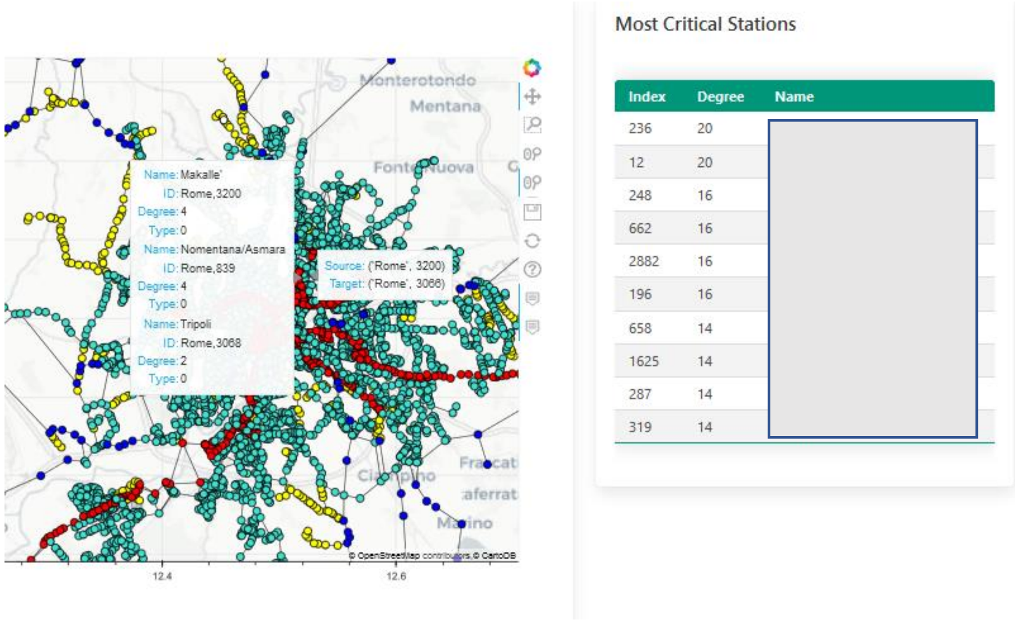
Test.-ID	CaESAR_TR_01
Addressed Requirement	CaESAR_01 **CaESAR should estimate how disruptive events impacts the infrastructure, its components and their functionalities** • Estimate impact failures to single components and their functionalities • Identify remaining functionalities in case of failure
HW / SW preparation	1. Laptop/Computer 2. Firefox/Chrome/Edge web-browser 3. Java Runtime Environment 4. Additionally, for offline version, Python 3.x with following packages: a. Numpy b. Shapely c. Matplotlib d. Geo-pandas e. Openpyxl f. Bokeh g. Cartopy h. Networkx
Test inputs	Graph network file with: 1. Nodes.csv: semicolon separated file with information on nodes (representing stations) in the network and information on their repair times. 2. Edges.csv: semicolon separated file with information on edges (inter-connections) between nodes/stations in the network. 3. Config.JSON: JSON file containing information on points of failures along with time step.
Test procedure	Step 1: Open CaESAR url: https://192.102.163.105/ Step 2: Put the username and password Step 3: In the Simulation section of the page, upload the node, edge and config files. Step 4: Click on 'Simulate' Step 5: After simulation ends, a zip file is generated. Extract the file and results will be present in the form of HTML, .csv, .gif and .png files.
Expected Results	**HTML**: Network in the graphical form with information on nodes and their interconnections. **Resilience curves**: Graph of time-series of average state of stations in the network over time. State is availability of the stations in range [0, 1]. **GIF**: Visualization of impact propagation in the network. **CSV**: Time-series of state of the systems involved in the exercise. CaESAR provides list of working and failed components as a result of the single point failure and cascade. Following is a screen-shot of the result of resilience curve generated from state of components in the network.

	 FIGURE 1: GRAPH SHOWING RESILIENCE OF THE NETWORK IN TERMS OF %WORKING COMPONENTS. THE PROGRESSIVE DECLINE IN THE RESILIENCE IS DUE TO IMPACT PROPAGATION IN THE NETWORK AND GRADUAL IMPROVEMENT IS DUE TO RECOVERY OF INDIVIDUAL COMPONENTS.[4]
Pass/Fail	Pass
Deviation Encountered	In absence of relevant information related to exact functionality of the connected components, CaESAR cannot specifically list remaining functionalities of the components.
Problems	
Comments	

Test.-ID	CaESAR_TR_02
Addressed Requirement	CaESAR_02 CaESAR should identify weak points in the railway/metro system
HW / SW preparation	1. Laptop/Computer 2. Firefox/Chrome/Edge web-browser 3. Java Runtime Environment
Test inputs	Test bed (Railway/Metro grid network) with inter-connections. 1. Nodes.csv: semicolon separated file with information on nodes (representing stations) in the network and their repair times. 2. Edges.csv: semicolon separated file with information on edges (inter-connections) between nodes/stations in the network.
Test procedure	Step 1: Open CaESAR url: https://192.102.163.105/ Step 2: Put the username and password Step 3: In the Simulation section of the page, upload the node, edge and config files. Step 4: Click on ‘Simulate’ Step 5: After simulation ends, a zip file is generated. Extract the file and results will be present in the form of HTML, .csv, .gif and .png files.
Expected Results	In the Overview section of the web-page: 1. Under the section ‘Most Critical Stations’, the list of critical stations based on degree of connectivity and betweenness centrality is presented. This is shown in Figure 2. 2. Under the section ‘What-If Scenarios’, with selective stations, single point

[4] Station ID redacted.

failures are introduced in the network and results are presented in tabular form representing resilience of the network and impact propagation in the network. A comparative graph of resilience of the network for these individual failures is also displayed.



Name: Makalle'
ID: Rome,3200
Degree: 4
Type: 0
Name: Nomentana/Asmara
ID: Rome,839
Degree: 4
Type: 0
Name: Tripoli
ID: Rome,3068
Degree: 2
Type: 0

Source: ('Rome', 3200)
Target: ('Rome', 3068)

Most Critical Stations

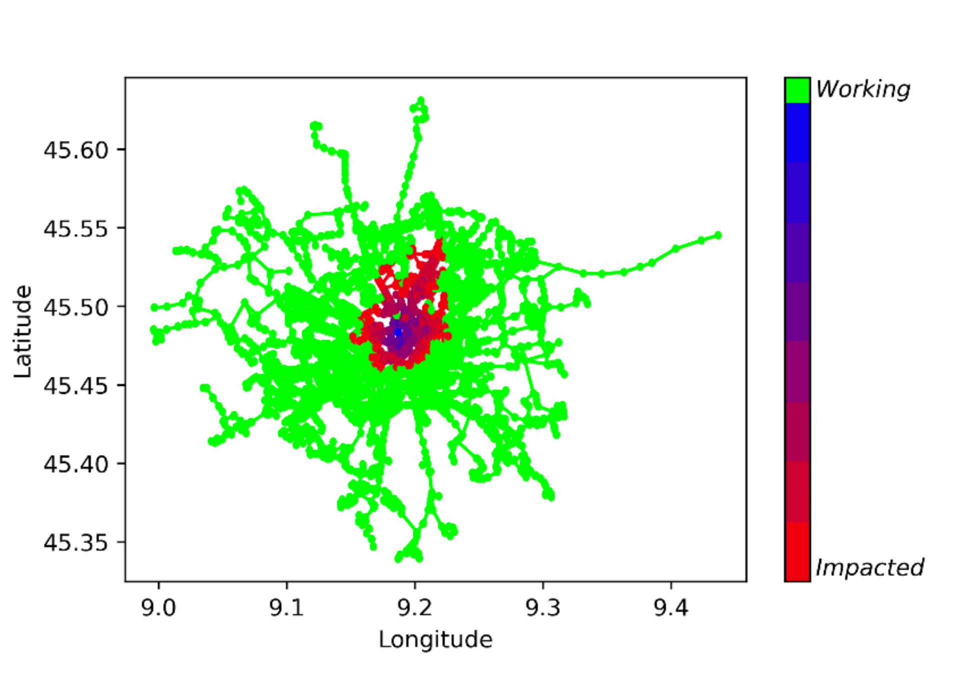
Index	Degree	Name
236	20	[redacted]
12	20	[redacted]
248	16	[redacted]
662	16	[redacted]
2882	16	[redacted]
196	16	[redacted]
658	14	[redacted]
1625	14	[redacted]
287	14	[redacted]
319	14	[redacted]

FIGURE 2: SCREENSHOT OF THE OVERVIEW PAGE WITH ON THE LEFT, INTERACTIVE VISUALIZATION OF THE NETWORK AND ON THE RIGHT LIST OF STATIONS IN DESCENDING ORDER OF THEIR CRITICALITY.[5]

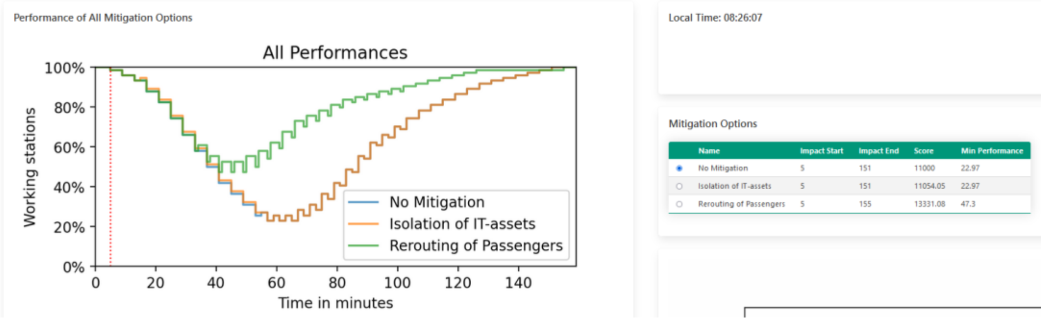
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	Further classification of vulnerable/critical components depends on properties and behavior of the system. This needs to be defined in co-ordination with the end-users.

Test.-ID	CaESAR_TR_03
Addressed Requirement	CaESAR_03 **CaESAR should estimate the propagation of failure caused by disruptive events to from interdependent infrastructures**, i.e : • **From railway to metro** • **From metro to railway** • **Intra propagation metro/railway** • **To other critical infrastructures (power or telecommunication)** • **To other transportation infrastructures (bus)** • Identify how different disruptive events located in one network impact interconnected infrastructures and their resilience • Identify weak points in the interconnections to other systems • Identify consequences of propagation to/from interconnected infrastructures
HW / SW preparation	1. Laptop/Computer 2. Firefox/Chrome/Edge web-browser 3. Java Runtime Environment

[5] Names redacted.

Test inputs	Test bed (Railway/Metro grid network) with inter-connections to relevant CIs (e.g. Bus network, power networks). 1. Nodes.csv: semicolon separated file with information on nodes (representing stations) in the network and their repair times. 2. Edges.csv: semicolon separated file with information on edges (inter-connections) between nodes/stations in the network. 3. Config.JSON: Configuration file with information on the attack on the network, with node number and time of attack.
Test procedure	Step 1: Open CaESAR url: https://192.102.163.105/ Step 2: Put the username and password. Step 3: In the Simulation section of the page, upload the node, edge and config files. Step 4: Click on 'Simulate'. Step 5: After simulation ends, a zip file is generated. Extract the file and results will be present in the form of HTML, .csv and .png files.
Expected Results	**HTML**: Network in the graphical form with information on nodes and their interconnections. **Resilience curves**: Graph of time-series of average state of stations in the network over time. State is availability of the stations in range [0, 1]. **GIF**: Visualization of impact propagation in the networks. **CSV**: Time-series of state of the systems involved in the exercise. In the web-page, under section 'Impact propagation' the results of the propagation are published along with different mitigation measures and their evaluations. A screenshot of the GIF showing propagation of impact is shown in Figure 3.  FIGURE 3: EXAMPLE OF IMPACT PROPAGATION IN THE CDM NETWORK. RED REPRESENTS DAMAGED NODES, BLUE RECOVERING AND GREEN RECOVERED NODES RESPECTIVELY.
Pass/Fail	Pass
Deviation Encountered	In absence of relevant data regarding power grids, the cascading from power to metro has only been studied conceptually (see D4.5).
Problems	Difficulty in obtaining relevant data.
Comments	Impact propagation uses propagation by connectivity, as a result cascades are visible based on connectivity in the network and inter-connectivity across the CIs. Further methods of propagation need to be added to work based on feedback from end-users.

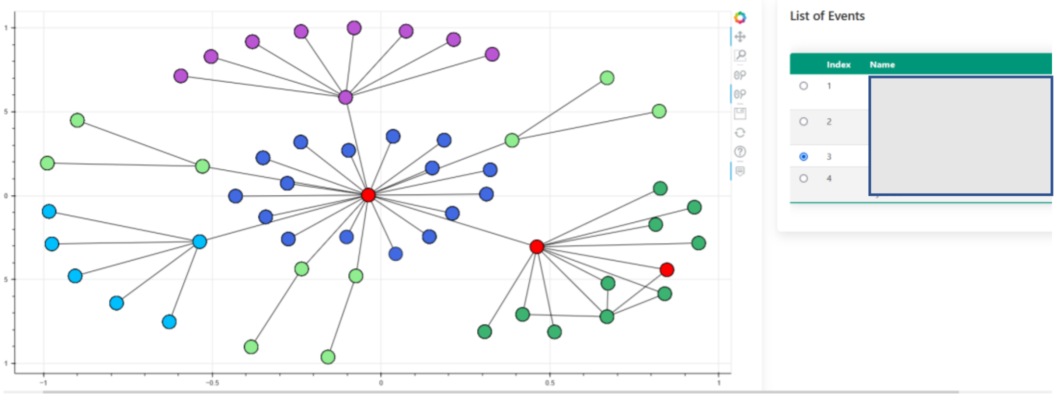
Test.-ID	CaESAR_TR_04
Addressed Requirement	CaESAR_04 **CaESAR should apply different strategies to recover from disruptive events and evaluate their impact on the infrastructure resilience** Minimize event impact by optimized recovery
HW / SW preparation	1. Laptop/Computer 2. Firefox/Chrome/Edge browser 3. Java Runtime Environment
Test inputs	Test bed (Railway/Metro grid network) with inter-connections to relevant CIs (e.g. Bus network, power networks). 1. Nodes.csv: semicolon separated file with information on nodes (representing stations) in the network and their repair times. 2. Edges.csv: semicolon separated file with information on edges (inter-connections) between nodes/stations in the network. 3. Config.JSON: Configuration file with information on the attack on the network, with node number and time of attack. Further for different mitigation strategies, repair times and state of the system in case of failures.
Test procedure	Step 1: Open CaESAR url: https://192.102.163.105/ Step 2: Put the username and password Step 3: In the Simulation section of the page, upload the node, edge and config files. Step 4: Click on ‘Simulate’ Step 5: After simulation ends, a zip file is generated. Extract the file and results will be present in the form of HTML, .csv and .png files.
Expected Results	**HTML**: Network in the graphical form with information on nodes and their interconnections. **Resilience curves**: Graph of time-series of average state of stations in the network over time. State is availability of the stations in range [0, 1]. **GIF**: Visualization of impact propagation in the network. **CSV**: Time-series of state of the systems involved in the exercise. In meta_data.csv, for every recovery strategy, there is quantification of the method using area below the curve. The higher the value, the better the performance of the strategy.
Pass/Fail	Pass
Deviation Encountered	
Problems	Recovery in the network is dependent on the individual repair times of the nodes in the network.
Comments	As CaESAR is developed as a framework, different strategies can be added to the simulation. In future, this can be discussed with end-users and validated.

<table>
<tr><td>**Test.-ID**</td><td>CaESAR_TR_05</td></tr>
<tr><td>**Addressed Requirement**</td><td>CaESAR_05
Implementation and evaluation of mitigation measures
- Find new mitigation strategies
- Evaluate known, not used measures</td></tr>
<tr><td>**HW / SW preparation**</td><td>1. Laptop/computer
2. Firefox/Chrome/Edge browser
3. Java Runtime Environment</td></tr>
<tr><td>**Test inputs**</td><td>Test bed (Railway/Metro grid network) with inter-connections to relevant CIs (e.g. Bus network, power networks).
1. Nodes.csv: semicolon separated file with information on nodes (representing stations) in the network and their repair times.
2. Edges.csv: semicolon separated file with information on edges (inter-connections) between nodes/stations in the network.
3. Config.JSON: Configuration file with information on the attack on the network, with node number and time of attack. Further for different mitigation strategies, repair times and state of the system in case of failures.</td></tr>
<tr><td>**Test procedure**</td><td>Step 1: Open CaESAR url: https://192.102.163.105/
Step 2: Put the username and password
Step 3: In the Simulation section of the page, upload the node, edge and config files.
Step 4: Click on ‘Simulate’
Step 5: After simulation ends, a zip file is generated. Extract the file and results will be present in the form of HTML, .csv and .png files.</td></tr>
<tr><td>**Expected Results**</td><td>**HTML**: Network in the graphical form with information on nodes and their interconnections.
Resilience curves: Graph of time-series of average state of stations in the network over time. State is availability of the stations in range [0, 1].
GIF: Visualization of impact propagation in the network.
CSV: Time-series of state of the systems involved in the exercise.
Specifically, meta_data.csv is generated, which contains rating of different mitigation measures, as described in config. JSON. In the web-page, mitigation measures are mentioned under Impact propagation section. Below is a screen-shot of the same:


Local Time: 08:26:07
Mitigation Options
<table>
<tr><th></th><th>Name</th><th>Impact Start</th><th>Impact End</th><th>Score</th><th>Min Performance</th></tr>
<tr><td>●</td><td>No Mitigation</td><td>5</td><td>151</td><td>11000</td><td>22.97</td></tr>
<tr><td>○</td><td>Isolation of IT-assets</td><td>5</td><td>151</td><td>11054.05</td><td>22.97</td></tr>
<tr><td>○</td><td>Rerouting of Passengers</td><td>5</td><td>155</td><td>13331.08</td><td>47.3</td></tr>
</table>
FIGURE 4: IMPACT PROPAGATION SECTION ON THE WEB-PAGE. ON THE LEFT SIDE IS THE UNIFIED RESILIENCE GRAPH AND ON THE RIGHT IS THE SELECTABLE LIST OF DIFFERENT MITIGATION MEASURES.</td></tr>
<tr><td>**Pass/Fail**</td><td>Pass</td></tr>
<tr><td>**Deviation Encountered**</td><td></td></tr>
<tr><td>**Problems**</td><td></td></tr>
</table>

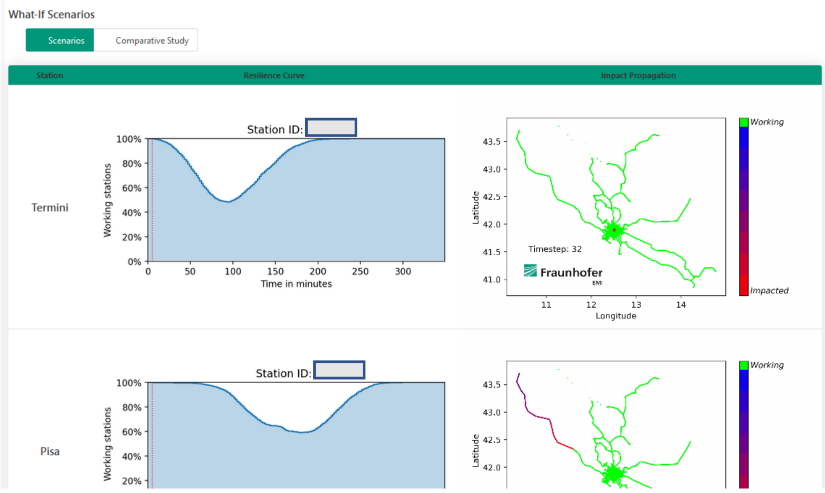
Comments	The assessment depends on the details of the modelled threats. Right now, threats have attributes including, repair times, attacked nodes, cascade probability and node types. To demonstrate the full capacity of the system, further parametrizing of the threats is needed.

Test.-ID	CaESAR_TR_06
Addressed Requirement	CaESAR_06 **CaESAR should be able to handle the following different types of attack:** • physical • cyber • cyber-physical estimate the impact of combined cyber-physical events on critical infrastructures
HW / SW preparation	1. Laptop/Computer 2. Firefox/Chrome/Edge web-browser 3. Java Runtime Environment
Test inputs	Test bed (Railway/Metro grid network) with inter-connections to relevant CIs (e.g. Bus network, power networks). 1. Nodes.csv: semicolon separated file with information on nodes (representing stations) in the network and their repair times. 2. Edges.csv: semicolon separated file with information on edges (inter-connections) between nodes/stations in the network. 3. Config.JSON: Configuration file with information on the attack on the network, with node number and time of attack. Define threats by attributes, e.g. type of component (cyber-attack), radius of impact (physical attack) or combination of both. Further define probability of attack and cascades for these attacks.
Test procedure	Step 1: Open CaESAR url: https://192.102.163.105/ Step 2: Put the username and password Step 3: In the Simulation section of the page, upload the node, edge and config files. Step 4: Click on ‘Simulate’ Step 5: After simulation ends, a zip file is generated. Extract the file and results will be present in the form of HTML, .csv and .png files.
Expected Results	For different types of threats, depending on the simulation run, results are generated as follows: **HTML**: Network in the graphical form with information on nodes and their interconnections. **Resilience curves**: Graph of time-series of average state of stations in the network over time. State is availability of the stations in range [0, 1]. **GIF**: Visualization of impact propagation in the network. **CSV**: Time-series of state of the systems involved in the exercise. For the Ankara exercise (EGO), an associated cyber grid is modelled and impact on the overall network is presented. Following screenshot shows station specific modelling of connected systems.

	 List of Events Index Name 1 2 3 4 -1 -0.5 0 0.5 1 FIGURE 5: SCREENSHOT OF CONNECTED COMPONENTS TO STATION IN EGO EXERCISE. THE NODES IN RED ARE THE IMPACTED COMPONENTS.[6]
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	The impact propagation depends on the components and inter-connections modelling of the network. Threats can attack a hybrid network (cyber-physical network) based on their attributes, however impact on the overall network depends on the inter-connections, which has to be clearly modelled. Currently, simulations are based on open-source data. With the help of some feedback from end-users, this can be further demonstrated in detail.

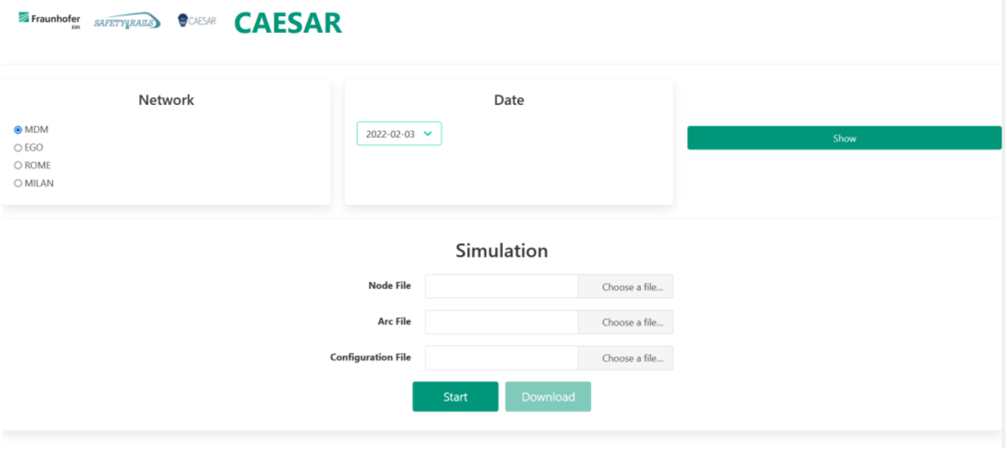
Test.-ID	CaESAR_TR_07
Addressed Requirement	CaESAR_07 **Implementation of what-if scenarios and varying disruptive events attributes** • model single-point failures in the network and estimate the impact on the resilience of the critical infrastructure • model multiple-point failures in the network and estimate the impact on the resilience of the critical infrastructure • model simultaneous failures in the cyber and the physical part of the network
HW / SW preparation	1. Laptop/Computer 2. Firefox/Chrome/Edge web-browser 3. Java Runtime Environment
Test inputs	Test bed (Railway/Metro grid network) with inter-connections to relevant CIs (e.g. Bus network, power networks). 1. Nodes.csv: semicolon separated file with information on nodes (representing stations) in the network and their repair times. 2. Edges.csv: semicolon separated file with information on edges (inter-connections) between nodes/stations in the network. 3. Config.JSON: Configuration file with information on the attack on the network, with node number and time of attack. For specific what-if scenarios, add threats, with single-point/multi-point failure inputs for different stations/components in the network.
Test procedure	Step 1: Open CaESAR url: https://192.102.163.105/ Step 2: Put the username and password. Step 3: In the Simulation section of the page, upload the node, edge and config files. Step 4: Click on ‘Simulate’.

[6] Names redacted.

	Step 5: After simulation ends, a zip file is generated. Extract the file and results will be present in the form of HTML, .csv and .png files.
Expected Results	**HTML**: Network in the graphical form with information on nodes and their interconnections. **Resilience curves**: Graph of time-series of average state of stations in the network over time. State is availability of the stations in range [0, 1]. **GIF**: Visualization of impact propagation in the network. **CSV**: Time-series of state of the systems involved in the exercise. With selective stations, single point failures are introduced in the network and results are presented in tabular form representing resilience of the network and impact propagation in the network. A comparative graph of resilience of the network for these individual failures is also displayed.  What-If Scenarios Scenarios Comparative Study Station Resilience Curve Impact Propagation Termini Station ID: [redacted] 100% 80% 60% 40% 20% 0% Working stations 0 50 100 150 200 250 300 Time in minutes 43.5 43.0 42.5 42.0 41.5 41.0 Latitude 11 12 13 14 Longitude Timestep: 32 Fraunhofer EMI Working Impacted Pisa Station ID: [redacted] 100% 80% 60% 40% 20% Working stations 43.5 43.0 42.5 42.0 Latitude Working FIGURE 6: WHAT-IF SCENARIOS PRESENTED IN TABULAR FORMAT. THE RESULT PRESENTS DIFFERENT SINGLE POINT FAILURES IN NETWORK AND CORRESPONDING IMPACT PROPAGATION USING GIF.[7]
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	CaESAR_TR_08
Addressed Requirement	CaESAR_08 **Conformity with overarching and S4RIS platform specific requirements** Ensure that any work connected with this tool conforms to the overarching and S4RIS platform specific requirements.
HW / SW preparation	1. Laptop/computer 2. Firefox/Chrome/Edge browser 3. Java Runtime Environment
Test inputs	This can be tested only from S4RIS platform or the DMS interface (RAM2).
Test procedure	**Test 1:** Step 1: For a pre-defined channel (for example: cdm_demo), via RAM2, send an alert with information on an event. Step 2: On the CaESAR server, check if the message is received. Step 3: After simulation is finished, CaESAR sends a response on the same channel. Check in RAM2, if the response has been received. **Test 2:**

[7] Names redacted.

	Step 1: Login to S4RIS platform. Step 2: On the home page, select CaESAR.. A new tab with login popup should open. Step 3: Enter the username and password for CaESAR. Step 4: CaESAR home page should open. The expected page is shown in Figure 7.
Expected Results	The tool is capable of receiving messages from the distributed messaging system (DMS) and is able to publish corresponding information on the relevant channel on DMS. For the test 2, tool should be accessible via the S4RIS platform. Following is the screen-shot of the homepage for CaESAR.  Network: ● MDM ○ EGO ○ ROME ○ MILAN Date: 2022-02-03 Fraunhofer SAFETY RAILS CAESAR CAESAR Show Simulation Node File Choose a file... Arc File Choose a file... Configuration File Choose a file... Start Download FIGURE 7: HOMEPAGE OF THE CAESAR TOOL
Pass/Fail	Pass
Deviation Encountered	CaESAR does not provide a direct user operable interface for DMS. However, in the connected environment, CaESAR continuously polls for the messages and responds accordingly. This is relevant for live production environment.
Problems	
Comments	

3.3 CAMS

3.3.1 Overview

The **C**entral **A**sset **M**anagement **S**ystem (CAMS) provides deterioration modelling, risk assessment, rehabilitation cost forecasting, and an integrated mobile solution for data collection.

Budget policies will also affect resilience, as different recovery plans, which mean different budget allocations, will lead to different recovery times and resilience factors.

CAMS forecasts asset aging damage. An effective maintenance plan and budget allocation require insight into the deterioration process of each asset. Variations in conditions over time will be represented by curves.

Based on the predicted damage conditions, the model will forecast future maintenance and repair expenditures. Using this data, asset managers can maximize impact and reduce risk by choosing the most suitable time and place to invest. This module determines the final damage condition after a disruptive event. An intensity measure of the disruptive event is used to determine fragility functions that express the probability of reaching or exceeding a level of damage. The response of an asset to a certain event depends also on its current infrastructure state. Deterioration also affects fragility analysis. Defining the extreme event is the first step in performing this analysis.

By defining level-of-service criteria for the given elements and suggesting rehabilitation strategies, risk cost mitigation and expenditure projection can be achieved.

CAMS can include inflation's effect based on inflation rates. Based on the forecasting of damage and maintenance costs, the backlog estimation provides the asset manager with valuable decision-making information. CAMS will inform the asset manager about which is the most effective financial strategy to enhance resilience against different threats, taking into account other asset management activities such as maintenance, repair, and rehabilitation. CAMS will be applied to IT assets as a budgeting tool described in the previous requirements. By integrating physical and digital elements, budgetary and financial strategies will be more effective.

CAMS provides analysis of different budgetary scenarios based on different maintenance, repair, rehabilitation, and enhancement strategies. CMAS optimizes resilience enhancement strategies within regular asset management plans. It will therefore utilize the modules for optimization and budgeting. In order to evaluate all possible strategies, CAMS could define normal and crush times as well as cost.

3.3.2 Development and Quality standards adopted

CAMS software is a SAS (Software as a Service) model. The software is based on Mongo DB database structure with Angular powering the online code. The CAMS software is aligned with ISO55000 (asset management) international standard.

This is due to the fact that CAMS supports a methodology for making decisions about infrastructure life cycle management based on an analysis of data.

3.3.3 Data used for tests

CAMS collected data from end-user organizations, their staff experiences, researchers and/or inspectors from historical incidents including but not limited to:

- Capital value of the elements;
- Cost of asset maintenance under normal degradation;
- Time allocated for maintenance of the element;
- Cost of asset repair under normal degradation and hazard event;
- Time and cost spent in maintenance, repair or renewal;
- Cost and time of asset rehabilitation under normal degradation and/or hazard event.

CAMS data needed were developed based on previously designed questionnaires by RMIT, which contained open-ended fields. For CAMS to perform optimally, the following information was collected from end users.

- Phase 1, asked about the presence or absence of a number of main assets (from 35 to 58 items) from the list of assets elaborated by RMIT in D7.1. It also asks about maintenance strategies, offering four non-exclusive possibilities: 1) run to failure, 2) preventive maintenance, 3) predicative maintenance and 4) reliability centred maintenance. Furthermore, the way components are checked is also requested, offering two possibilities: 1) manually checked and 2) automatically monitored.
- Phase 2, presented 13 data lists with a variable number of non-exclusive answers depending on the question. These data lists refer to asset management, including specific questions on the forms of maintenance, overhaul, the functioning and characteristics of the asset management system and the difficulties in its implementation and operation. This phase had a specific emphasis on the asset management strategy, asset inventory, condition inspection methods and decision-making scenarios.
- Phase 3, improved the data lists includes some additional data lists.

The data used for the tests was the data collected for the four simulation exercises in WP8.

3.3.4 Test Data Report

This section reports the tests executed for CAMS, based on requirements described in D1.4 par. 2.3.3.

Test.-ID	CAMS_TR_01
Addressed Requirement	CAMS_01 **Prediction of normal deterioration due to aging and degradation of assets** • Understand the deterioration process of assets • Predict the future damage condition of an asset given its current condition. • Predict the damage condition at the moment of an attack
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input. Step 5: Editing data file before calculation. Step 6: Defining the person authorized to access CAMS. Step 7: Input data file via CAMS dashboard tool.
Expected Results	The determination of when assets will degrade due to normal aging and degradation based on their current condition and at the time of the attack.nd predicting their future damage conditions based on their present state and at the time of the attack.
Pass/Fail	Passed
Deviation Encountered	None
Problems	-
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_02
Addressed Requirement	CAMS_02 **Maintenance and repair budget calculation** • Estimate the maintenance and repair budget • Help the asset manager to take informed decisions • Elaborate and compare maintenance plans
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the

	associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input. Step 5: Editing data file before calculation. Step 6: Determining Renewal Cost by Unit Price Step 7: Identifying Maintenance Cost by Unit Price Step 8: Defining the person authorized to access CAMS. Step 9: Input data file via CAMS dashboard tool. Step10: Generating budget plans for damaged components or aging equipment.
Expected Results	Providing repair, maintenance, and replacement schedules to infrastructure decision makers.
Pass/Fail	Passed with Deviations
Deviation Encountered	The updating of the price of infrastructure components could provide CAMS with a better analysis of the results.
Problems	Different security policies implemented by infrastructure decision-makers and security authorities affected output reliability differently.
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_03
Addressed Requirement	CAMS_03 **State-dependent fragility analysis** • Calculation of the damage to an asset after a disruptive event (man-made, natural, etc.) • •Take into account the initial damage condition before the attack • •Estimate the performance loss after the event
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input.

	Step 5: Editing data file before calculation. Step 6: Defining the person authorized to access CAMS. Step 7: Input data file via CAMS dashboard tool. Step 8: Classifying intact elements into fragility functions as slight states Step 9: Classifying intact elements into fragility functions as moderate states Step 10: Classifying intact elements into fragility functions as extensive states Step 11: Classifying intact elements into fragility functions as complete states Step 12: Generating the fragility module of the disruption damages.
Expected Results	The fragility module calculates how much damage would be caused after a disruption. In this situation, a natural hazard or terrorist attack may occur. It can happen in a cyber, physical or combined. In addition, the damage assessment must consider the initial damage caused by the aging of the elements. Fragility is a new feature that has been included in the CAMS and has been integrated into the SAFETY4RAILS framework following the degradation module. This module can take as inputs the initial damage condition and the type and intensity of the disruptive event. The outcome is the final damage condition after the event. To determine the damage after a disruptive element, a fragility analysis is required.
Pass/Fail	Pass
Deviation Encountered	None
Problems	-
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_04
Addressed Requirement	CAMS_04 **Resilience module:** • Calculate the resilience normalized factor for an asset facing a disruptive event • Establish the relation between damage and impact on the performance of the asset • Define the recovery plans, based on the cost and time for a given level of resilience
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input. Step 5: Editing data file before calculation. Step 6: Determining Renewal Cost by Unit Price

	Step 7: Identifying Maintenance Cost by Unit Price. Step 8: Defining the person authorized to access CAMS. Step 9: Input data file via CAMS dashboard tool. Step 10: Classifying intact elements into fragility functions as slight states Step 11: Classifying intact elements into fragility functions as moderate states Step 12: Classifying intact elements into fragility functions as extensive states Step 13: Classifying intact elements into fragility functions as complete states Step 14: Generating the fragility module of the disruption damages. Step 15: Establish the relationship between damage components and impact on the performance of the asset. Step 16: Achieving given levels of resilience with the appropriate time and cost.
Expected Results	The resilience module would calculate the resilience normalized factor for an infrastructure asset facing a disruptive event. The resilience module may also establish the relationship between damage and the impact on the performance of the components by using the recovery plans based on the cost and time.
Pass/Fail	Passed
Deviation Encountered	None
Problems	-
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_05
Addressed Requirement	CAMS_05 **Risk/cost evaluation** • Calculate the risk cost based on the foreseen damage condition. • Long-term planning in asset management. • Provide information to optimize the decision and intervention policies. • Provide support for the prioritisation of the financial/budgetary alternatives.
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input. Step 5: Editing data file before calculation. Step 6: Determining Renewal Cost by Unit Price Step 7: Identifying Maintenance Cost by Unit Price. Step 8: Identifying Repair Cost by Unit Price Step 9: Classification Component Priority of recovery. Step 10: Defining the person authorized to access CAMS.

	Step 11: Input data file via CAMS dashboard tool. Step 12: Classifying intact elements into fragility functions as slight states Step 13: Classifying intact elements into fragility functions as moderate states Step 14: Classifying intact elements into fragility functions as extensive states Step 15: Classifying intact elements into fragility functions as complete states Step 16: Generating the fragility module of the disruption damages. Step 17: Establish the relationship between damage components and impact on the performance of the asset. Step 18: Achieving given levels of resilience with the appropriate time and cost. Step 19: Recalculating each initial condition for optimizing after occurred damage.
Expected Results	Based on the foreseen damage condition and long-term asset management planning, the cost of recovery might be reduced. By providing information to optimize proper budgeting and prioritizing railroad assets.
Pass/Fail	Passed with Deviations
Deviation Encountered	The variety of tools used in the experiment made it difficult to communicate the results. In some cases, users used different communication platforms and different options for data handover, which created some issues between participants of the project.
Problems	Different security policies implemented by infrastructure decision-makers and security authorities affected output reliability differently.
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_06
Addressed Requirement	CAMS_06 **Backlog estimation** • Estimate the backlog in the maintenance expenditures. • Provide information to the asset manager on how and when to spend the available budget.
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input. Step 5: Editing data file before calculation. Step 6: Determining Renewal Cost by Unit Price Step 7: Identifying Maintenance Cost by Unit Price. Step 8: Identifying Repair Cost by Unit Price Step 9: Classification Component Priority of recovery. Step 10: Assign a rating from 1 to 5 to components' conditions before an incident or aging.

	Step 11: Assign a rating from 1 to 5 to components' conditions after an incident or aging. Step 12: Define dependencies components for recovery. Step 13: Defining the person authorized to access CAMS. Step 14: Input data file via CAMS dashboard tool. Step 15: Classifying intact elements into fragility functions as slight states Step 15: Classifying intact elements into fragility functions as moderate states Step 16: Classifying intact elements into fragility functions as extensive states Step 17: Classifying intact elements into fragility functions as complete states Step 18: Generating the fragility module of the disruption damages. Step 19: Establish the relationship between damage components and impact on the performance of the asset. Step 20: Achieving given levels of resilience with the appropriate time and cost. Step 21: Recalculating each initial condition for optimizing after occurred damage. Step 22: By adding more detail items to estimates, backlog refinement will be achieved.
Expected Results	CAMS allow managers to evaluate various analysis reports related to asset deterioration, risk, and budget forecasting. Therefore, they will be able to make informed decisions regarding maintenance and budget allocations.
Pass/Fail	Passed with Deviations
Deviation Encountered	A better integration between tools could lead to a better outcome in similar projects in the future. As well, End-users faced many limitations in presenting needed data and also encountered a delay in this item.
Problems	Different security policies implemented by infrastructure decision-makers and security authorities affected output reliability differently.
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_07
Addressed Requirement	CAMS_07 **Optimization budget** • Optimize the available budget which can be divided into maintenance/repair, rehabilitation, resilience enhancement retrofits, and reconstruction/replacement. • The optimization of the budget is made to achieve a certain level of resilience facing a given intensity of an extreme event (including manmade or natural hazards, etc.) • Provide support for the prioritisation of the financial/budgetary alternatives • Provide information to optimize the decision and intervention policies.
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.

Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input. Step 5: Editing data file before calculation. Step 6: Determining Renewal Cost by Unit Price Step 7: Identifying Maintenance Cost by Unit Price. Step 8: Identifying Repair Cost by Unit Price Step 9: Estimating Time Spent for Maintenance Step 10: Estimating Time Spent for Repair Step 11: Estimating Time Needed for Replacement Step 12: Classification Component Priority of recovery. Step 13: Assign a rating from 1 to 5 to components' conditions before an incident or aging. Step 14: Assign a rating from 1 to 5 to components' conditions after an incident or aging. Step 15: Define dependencies components for recovery. Step 16: Defining the person authorized to access CAMS. Step 17: Input data file via CAMS dashboard tool. Step 18: Classifying intact elements into fragility functions as slight states Step 19: Classifying intact elements into fragility functions as moderate states Step 20: Classifying intact elements into fragility functions as extensive states Step 21: Classifying intact elements into fragility functions as complete states Step 22: Generating the fragility module of the disruption damages. Step 23: Establish the relationship between damage components and impact on the performance of the asset. Step 24: Achieving given levels of resilience with the appropriate time and cost. Step 25: Recalculating each initial condition for optimizing after occurred damage. Step 26: By adding more detail items to estimates, backlog refinement will be achieved. Step 26: Prioritizing an alternative financial and budgetary plan during the recovery phase by modifying the resilience of damaged components. Step 27: Optimizing the recovery plan with budget information based on historical events.
Expected Results	CAMS is able to work on infrastructure such as buildings, drainage assets, bridges, and railways. The SAFETY4RAILS project will expand the concept to include railway assets, optimal budget, and planned assets. A further improvement of the current system is its resilience to extreme incidents, such as combined terrorist attacks.
Pass/Fail	Passed with Deviations
Deviation Encountered	The optimization of the budget failed due to a lack of cost data and historical events for component replacement and repair, thus affecting the accuracy of the budget evaluation.
Problems	Different security policies implemented by infrastructure decision-makers and security authorities affected output reliability differently.
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_08
Addressed Requirement	CAMS_08 **Extension of the framework to IT assets** • Include in the proposed model IT assets such as control sys-tems, communication systems, ticketing systems, software, da-tabases, among others.

	• Address for cyber and combined attacks on both physical and IT assets. • Developed a unified asset management system for physical and IT assets • Provide information to perform IT maintenance. • Provide support for the prioritisation of the financial/budgetary alternatives in the asset management of IT assets
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input. Step 5: Editing data file before calculation. Step 6: Determining Renewal Cost by Unit Price Step 7: Identifying Maintenance Cost by Unit Price. Step 8: Cataloguing Railroad Equipment Subsystems. Step 9: Identifying stations' physical components Step 10: Cataloguing tunnel and access facilities. Step 11: Cataloguing the items in control rooms. Step 12: Cataloguing of components within TPS rooms. Step 13: Cataloguing of AC Room components. Step 14: Cataloguing of Battery Room components. Step 15: Cataloguing of EER Room components. Step 16: Cataloguing CCTV System network Step 17: Cataloguing IoT components Step 18: Cataloguing ticket machines and network panels. Step 19: Cataloguing Electrical Equipment and Ventilation System. Step 20: Cataloguing UPS and Rectifier Batteries Step 21: Sorting all assets by quantities. Step 22: Categorize components cycle life. Step 23: Recalculating each initial condition for optimizing after occurred damage.
Expected Results	The management of IT assets should be part of a unified asset management system that allows for IT maintenance to be performed as well as guidance on where to invest in infrastructure in the future. End-user data usually included minimum details about these types of components.
Pass/Fail	Passed with Deviations
Deviation Encountered	Some simulation exercises were not part of the cyber-attack in terms of the IT component. Also, some of the physical attack simulation exercises are less overlaid and are a mixture of cyber attacks and physical attacks.
Problems	Different security policies implemented by infrastructure decision-makers and security authorities affected output reliability differently.
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_09
Addressed Requirement	CAMS_09 **Analysis of compromise between maintenance, repair, rehabilitation and resilience enhancement effort** • Perform analysis to find the best way to invest limited budget to face disruptive events ensuring a minimum level of resilience. • Provide the asset manager with relevant information to make financial planning and allocation of resources. • Identify the best way to achieve a given level of resilience • Provide support for the prioritisation of the financial/budgetary alternatives.
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input. Step 5: Editing data file before calculation. Step 6: Determining Renewal Cost by Unit Price Step 7: Identifying Maintenance Cost by Unit Price. Step 8: Identifying Repair Cost by Unit Price Step 9: Calculation Time Spent for Maintenance Step 10: Calculation Time Spent for Repair Step 11: Calculation Time Needed for Replacement Step 12: Assessment Time required performing the above steps. Step 13: Classification Component Priority of recovery. Step 14: Changing component rating from 5 to 1 to components' conditions before an incident or aging. Step 15: Changing component rating from 5 to 1 to components' conditions after an incident or aging. Step 16: Redefine dependencies components for recovery. Step 17: Optimizing the recovery plan with budget information based on historical events.
Expected Results	Analysis of the compromise between maintenance, repair, rehabilitation, and resilience enhancement efforts following results.
Pass/Fail	Passed
Deviation Encountered	None
Problems	-

Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_10
Addressed Requirement	CAMS_10 **Assessment of recovery** • Evaluate different recovery and response actions from a performance and budgetary point of view. • Evaluate the budget allocation needed for facing a disruptive event ensuring a minimum level of resilience. • Establishing the crash and normal times and costs for each recovery strategy. • Provide information for a taking better informed decisions on different recovery strategies.
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Gathering of Principal Asset Data from End User Data Base. Step 2: Taxonomizing each asset based on component technology and operation. Step 3: Breaking assets down according to the following steps. Step 4: Preparing Excel/CVS data files as CAMS input. Step 5: Editing data file before calculation. Step 6: Determining Renewal Cost by Unit Price Step 7: Identifying Maintenance Cost by Unit Price. Step 8: Identifying Repair Cost by Unit Price Step 9: Calculation Time Spent for Maintenance Step 10: Calculation Time Spent for Repair Step 11: Calculation Time Needed for Replacement Step 12: Assessment Time required performing the above steps. Step 13: Classification Component Priority of recovery. Step 14: Changing component rating from 5 to 1 to components' conditions before an incident or aging. Step 15: Changing component rating from 5 to 1 to components' conditions after an incident or aging. Step 16: Redefine dependencies components for recovery. Step 17: Optimizing the recovery plan with budget information based on historical events. Step 18: Prioritizing an alternative financial and budgetary plan during the recovery phase by modifying the resilience of damaged components.
Expected Results	Management of assessment in the recovery phase after incidents could analyze the best way to allocate budget to meeting disruptive events in a way that ensures a minimum level of resilience. Include in the proposed model IT assets

	such as control systems, communication systems, ticketing systems, software, databases, among others.
Pass/Fail	Passed
Deviation Encountered	None
Problems	-
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

Test.-ID	CAMS_TR_11
Addressed Requirement	CAMS_11 **Conformity with overarching and S4RIS platform specific requirements**
HW / SW preparation	There are constraints that are based on the infrastructure components, so a list of infrastructure assets is needed. The value and quantities of components, the renewal, maintenance, or repair costs, and time spent on maintenance, repair, or replacement of the out-of-service components during the recovery phase of the associated infrastructures are required as references in order to compute the actual evaluation.
Test inputs	Excel/CVS files contain at least five of the above fields and at least two similar events. The input file was designed by CAMS to store simple tables and spreadsheets. The contents of the table are usually a table of text, numbers, or cost or unit price and metric unit. It is possible to import, edit, and export Excel/CVS data files within a CAMS environment that can be synchronized and exchanged via DMS with KAFKA.
Test procedure	Step 1: Improving Asset Databases with the help of End-Users Step 2: Adding historical costs and recovery times. Step 3: Recalculation Budget planning with historical data. Step 4: Creating an alternative financial and budgetary plan during the recovery phase by modifying the resilience of damaged components:
Expected Results	A higher level of integration and a closer relationship with end-users will lead to a better outcome in the future. It may also be useful to define more realistic scenarios of simulation exercises from the perspective of the end-user.
Pass/Fail	Passed with Deviations
Deviation Encountered	There were insufficient data regarding the scenarios to draw better conclusions. As a result of the pandemic, physical communication was restricted, preventing the transfer of historical experiences.
Problems	Different security policies implemented by infrastructure decision-makers and security authorities affected output reliability differently.
Comments	There were a few deviations due to a lack of historical data and an insufficient categorization in accordance with end-user regulations.

3.4 CuriX

3.4.1 Overview

CuriX is a software solution for monitoring systems which entail heterogeneous infrastructure such as in the IT and railway environments.

One of the main capabilities that CuriX brings to the S4RIS is the ability to detect anomalies in the behaviour from the monitored system data, which are significant deviations from the normal behaviour of the monitored systems. Further details on the capabilities of the software solution can be found, for instance, in the deliverable D1.4

3.4.2 Development and Quality standards adopted

The features which have been developed for CuriX in SAFETY4RAILS, followed the Agile methodology, which is described in section 3.6.2. GitLab was used as a source code repository to enable management and collaboration on the software with the use of version control, tracking of issues, and code review.

For individual units of the source code, unit testing is performed whenever a new version is committed. Functional tests were performed in order to verify the intended working of the newly developed code.

3.4.3 Data used for tests

Partially synthetic and fully synthetic data which realistically represents the behaviour of time-series data from railway systems, which we would encounter in the planned simulation exercises, was created as test input.

Partially synthetic data was created from a small sample of real data (e.g., by pseudonymizing and sampling) for noise levels in a station environment, passenger information system broadcasting frequency, and total and station energy consumption.

For the noise level data in a station environment the following sources were used (Prediction of noise of the stations of the new Budapest metro line M4, 2014), (Noise impact assessment of mass rapid transit systems in Delhi city, 2011) and (Prediction of noise from small to medium sized crowds, 2011).

For the passenger information system broadcasting frequency, we received data which was collected from our consortium partner EGO.

For the station energy consumption, we received data which was collected from our consortium partner MdM, while for the total energy consumption we adapted data from (Hourly energy consumption characteristics of metro rail transit: Train traction versus station operation, 2022).

Five fully synthetic time series were generated representing the behaviour of other systems. Both partially and fully synthetic generated data correspond to time series of a length of two weeks.

The test was performed several dozens of times for various time series in different scenarios.

3.4.4 Test Data Report

This section reports the tests executed for CuriX, based on requirements described in D1.4 par. 2.3.4

Test.-ID	CuriX_TR_01
Addressed Requirement	CuriX_01 **Anomaly Detection (univariate and multivariate)** • •AIOps techniques to determine observed anomalies within Rail-way infrastructure (IT, OT) • •Anomaly detection for the whole Railway infrastructure based on specific KPIs • •Detection of system faults (IT / IoT, OT operation management)

	• •Detection of cyber threats (system vulnerabilities)
HW / SW preparation	A dedicated virtual machine which runs CuriX for SAFETY4RAILS has been provisioned and set up for testing and for providing a demonstration for the simulation exercises.
Test inputs	Synthetic data which realistically represents the behaviour of time-series data from railway systems, which we would encounter in the planned simulation exercises, was created as test input.
Test procedure	Step 1: Ingestion of synthetic data into the data collector for CuriX. Making sure that the anomaly detector is being trained on data representing two weeks. Step 2: Injecting anomalies which correspond to the threats envisioned by the simulation exercises by manipulation of the time-series values. Step 3: Open anomaly detector to observe the correctness of the injected anomalies in the back end. Step 4: Verify that injected anomalies are recognized as such by the anomaly detector. Step 5: Open the dashboard for CuriX and verify that the anomalies have translated in the correct resilience issue (i.e., alarm) regarding the anomaly.
Expected Results	CuriX generates an alarm (in CuriX it is called a “resilience issue”) that informs about an increase of anomalies on the specific time-series due to the injection of a threat.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	CuriX_TR_02
Addressed Requirement	CuriX_02 **Catalogue based outage prevention** • System Failures and Outages Prediction • Trigger warnings in advance to avoid potential failures • Cyber threat identification (based on security KPIs) • Predefined healings based on fix execution scenarios • (optional) Catalogue-based attack simulation • (optional) Generic Heal Advice
HW / SW preparation	See Test-ID CuriX_TR_01. In addition, the software has been configured to include tags such as “Network”, “Energy”, “Memory”, etc.
Test inputs	See Test-ID CuriX_TR_01
Test procedure	Step 1: Ingestion of synthetic data into the data collector for CuriX. Step 2: Injecting anomalies by manipulation of the time-series values. Step 3: Open the dashboard for CuriX and verify that the correct tags are appearing for the corresponding time series in the resilience issues tab.
Expected Results	For each generated alarm by CuriX, tags should be added according to the meaning of the underlying time-series, i.e., a memory related time-series anomaly should be tagged with “Memory”.
Pass/Fail	Pass
Deviation Encountered	

Problems	
Comments	

Test.-ID	CuriX_TR_03
Addressed Requirement	CuriX_03 **Infrastructure monitoring (including cyber threats)** • Real time monitoring of the Railway infrastructure (IT, IoT, OT) • Real time monitoring of cyber threats • Trigger alerts • Provide data to be able to process anomaly detection (CuriX_01) and outage prevention (CuriX_02) • Real time monitoring (time series analysis)
HW / SW preparation	See Test-ID CuriX_TR_01
Test inputs	Synthetic data which realistically represents the behaviour of time-series data from railway systems, which would only occupy a limited set of discrete values, e.g. 0 for a closed and 1 an open door, was created.
Test procedure	Step 1: Ingestion of synthetic data into the data collector for CuriX. Making sure that the anomaly detector is being trained on data representing two weeks. Step 2: Open anomaly detector to observe and verify the correctness of the trained model in the back end.
Expected Results	The trained baseline model should only take values that are in the same discrete value set as the original data which represent infrastructure environment.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	CuriX_TR_04
Addressed Requirement	CuriX_04 **CuriX user-friendly dashboard** • Easy and intuitive to use • Easy to understand the data because of the customized visualization • S4RIS user can access CuriX Dashboard (GUI)
HW / SW preparation	See Test-ID CuriX_TR_01
Test inputs	See Test-ID CuriX_TR_01
Test procedure	Step 1: Ingestion of synthetic data into the data collector for CuriX. Step 2: Injecting anomalies. Step 3: Open the dashboard for CuriX. Step 4: Verify that all the dashboard components are displaying correctly and that the results are visible. Step 4: Open the S4RIS GUI and click on the links for CuriX. Step 5: Verify that all the dashboard components of CuriX are displaying correctly.

Expected Results	• Dashboard opens and contains the results from CuriX. • Dashboard opens within the S4RIS GUI. • Dashboard should be easier to use than the version before SAFETY4RAILS had started. Was qualitatively evaluated by persons not involved in the CuriX development.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	Some parts are only qualitatively assessable since appearance, easy to understand and use are not measurable by technical means / measures.

Test.-ID	CuriX_TR_05
Addressed Requirement	CuriX_05 **System resource optimization for the railway infrastructure** • Optimize resource used within the infrastructure • Enhance response time efficiency (IT, IoT and OT services) • Trigger capacity alerts
HW / SW preparation	NA
Test inputs	NA
Test procedure	NA
Expected Results	NA
Pass/Fail	NA
Deviation Encountered	
Problems	
Comments	This requirement was not addressed within SAFETY4RAILS.

Test.-ID	CuriX_TR_06
Addressed Requirement	CuriX_06 **CuriX dashboard to be provided multilingual** • Support Customer languages / Languages of end users • Implement translations tables to CuriX.Portal / Dashboard
HW / SW preparation	NA
Test inputs	NA
Test procedure	NA
Expected Results	NA
Pass/Fail	NA
Deviation Encountered	

Problems	
Comments	This requirement was not addressed within SAFETY4RAILS.

Test.-ID	CuriX_TR_07
Addressed Requirement	CuriX_07 **CuriX integration (connectors) to S4RIS and interface to other tools** • Follow the rules of interoperability (following the interoperability concept described in D2.4) • Provide a REST API (JSON) for data collection (measurement and log data exchange) • Provide a REST API (JSON) to transfer results (outage prediction) to S4RIS and customer specific monitoring tools. • Date integration to SAFETY4RAILS tools on Source Layer: e.g. Senstation, PRIGM, uni|MSTM, Ganimede • Date integration to SAFETY4RAILS tools on Data processing Layer: e.g. SARA, DATA FAN, WINGSPARK, SECURAIL, • Date integration to SAFETY4RAILSl tools on Decision support and Simulation: e.g. CaESAR, RAM2 • Definition of the import / export format • Definition of the data to be imported / exported
HW / SW preparation	See Test-ID CuriX_TR_01. In addition, the connection to the DMS (KAFKA) for the S4RIS is established. We agreed with partners on scenario specific event definitions, which we set up accordingly in CuriX.
Test inputs	See Test-ID CuriX_TR_01
Test procedure	Step 1: Ingestion of synthetic data into the data collector for CuriX. Making sure that the anomaly detector is being trained on data representing two weeks. Step 2: Set up a consumer and subscribe to a DMS topic with the Postman API platform. Step 3: Injecting anomalies which correspond to the threats envisioned by the simulation exercises by manipulation of the time-series values. Step 4: Open the dashboard for CuriX and verify that the anomalies have translated in the correct resilience issue (i.e., alarm) regarding the anomaly. Step 5: Poll via an API call the JSON messages to the subscribed topic from the DMS. Step 6: Verify the correctness of the published message Step 7: Let RAM² consume the published message for verification.
Expected Results	Messages of alarms seen at the message bus Messages consumable by other tools in the correct form (JSON)
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	Step 7 from the test procedure has been conducted in the light of the rehearsal and actual simulation exercises.

Test.-ID	CuriX_TR_08
Addressed Requirement	CuriX_08 **Hardening anomaly detection against data interruption**

	• Provide advanced anomaly detection for time series that re-ceive interrupted data; also named “multiple-step time series” (respecting time lags) • data processing respecting time interruptions which may well occur in S4RIS ecosystem
HW / SW preparation	See Test-ID CuriX_TR_01
Test inputs	See Test-ID CuriX_TR_01
Test procedure	Step 1: Ingestion of synthetic data into the data collector for CuriX. Step 2: Interrupt data flow to CuriX for at least more than 2 minutes. Step 3: Open anomaly detector to observe and verify that missing values are filled in the back end.
Expected Results	Interrupted values should be filled with the last observed value.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	CuriX_TR_09
Addressed Requirement	CuriX_09 **System intelligence and visualization** • Identification of critical system states for predefined subsystems • ITSM (IT Service Management) – Provide data of business domain, service domain and infrastructure domain in order to show dependencies • identification of root cause (root cause analysis)
HW / SW preparation	NA
Test inputs	NA
Test procedure	NA
Expected Results	NA
Pass/Fail	NA
Deviation Encountered	
Problems	
Comments	This requirement was not addressed within SAFETY4RAILS.

Test.-ID	CuriX_TR_10
Addressed Requirement	CuriX_10 **Conformity with overarching and S4RIS platform specific requirements**
HW / SW preparation	See Test-ID CuriX_TR_07
Test inputs	See Test-ID CuriX_TR_01

Test procedure	See Test-ID CuriX_TR_07
Expected Results	See Test-ID CuriX_TR_07
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

3.5 DATAFAN

3.5.1 Overview

The main functionalities of the DATAFAN tool are:

- Time-series forecasting using Deep Neural Networks:
    - The train passenger load is predicted on the basis of data from historical events with exceptional (and potentially critical) passenger loads.
    - The train passenger load is predicted for various stations of a railway or metro network.
- Graphical representation of a potential anomaly (in the prediction module) due to a significant divergence between predicted and actual or expected number of passengers (as identified in training data for prediction module).
- Analysis of what-if scenarios:
    - The target station is closed (i.e. blocked turnstiles at the gates) affecting surrounding stations and passenger traffic distribution.
- Operational support in re-directing passenger flow:
    - The free capacity of the surrounding stations as an additional property, which is calculated from the predicted number of passengers and an estimated station capacity.
    - A network graph that incorporates information on the geographic location of and distances to other interconnected stations. Different modes of transport as well as three station attributes can be selected.
    - A reliability score (RLS) for the results to help the end-user in the decision-making process and to support the technology acceptance.

3.5.2 Development and Quality standards adopted

The DATAFAN tool was developed as a demonstrator and is currently (status: 6th July 2022) at technological readiness level (TRL) 5.

For quality management, the development process was guided by agile practices and implemented using software development frameworks such as Kanban[8].

Data and code integrity during software development was ensured through the use of Git[9] and standard practices such as merge requests. No ISO standards or unit testing frameworks were implemented at this stage.

3.5.3 Data used for tests

Conforming to the data gathering methods described in D1.4, most of the data used for testing was collected by end-users involved in SAFETY4RAILS and shared. The following end-users shared data:

- **Metro de Madrid (MdM):** A dataset with number of passengers for the Metro of Madrid. The data includes information on 13 metro stations, namely Santiago Bernabéu, Lima, Tetuán, Estrecho, Cusco, República Argentina, Nuevos Ministerios, Concha Espina, Gregorio Marañón, Alonso Martínez, Chamartín, Plaza de Castilla and Tribunal, for a period of approximately one week during six major soccer events between September 2018 and March 2019 (Table 2). The passenger data was provided at 5-minute intervals for the total of all metro lines frequenting the respective station.

[8] Anderson, David J. (April 2010). *Kanban: Successful Evolutionary Change for Your Technology Business*. Blue Hole Press. ISBN 978-0-9845214-0-1.

[9] Git (git-scm.com)

TABLE 2: DATA FOR SIX MAJOR SOCCER EVENTS IN MADRID

From	To	Event	Number of Visitors[10]
20.09.2018	25.09.2018	22.09.2018: Real Madrid - Espanyol	67757
21.10.2018	26.10.2018	23.10.2018: Real Madrid – Viktoria Pilsen	67356
31.10.2018	06.11.2018	02.11.2018: Real Madrid – Real Valladolid	68050
27.09.2018	02.10.2018	29.09.2018: Real Madrid Atlético	78642
25.02.2019	03.03.2019	27.02.2019: Real Madrid - FC Barcelona (Cup)	78921
28.02.2019	05.03.2019	02.03.2019: Real Madrid - FC Barcelona	80472

- **EGO:** A dataset with number of passengers for the Metro of Ankara. The data includes information on five metro stations, namely Mili Kütüphane, Atatürk Merkezi, Kizilay, Necatibey and Sögütözü, for the period from 03/01/2019 to 03/15/2019, provided at 15-minutes intervals for the total of all metro lines frequenting the respective station.

Additionally, we used open data for some preliminary testing of our algorithms at the beginning of the SAFETY4RAILS project. The data was acquired before the end-user data became available. Although it was not used for the tests in D6.4, it was still critical to the overall development. The data was acquired from the following providers

- **Deutsche Bahn:** An open dataset with a Creative Commons Attribution 4.0 International (CC BY 4.0) license, with train passenger numbers for Hamburg, downloaded from the Deutsche Bahn data portal in November 2021. The data includes information on five stations of the S1 line, namely Hamburg Hauptbahnhof, Altona, Sternschanze, Reeperbahn and Jungfernstieg, for the period from 12/11/2016 to 03/31/2017, provided at approximately 1-hour intervals.

In order to obtain time and distance information between a set of locations (origins and destinations), we collected shared open data using the following services:

- **OpenRouteService:** Extract a time-distance matrix for the transportation modes walking, car and cycling via API call. A more detailed description of the service can be found at https://openrouteservice.org.
- **Google Maps:** Manual extraction of time-distance information for the means of transport train/tram, bus and metro of the EGO use case from Google Maps on Monday, May 23rd 2022 at around 9 am.

Furthermore, we generated partially artificial data for the bus, tram/train and metro time-distance information of the remaining use cases (MdM, RFI and CdM). For this purpose, the walking distance consumed from OpenRouteService for the respective station was multiplied by a factor of 0.2, 0.5 and 0.7 for the transportation modes metro, train and bus, respectively.

The entirety of all data provides the basis for the previously defined tests. Without exception, these were carried out several times (>= 3).

3.5.4 Test Data Report

This section reports the tests executed for DATAFAN, based on requirements described in D1.4 par. 2.3.5.

Test-ID	DATAFAN_TR_01
Addressed Requirement	DATAFAN_TR_01 **Reliable and understandable Machine Learning (ML)- based results** • ML-based results clearly show used algorithms and methods • Clear explanation of algorithms and methods • Percentage values indicate reference of the results on the referred methods

[10] Source: Bernabéu nur einmal ausverkauft: Gründe für Reals Zuschauerschwund

	- Degree of reliability indicates reference to applied methods - Aim: to enhance technology acceptance
HW / SW preparation	Open the DATAFAN tool using the DATAFAN.exe on a standard Windows PC (no special hardware is required)
Test inputs	None
Test procedure	**Step 1:** Select one of the available use cases (e.g. MDM, EGO, RFI, CDM). **Step 2:** Skip this page and directly move on to page 3 using the [next >>] button. **Step 3:** Select any station and event (or day and time interval) from the dropdown menus on the left side of the tool page 3 ("Select prediction Options") of the GUI. **Step 4:** Select a value for the algorithm parameters "number of epochs" and "number of Monte Carlo simulations" on the right side of tool page 3. Start the prediction. **Step 5:** Once the prediction is completed, skip page 4 of the tool using the [next >>] button and directly move on to tool page 5 to check the "Overall Performance" of the prediction. **Step 6:** Verify that the parameters match those previously selected for the algorithm and methods. **Step 7:** Verify that the key performance metrics are displayed on tool page 5, including the mean absolute percentage error. **Step 8:** Verify that on tool page 6 individual scores and a final reliability score (RLS) are displayed.
Expected Results	- The selected parameters for the algorithm and methods match the information on tool page 5 (Step 6). - The key performance metrics provide information about the quality of the results (Step 7) - The overall reliability of the results is provided by the RLS (Step 8)
Pass/Fail	Pass
Deviation Encountered	None
Problems	None identified
Comments	Internally tested several times

Test-ID	DATAFAN_TR_02
Addressed Requirement	DATAFAN_02 **High prediction performance of results, e.g. anomaly detection** - Applied algorithms e.g. for anomaly detection achieve a high prediction performance - The better and more precise the data, the better the predictions - Percentage values indicate reference of the results on the referred methods - Degree of reliability indicates reference to applied methods - Aim: to enhance technology acceptance
HW / SW preparation	Open the DATAFAN tool using the DATAFAN.exe on a standard Windows PC (no special hardware is required)
Test inputs	None
Test procedure	**Step 1:** Select EGO from the available use cases on tool page 1. **Step 2:** On tool page 2, select the following event from the data: - Station = Milli Kütüphane - day = Wednesday

	- Time interval = From 7:00 to 9:00 **Step 3:** Run a prediction with the following parameters on tool page 3: - Number of epochs = 30 - Number of Monte Carlo Simulations = 100 Once completed, skip tool page 4 and 5 by clicking the [next >>] button and continue to the results on tool page 6 of the GUI. **Step 4:** Check the results of the applied algorithm for time series forecasting, which are summarized on tool page 6. **Step 5:** Make sure, the individual and the final reliability scores are acceptable and represent a high prediction performance. **Step 6:** Refer to the graphs for more detailed information on the forecast and its trustworthiness. **Step 7:** If necessary, improve the results by going back to tool page 3.
Expected Results	- RLS score > 0.5 - S_distance > 0.7 - S_xAI > 0.75 - The graph shows a good fit between predicted and actual data
Pass/Fail	Pass
Deviation Encountered	None
Problems	None identified
Comments	Internally tested several times.

Test-ID	DATAFAN_TR_03
Addressed Requirement	DATAFAN_03 **Software application with a user friendly interface** - Clear user interface - The user will be directed through the software and the single steps to apply the software - The used algorithms and functionalities will be briefly explained to the user - Clear presentation and visualization of the results and hints to improve the results - Aim: The end-user should be able to use the software with “normal” technical knowledge
HW / SW preparation	Open the DATAFAN tool using the DATAFAN.exe on a standard Windows PC (no special hardware is required)
Test inputs	None
Test procedure	**Step 1:** Wait for the tool wizard to load. **Step 2:** Follow the wizard page header instructions as guidance for the action required by the user (e.g. select input Options; tool pages 2-6). **Step 3:** Select and click on any of the gray boxes, which are generic placeholders for a given choice in the tool (e.g. MDM, EGO, RFI or CDM use case). **Step 4:** Navigate through the GUI using the "next" and "back" button. **Step 5:** If necessary, use the tooltip explanations for the parameters by hovering over their names with the mouse. **Step 6:** Use the drop-down menus to select the data (tool page 2 and 3), algorithm parameters (tool page 3) and network graph parameters (tool page 4). Use the default values as guidance. On tool page 3, run a prediction with parameters of your choice.

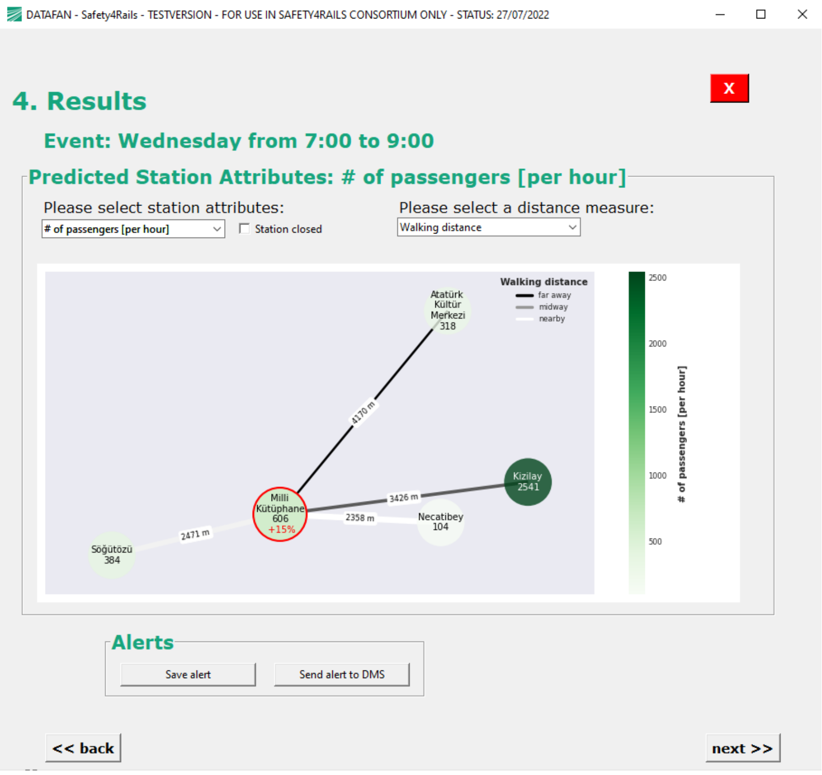
	Step 7: The results regarding the passenger numbers, overall performance and reliability metrics are visualized and presented on tool page 4, 5 and 6, respectively. **Step 8:** Follow the hints on page 6 to improve the results.
Expected Results	• The selected gray boxes turn green (Step 3) • The drop-down menu returns a list of possible parameters (Step 6): ○ On tool page 2, the data overview plots are updated according to the selection ○ On tool page 4, the selected station attribute and the distance measure is displayed in the network graph • The defaults in the drop-down menus are all visible and have the following values (Step 6): ○ Number of epochs = 10 ○ Number of Monte Carlo Simulations = 10 ○ Selected station attribute = Capacity [per hour] ○ Selected distance measure = Walking distance
Pass/Fail	Pass
Deviation Encountered	None
Problems	None identified
Comments	Internally tested several times.

Test-ID	DATAFAN_TR_04
Addressed Requirement	DATAFAN_04 **How to use the software** • Clear explanation for the end-user to apply the different functionalities • The user will be guided through the software and the single steps to apply the software • The used algorithms and functionalities will be briefly explained to the user • The user does not have to be an expert in ML-algorithms, but a good technical knowledge is of benefit • Aim: The end-user should be able to use the software with “normal” technical knowledge
HW / SW preparation	Open the DATAFAN tool using the DATAFAN.exe on a standard Windows PC (no special hardware is required)
Test inputs	None
Test procedure	**Step 1:** Follow the wizard page header instructions as guidance for the action required by the user (e.g. select input Options, select prediction options, etc.). **Step 2:** Select EGO from the available use cases on tool page 1. **Step 3:** Keep the default settings on tool page 2 and use the [next >>] button to directly move to tool page 3. **Step 4:** Check the tooltip explanations for the algorithm parameter “Number of Monte Carlo Simulations” by hovering over the names with the mouse. **Step 5:** Start the prediction with the default settings and wait for it to finish (wait for the green button “Go to results”).
Expected Results	• The “EGO use case” button turns green on tool page 1 (Step 2). • The tool tip on tool page 3 should read “The number of Monte Carlo simulations determines the number of predictions for randomly sub-networks.” (Step 4). • The “Go to results” button on tool page 3 is turning green (Step 5).

Pass/Fail	Pass
Deviation Encountered	None
Problems	None identified
Comments	Internally tested several times.

Test-ID	DATAFAN_TR_05
Addressed Requirement	DATAFAN_05 **Moderate hardware requirements for using the software** • Usable on a common laptop in the field • Usable without special technical requirements • Contains a toolbox of predefined datasets to evaluate a certain pre-specified task properly (also without a WIFI connection) • Aim: The end-user should be able to use the software without any special requirements**.**
HW / SW preparation	Standard Laptop, e.g.: • Processor: Intel(R) Core(TM) i7-10510U CPU @ 1.80GHz 2.30 GHz • RAM: 16 GB • No dedicated GPU required
Test inputs	None
Test procedure	**Step 1:** In the systems settings, select “100 %” for the appearance size of text and apps. **Step 2:** Execute DATAFAN.exe available via the S4RIS platform -> Milano Exercise -> DATAFAN (Please send an email to a Fraunhofer EMI project member for the password) **Step 3:** Select one of the predefined datasets (e.g. EGO use case). **Step 4:** Select data and algorithm parameters appropriate to the task. **Step 5:** Start the prediction.
Expected Results	• The DATAFAN tool starts with a banner showing a moving train. The actual wizard menu window opens with a short delay. • There are several datasets (use-cases) the user can select from on the first tool page. • The prediction runs successfully, indicated by the "next" button on tool page 3 turning green to “Go to results”. • The prediction is made in a reasonable amount of time (< 15 minutes).
Pass/Fail	Pass
Deviation Encountered	None
Problems	None identified
Comments	Internally tested several times.

Test-ID	DATAFAN_TR_07
Addressed Requirement	DATAFAN_07 **Manner of the applied anomaly detection** • Detection of outliers, i.e. anomalies which are only sparsely contained in the data set used for training • Detection of novelties, i.e. anomalies which are not contained in the data set used for training

	- Usage of different ML algorithms such as Isolation Forests, One-class SVM or Local Outlier Factor, Autoencoder based anomaly detection
HW / SW preparation	Open the DATAFAN tool using the DATAFAN.exe on a standard Windows PC (no special hardware is required)
Test inputs	None
Test procedure	**Step 1:** Select one of the available use cases (e.g. MDM, EGO, RFI, CDM) on tool page 1. **Step 2:** Keep the default settings on tool page 2 and use the [next >>] button to directly move to tool page 3. **Step 3:** Start the prediction with the default settings on tool page 3 and wait for it to finish. **Step 4:** Once the prediction is completed, move to tool page 4 by using the green button [Go to results]. **Step 5:** Select the "# of passengers [per hour]" option from the "Select station attribute" drop-down menu. The graph will update and the target station at the center of the network graph will be highlighted by a red circle. In addition, a red "+15%" is displayed in the text of the central station, which indicates the degree of deviation of the (fictitious) anomaly in comparison to the normal situation of expected passengers.
Expected Results	The network graph for the station attribute "# of passengers [per hour]" on tool page 4 features: - A red circle around the central stations' node - A red "+15%" is displayed in the text of the central stations' node  DATAFAN - Safety4Rails - TESTVERSION - FOR USE IN SAFETY4RAILS CONSORTIUM ONLY - STATUS: 27/07/2022 **4. Results** **Event: Wednesday from 7:00 to 9:00** **Predicted Station Attributes: # of passengers [per hour]** Please select station attributes: # of passengers [per hour] □ Station closed Please select a distance measure: Walking distance **Alerts** X Walking distance far away midway nearby Atatürk Kültür Merkezi 318 4170 m Kizilay 2541 3426 m Milli Kütüphane 606 +15% 2358 m Necatibey 104 2471 m Söğütözü 384 2500 2000 1500 1000 500 # of passengers [per hour] Save alert Send alert to DMS << back next >>
Pass/Fail	Pass
Deviation Encountered	None
Problems	None identified
Comments	Up to this date (status: July 1st 2022), no anomaly detection has been implemented. However, a first step towards the integration was taken with a feature for visualizing a potential anomaly.

Test Results Considerations

Some of the tool tests formulated on the basis of the requirements in D1.4 par 2.3.5 do not fully reflect the current development status of the DATAFAN and therefore do not apply. Accordingly, no meaningful test procedures could be formalized for DATAFAN_TR_06, DATAFAN_TR_08 or DATAFAN_TR_09. This chapter addresses the actual development status (as of July 1st 2022) of the tool and the features in question.

Test ID: DATAFAN_TR_06 - Web Service for computation of expensive ML-algorithms

- Usable by the DATAFAN software on a common laptop, without special technical requirements
- Contains a toolbox of predefined datasets to evaluate a certain pre-specified task properly
- Provides the functionality to evaluate also expensive ML-algorithms
- Aim: The end-user should be able to evaluate expensive ML-algorithms without an own special technical equipment

No web service is provided for DATAFAN due to development time constraints. At this stage of the development phase (TRL 5), the DATAFAN tool can be downloaded as a .zip-file (which contains an executable) from the S4RIS platform > Milano exercise. Furthermore, a user-friendly manual and step-by-step tutorial to set-up a first full scenario is provided via the same link.

Please refer to Test 2 and 5 for evaluating a predefined task and dataset, and testing the technical requirements.

Test ID: DATAFAN_TR_08 - Requirements for the used data

- For a classification task, roughly 5000 instances per class are needed to solve the classification task properly; this number can vary according to the specific task which is to be solved.
- For real-time monitoring, data has to be continuously provided.

No real-time monitoring is implemented in the DATAFAN tool yet. Only the data provided for the four different use cases (MDM, EGO, RFI and CDM) and corresponding simulation exercises are available in the tool.

Furthermore, the DATAFAN tool was not used for any classification tasks during the SAFETYRAILS project.

Test ID: DATAFAN_TR_09 – Conforming with overarching and S4RIS platform specific requirements

- Ensure that any work connected with this tool conforms to the overarching and S4RIS platform specific requirements

No development carried out in SAFEYT4RAILS which would negates the possibility or makes it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s).

3.6 Ganimede

3.6.1 Overview

Ganimede is the Leonardo platform for the large-scale analysis of live and recorded data streams based on Deep Learning. Ganimede is implemented exploiting Leonardo's extensive know-how in Video Analysis, in IT platforms and security, supported by competence centers specialized in artificial vision and deep learning.

Key Features

Ganimede Video Content Analysis platform enhances situational awareness and transform threat detections from a manual, resource-intensive operation into an efficient and automated process.

It is designed and developed to:

- provide a unique platform for audio/video analysis
- have a unique framework deployable for Data Center, edge computing, automotive.

Scalability and Flexibility

The platform can support different usage patterns:

- an online video processing component for analyzing, recording and generating real-time alerts towards an event management platform.
- an offline video processing component for analyzing videos after events.
- Ganimede can be deployed in different configuration supporting different workloads an operational context:
- Data center centralized architecture serving extended areas in a centralized architecture
- Edge computing where optimized bandwidth management and distributed autonomy is required, such as for intelligent applications in LTE/5G environments.

Thanks to its flexibility and scalability features, users of the platform will be able to:

- Make the outcome of processed video available.
- Configure the sending of events associated with patterns detected by specific algorithms.
- Create tasks by dynamically allocating algorithms to configured video streams.
- Dynamically allocate tasks based on available resources.

3.6.2 Development and Quality standards adopted

The development process adopted in Leonardo is based on an internal **Design and Development Framework.**

This framework covers different approaches to design and development, with different management and control methodologies. Each project will choose the most appropriate reference model and adapt it to the nature of the development.

The reference models used in the Framework are:

- "V" model
- "Agile" model
- "Incremental" model

The "**V-model**" is a graphic representation of the life cycle of a product in which on the left side there are the phases related to requirements, design and implementation, while on the right side those relating to verification, integration and validation. Horizontal links represent the link between verification activities and what is verified. The V-model can be used for projects of any size and complexity, it is best suited to projects where the requirements are clearly defined in the beginning.

The **Agile model** is best suited to the scenario where the requirements will be developed iteratively; the ability to use an agile model is largely determined by the ability to define a system architecture where user functionality can be created in small steps. This model can only be applied if all stakeholders, and in particular the customer, are actively involved in all phases of the process.

The use of **Incremental Model** favors the creation of prototypes, that is working application parts, which in turn favor the dialogue with the customer and the validation of the requirements through incremental testing and integration. It is particularly suitable when the complete specification of requirements is not available at the outset and requirements are likely to be refined based on the experience of the previous increment.

The incremental model was considered the most suitable for the development of the new functions of Ganimede for the SAFETY4RAILS project.

For what concerns the software documentation, it is based on MIL STD 498g[11] Standard that requires the production of the following documents: SRS (System Requirement Specification), SSDD (System /Subsystem Design Description), SDD (Software Design Description) IRS (Interface Requirement Specification) and STR (Software Test Report).

The quality standard adopted is AQAP 2105[12].

3.6.3 Data used for tests

In order to test the functionalities of Ganimede diverse types of data has been used depending on the particular function to be tested.

The tool has been deeply tested with ad-hoc synthetic data created for this purpose. The following table describes the type of data used for the four different functionalities developed for SAFETY4RAILS project.

TABLE 3: AUDIO PATTERN DETECTION TEST DATA

Type	Audio streams in the form of .mp3 or .wav files.
Source	These files are provided for test purpose by a single microphone or an array of microphones depending on the test setting
Amount / Number of time tests performed	Neural network model is trained on a dataset that provides over 4K video samples with gunshot events. The model is validated using 20% of the dataset and tested on 10% of the dataset. The remaining 70% is used for training only

TABLE 4: ABANDONED BAGGAGE DETECTION TEST DATA

Type	Video stream in the form of .mp4 files provided by
Source	Surveillance cameras from different vendors
Amount / Number of time tests performed	The temporal and spatial constraints depend on the camera point of view and the FPS. The experiments were conducted in a controlled environment. The next steps are aimed at ensuring scalability in the operational environment. The system has been tested on various (20+ samples) videos from publicly available dataset for abandoned object detection and on 10 videos recorded in laboratory

TABLE 5: PEOPLE RE-IDENTIFICATION TEST DATA

Type	Video stream in the form of .mp4 files by surveillance cameras from different vendors
Source	Surveillance cameras from different vendors
Amount / Number of time tests performed	The system has been tested on 20+ video samples recorded in laboratory

[11] Reed Sorensen (June 1996). "MIL-STD-498, J-STD-016, and the U.S. Commercial Standard". CrossTalk Magazine. Archived from the original on 2004-12-16.

[12] https://www.bundeswehr.de/resource/blob/133194/86cdf56ee04a00f8e43172762973c6fa/aqap-2105-2019-eng-data.pdf

TABLE 6: MAN DOWN TEST DATA

Type	Video stream in the form of .mp4 files
Source	Surveillance cameras from different vendors
Amount / Number of time tests performed	The man down detection relies on person detection itself. If there are occlusions that prevent person detection, nor the man down detection is feasible. The system is meant to raise an alarm if a person is down and nobody is there. If there is a crowd of people around the man down, no alarm is raised because occlusion prevent the system to work properly. The system has been tested on 20+ video samples recorded in laboratory

3.6.4 Test Data Report

This section reports the tests executed for Ganimede, based on requirements described in D1.4 par. 2.3.6.

Test.-ID	*GAN-TR-01*
Addressed Requirement	Ganimede_1 Audio pattern detection Evaluation of AI models for audio pattern detection
HW / SW preparation	Recording of different types of audio stream (gun shots, screams, sirens etc.)
Test inputs	Different types of audio streams
Test procedure	Step 1: Read the audio streams and extract Mel Spectrograms at constant time intervals with proper overlapping Step 2: Detect relevant audio pattern like screams, gun-shots and similar within the spectrogram Step3: Notify the occurrence of relevant audio patterns
Expected Results	The system outputs the detected audio pattern and the timestamp in which it occurs within the audio stream
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	*GAN-TR-02*
Addressed Requirement	Ganimede_2 Enhanced abandoned baggage detection Evaluation of AI models for abandoned baggage detection in a real scenario
HW / SW preparation	Calibration is needed, since there are constraints that depend on the camera's point of view. It is required to know the real dimension of some object in the scenario to have references in order to compute actual distances
Test inputs	Video streams from surveillance camera
Test procedure	Step 1: Detect objects and people in a given frame with CNN Step 2: Check if objects are moving (carried) Step 3: If an object is standing still and there are no people around within a certain distance threshold, the object is candidate for abandon Step 4: Raise an alarm if this condition remains for more than a certain time threshold

	Step 5: Apply homographic transformation to retrieve position of detected object on a Cartesian plane Step 6: Compute distance between pixel and mapping back to actual distance since real dimension of the floor are known Step 7: Notify abandonment event with location of the object and ID of the person who dropped it
Expected Results	An alarm should be raised if there is an abandoned object in the camera field of view
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	The temporal and spatial constraints depend on the camera point of view and the FPS. The experiments were conducted in a controlled environment. The next steps are aimed at ensuring scalability in the operational environment

Test.-ID	*GAN-TR-03*
Addressed Requirement	Ganimede_3 People re-identification Evaluation of AI models for people re-identification
HW / SW preparation	The system must be fed with the probe which it need to retrieve within the video stream
Test inputs	Video streams from surveillance cameras
Test procedure	Step 1: Extract a feature vector from the probe with a dedicated neural network Step 2 Detect people within the field of view of the cameras with a CNN Step 3: Extract the features as in step 1 from all detections Step 4: Compute L2 distance between the probe feature vector and all the vectors extracted from step 3. Step 5: Sort matches based on the calculated distance value
Expected Results	The system outputs the best matches and the timestamp in which it occurs within the video stream
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	*GAN-TR-04*
Addressed Requirement	Ganimede_4 Man down Evaluation of AI models for man detection
HW / SW preparation	
Test inputs	Video stream from surveillance cameras
Test procedure	Step 1: Detect people within the field of view of the cameras with a CNN Step 3: Detect person pose (standing or lying)

	Step 2: Raise an alarm if the person detected falls on the ground
Expected Results	An alarm should be raised if there is a man down in the field of view of the camera
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	As described in Table 6: man down test data man down detection relies on person detection itself. If there are occlusions that prevent person detection, nor the man down detection is feasible. The system is meant to raise an alarm if a person is down and nobody is there. If there is a crowd of people around the man down, no alarm is raised because occlusion prevent the system to work properly.

3.7 iCrowd

3.7.1 Overview

The iCrowd platform is an agent-based crowd simulator, capable of simulating large scale crowds (up to tens of thousands of agents). It can be utilized for scenarios in any bounded area, such as buildings' interior and exterior, stadiums, open-air festivals and public areas of increased traffic.

iCrowd is a fully-featured simulation tool regarding the physical level of behaviour modelling, based on biometric attributes like mass, velocity, geometry, as well as the interaction between agents during their movement by performing collision avoidance among them for a realistic representation. Interaction between agents is also possible in the cognitive and decision-making level, where the behaviour of one affects the behaviour of the other.

iCrowd utilizes the concept of Behaviour Trees to model agents' intelligence regarding special-purpose intentions and targets. Behaviour Trees are a well-established modelling technique widely used in Artificial Intelligence and game development domains. This technique is widely used in the design and implementation of intelligent software systems that must exhibit complex behaviours in a modular fashion.

In the context of SAFETY4RAILS, the iCrowd simulator has been used for the detection of possible vulnerabilities in multi-modal railway and metro stations, the extraction of useful metrics for their evaluation, and, by doing so, provides a risk assessment tool to develop better resilience strategies for the safety and security of the users of such infrastructures.

This was achieved by simulating the impact of cyber-physical threats on metro and railway stations, taking into account the crowd's behaviour, external interconnected infrastructures, simulating realistic information propagation models, while using the infrastructure's current surveillance and security policies, such as evacuation processes, CCTV systems, security personnel positioning, etc.

More information regarding the architecture of the iCrowd simulator, its role in the SAFETY4RAILS platform, and the functionalities that were added to it as part of this project, can be found in Deliverables D5.2 and D5.7.

3.7.2 Development and Quality standards adopted

iCrowd is based on an extensible architecture that separates core services from the individual layers of agent behaviour, offering a concrete simulation kernel designed for high-performance and stability. It is based on a modular architecture that builds on the Entity-Component design paradigm, where live Entites have very basic functionality, and complex behaviors are provided by plug-in modules that attach their own Components at the Entities they wish to affect. This allows the separation of the core services of the simulation engine from the distinct Layers that comprise each entity's profile and behaviour.

Thus, the main processing kernel that deals with resource allocation and processing synchronization is separated from the individual behaviour implementations that usually deal with higher level functionalities (steering, pathfinding, intelligence, communications etc.). The simulation engine acts as an orchestrator for the distinct Layers, which may function individually or in cooperation with one another.

This modular design enables safe and quick design and implementation of new functionality in the form of modules. New modules are developed for each aspect of the simulation, and they are loaded and executed independently. Of course, modules are allowed to communicate with each other to provide rich and realistic behaviors, but the implementation details of each function are abstracted for the rest of the program. The main simulation kernel offers communication and synchronization mechanisms, allowing the safe and robust exchange of information between modules.

While the iCrowd simulator offers quite complex functionalities, internally everything is separately designed, implemented, and tested. Unit testing is facilitated using the C++ Catch2 framework offering concrete verification of low-level operations and data structures. More complex testing of modules and behaviors is accomplished using specialized test scenarios. These load and setup the needed modules, usually use a simple white-plane 3D model, create the necessary conditions to trigger and test various functionalities, and report on themselves by setting an appropriate exit code. Both unit testing and scenario testing is automated.

3.7.3 Data Used for tests

The following table lists characteristics of data used for tests:[13]

TABLE 7 DATA CHARACTERISTICS FOR ICROWD TESTING

Data	Type	Source	# of uses/tests
White-plane model	3D model	Generated by NCSRD	2
Madrid 1 metro station model	3D model	Generated by MDM and NCSRD	1
Madrid 2 metro station model	3D model	Generated by STAM	1
Madrid 1 outdoor model	3D model	Generated by RINA and NCSRD	1
Ankara metro station model	3D model	Generated by EGO	1
Camera locations	List of locations	Artificially generated by NCSRD	1
Guard locations and partol routes	List of lists of locations	Artificially generated by NCSRD	2

3.7.4 Test Data Report

This section reports the tests executed for iCrowd, based on requirements described in D1.4 par. 2.3.7.

Test.-ID	iCrowd_TR_01
Addressed Requirement	iCrowd _01 **Simulate Realistic crowd congestion levels**
HW / SW preparation	Collision avoidance and autonomous routing enabled for all agents
Test inputs	3D model of the Madrid 1 metro station Scenario with a large number of agents (2000) navigating and moving in and out of a relatively small area.
Test procedure	Step 1: Load iCrowd with the 3D model of an underground metro station *(done by the initialization script).* Step 2: Generate 2000 agents in random positions *(done by the initialization script).* Step 3: Schedule all agents to periodically choose a random target point and move towards it *(done by the initialization script).* Step 4: Stop the simulation once it reaches 10 minutes of simulated time.
Expected Results	Agents should move around the environment without bumping into each other. Routing should take into account the congestion levels of given areas.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	iCrowd_TR_02
Addressed	iCrowd _02

[13] Name of specific stations/locations redacted.

Requirement	**Simulate an evacuation because of terrorism (bomb, gas release) or natural disaster (fire, flood)**
HW / SW preparation	Collision avoidance and autonomous routing enabled for all agents.
Test inputs	3D model of the Madrid 1 outdoor area Scenario with a large number of agents (3000) walking around in an outdoor area and a bomb planted at a predetermined location near the crowd. The bomb's detonation causes an evacuation.
Test procedure	Step 1: Load iCrowd with the 3D model of an outdoor area *(done by the initialization script)*. Step 2: Generate 3000 agents in random positions *(done by the initialization script)*. Step 3: Schedule all agents to periodically choose a random target point and move towards it *(done by the initialization script)*. Step 4: When the simulated time reaches 5 minutes, detonate bomb, and notify BB3D to start the explosion simulation. Step 5: Wait for results from BB3D *(done by iCrowd)*. Step 6: Apply results containing injuries and disabled infrastructure elements *(done by iCrowd)*. Step 7: Wait for all agents to reach a safe area. Step 8: Stop the simulation.
Expected Results	After step 6, all agents that are not fatally injured must immediately start moving towards the closest safe area. Fatally injured agents must be disabled and stop moving. Agents should move around the environment without bumping into each other. Routing should take into account the congestion levels of given areas.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	iCrowd_TR_03
Addressed Requirement	iCrowd _03 **Simulate crowd behaviour considering cyber agents (electronic boards)**
HW / SW preparation	Collision avoidance and autonomous routing enabled for all agents.
Test inputs	3D model of a white-plane area Scenario with a small number of agents (20) moving around a bare white-plane test area. A small number of entities (5) representing cyber-agents are generated uniformly around the environment. Each cyber-agent initially contains a spatial piece of information referring to an abstract point in space (randomly initialized). Agents initially have no spatial information.
Test procedure	Step 1: Load iCrowd with the test 3D model of a white-plane *(done by the initialization script).* Step 2: Generate 20 agents and 5 cyber-agents in random positions *(done by the initialization script)*. Step 3: Assign a random point of the environment to cyber-agent as its initial information *(done by the initialization script)*. Step 4: Schedule all agents to periodically choose a random target point and move towards it *(done by the initialization script)*. Step 5: Visually inspect the current spatial piece of information of each agent in

	the form of an arrow starting from the agent and ending at its currently known abstract point, if one exists. Step 6: Stop the simulation when the spatial information of all agents (visually shown by their arrows) has converged to a single point.
Expected Results	During step 5, as the agents move around and get in the information broadcast zone of other (cyber-)agents, their known spatial information should be updated as the average of their current and new pieces of information. If they currently have no information, then they copy the information of their neighbour. The spatial information of all agents should naturally converge to a single point in space, which must be the average point of all cyber-agents. The information held by cyber-agents should never change.
Pass/Fail	Pass
Deviation Encountered	The final point at which the knowledge of all agents has converged to might not be exactly the average of the points that are broadcast by the cyber-agents. This might happen if the information converges too fast for all agents to walk by all cyber-agents and receive their information. The information of some cyber-agents might end up dominating the information propagation process, so the final point will be closer to theirs. This is expected.
Problems	
Comments	

Test.-ID	iCrowd_TR_04
Addressed Requirement	iCrowd _04 **Detect blind spots because of guards' movements and insufficient cameras**
HW / SW preparation	Collision avoidance and autonomous routing enabled for all agents.
Test inputs	3D model of the Madrid 2 underground metro station Scenario with a small number of agents (20) moving around a medium sized area (a multi-floor underground metro station). A small number of entities representing cameras (2) and mobile guards (2) are generated at predetermined locations with preset settings (field-of-view, maximum distance). A malicious agent is generated at a random location.
Test procedure	Step 1: Load iCrowd with the 3D model of a multi-floor underground metro station *(done by the initialization script)*. Step 2: Generate 20 agents, 2 guards, and 1 malicious agent in random locations. Generate 2 cameras at predetermined locations *(done by the initialization script)*. Step 3: Schedule all agents and guards to periodically choose a random target in space and move towards it *(done by the initialization script)*. Step 4: Visually inspect the malicious actor avoids walking into the visibile areas of guards and cameras as it moves through the environment. Step 5: When the behavior of the malicious actor has been verified, stop the simulation. Step 6: Visually inspect the resulting heatmaps generated by iCrowd that show the overall, average, and history of area coverage by cameras and guards throughout the environment.
Expected Results	During step 4, the malicious actor should be observed to avoid walking in front of static cameras and moving guards by following potentially non-optimal routes. As the guards move around, the malicious actor should continuously adapt its path accordingly. At step 6, the heatmaps should show 100% overall and average coverage for areas that are monitored by cameras, since they never move. The heatmaps showing the history of coverage throughout the simulation should contain only values of 0%, 50%, and 100%, referring to areas that are not covered at all, covered by at least one camera or guard but are highly congested, and perfectly

	covered respectively.
Pass/Fail	Pass
Deviation Encountered	
Problems	When a malicious agent finds itself in a situation where there is no route that completely avoids being seen by a camera or guard, it chooses the path with the least exposure. This is acceptable when we have only static cameras whose fields of view do not change, but may not reflect a realistic behavior of a malicious actor when their path is blocked by a moving guard.
Comments	Realistically, malicious agents' behavior should incorporate the fact that guards might move, so it can potentially wait for an opening. Moreover, since high congestion levels affect the performance of simulated cameras, malicious actors could incorporate this into their behaviors by choosing to move through a monitored area while mixing into the crowd in order to lower the probability of being detected.
Problems	
Comments	

Test.-ID	iCrowd_TR_05
Addressed Requirement	iCrowd _05 **Simulate access to a restricted area by cyber-attack (hackage or door) or physical attack (disabling a guard)**
HW / SW preparation	Collision avoidance and autonomous routing enabled for all agents.
Test inputs	3D model of the Ankara underground metro station Scenario with a small number of agents (20) moving around in a small area (an underground metro station) containing at least one room. 1 malicious actor is generated far away from the room's entrance. Initially, the entrance of the restricted room is blocked for all agents.
Test procedure	Step 1: Load iCrowd with the 3D model of an underground metro station containing at least one room *(done by the initialization script)*. Step 2: Generate 20 agents and 1 malicious actor in random locations outside of the restricted room *(done by the initialization script)*. Step 3: Schedule all non-malicious agents to periodically choose a random target and move to it *(done by the initialization script)*. Step 4: Manually instruct the malicious agent to walk into the restricted room. Step 5: Verify that the malicious agent cannot in fact walk into the room. Step 6: Manually unblock the entrance of the restricted room for the malicious agent, to simulate a cyber attack. Step 7: Verify that the malicious agent can now walk into the room. Step 8: Stop the simulation.
Expected Results	During step 5, the malicious agent should not be able to walk past the blocked entrance and into the restricted room. After step 6 and during step 7, the malicious agent should walk into the restricted room successfully and without the need for an additional manual reroute.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	iCrowd_TR_06
Addressed Requirement	iCrowd _06 **Guards' distraction simulation** - Examine the effects of ineffective guards (due to distractions) on the station's security and safety - Verify that even with distracted guards, there are sufficient safety measures to prevent accidents or malicious behaviour
HW / SW preparation	Collision avoidance and autonomous routing enabled for all agents.
Test inputs	3D model of a white-plane area Scenario with 1 guard and 1 malicious actor in a bare white-plane test area. Initially, the guard's field of view and maximum detection distance are set to predetermined values.
Test procedure	Step 1: Load iCrowd with the test 3D model of a white-plane *(done by the initialization script).* Step 2: Generate 1 guard and 1 malicious actor in random positions *(done by the initialization script)*. Step 3: Schedule the malicious actor to periodically choose a random point and move towards it *(done by the initialization script)*. Step 4: Schedule the reduction of the guard's performance level, field-of-view, and max detection distance periodically, to simulate fatigue *(done by the initialization script)*. Step 5: Stop the simulation once the expected results have been obtained.
Expected Results	During step 4, the guard's field-of-view should be correctly updated and the malicious actor should take advantage of the reduced field-of-view.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	The fatigue effect causing the reduction of the guard's detection settings should be supported natively by the simulator instead of being programmed externally by the scenario, to allow for better control over many guards with different reduction factors.
Problems	
Comments	

Test.-ID	iCrowd_TR_07
Addressed Requirement	iCrowd _07 **Conformity with overarching and S4RIS platform specific requirements**
HW / SW preparation	N/A
Test inputs	N/A
Test procedure	N/A
Expected Results	See Deliverable D1.4 section 2.2.
Pass/Fail	Pass (see comments)
Deviation Encountered	

Problems	
Comments	P-01: The tool is modular (see previous sections and deliverables D5.2 and D5.7) P-02: Any information given by the user to the tool is relayed to other tools that needed (such as BB3D for bomb detonation simulation) P-03: The tool is configurable by the user using a Lua script. P-04: The tool provides a manual in PDF format. P-05: N/A P-06: Input data is given in text files following Lua syntax. P-07: Output data is provided graphically and is exported in CSV text files. P-08: The tool provides a network communication system that supports raw TCP streams, HTTP APIs, and is integrated with the platform’s DMS (Apache Kafka) P-09: The tool offers synchronization mechanisms through all of its network communication system’s interfaces. P-10: User-provided data is validated during initialization. P-11: The tool validates the working state of its modules and validates the response status codes of interconnected tools (BB3D) P-12: Simulation steps and events are sent to DMS to be archived. P-13: N/A P-14: N/A P-15: The tool provides a manual in PDF format. P-16: NCSRD can provide training sessions for the use of the tool (see Deliverable D5.2 section 3.5) P-17: The tool is executed on an isolated container (Docker) and can be accessed by the end-users through a web-based password-protected VNC client served over HTTPS. P-18: N/A P-19: N/A P-20: The tools has been integrated with DMS and uses it to facilitate its communication with other tools. P-21: N/A P-22: N/A P-23: The formats of messages posted on DMS regarding various events in the simulation have been defined and are strictly followed. P-24: The tool offers connectivity through raw TCP streams and HTTP APIs, independently of its integration in SAFETY4RAILS.
Problems	
Comments	

3.8 PRIGM

3.8.1 Overview

PRIGM was developed as a multipurpose Hardware Security Module (HSM) and improved for IoT-enabled secure cyber-physical communication and data storage in SAFETY4RAILS. As was demonstrated Ankara simulations and also at the laboratory scale, PRIGM presents end-to-end secure communication and data exchange over S4RIS. PRIGM presents a very high throughput enabling symmetric encryption of any travelling data within S4RIS (though this was not operationalised in SAFETY4RAILS). PRIGM operates at the server side enabling the fast encryption and decryption of data, e.g. sensory data collected from the endpoints or any service data gathered from the SCADA system. Thus, the operations of PRIGM become more meaningful if it co-operates with the systems at edge nodes, i.e. Senstation, where the data is generated. It is noteworthy that both PRIGM and Senstation are hardware devices providing backend services for S4RIS. See Section 3.13 for more details about Senstation.

3.8.2 Development and Quality standards adopted

PRIGM relies on the following standards and test criteria which are accepted as de facto in any information system:

1. The Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408[14]) for computer security certification. This standard is the widely adopted security standard for cryptographic devices assuring the holistic security and trustworthiness of the device at an international level.
2. NIST 800-22[15]: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. In any cryptosystem, the crypto algorithm and the device topology or circuitry are assumed to be open. However, the key generation scheme so as the random number generation method should be secret and rely on unpredictable and truly random numbers (Truly Random Number Generators - TRNG). NIST 800-22 is the widely adopted test criteria used for ensuring the key generation scheme is built on truly random numbers (not the pseudorandom numbers which can easily be hacked).

3.8.3 Data used for tests

Data used in NIST-800-22 True Randomness Test Suite:

- type(s): file with binary stream
- source(s): PRIGM HSM TRNG output
- amount(s): ~2 MB random bit stream
- number of times test(s) performed: 4

Data used in ned-to-end communication with a generic central control unit:

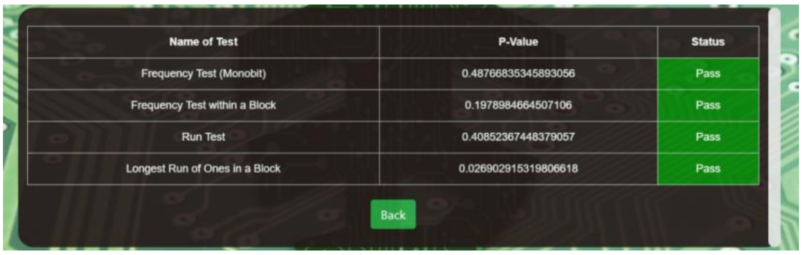
- type(s): system log file
- source(s): PRIGM HSM and host system logs
- amount(s): ~3-day live usage logs (~25MB)
- number of times test(s) performed: 2

3.8.4 Test data Report

This section reports the tests executed for PRIGM, based on requirements described in D1.4 par. 2.3.8

[14] ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, accessible via: https://www.iso.org/standard/50341.html

[15] SP 800-22 Rev. 1a, accessible via: https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final
A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications

<table>
<tr><td><b>Test.-ID</b></td><td>PRIGM_TR_01</td></tr>
<tr><td><b>Addressed Requirement</b></td><td>PRIGM _01
<b>PRIGM must have hardware encryption and random number generation modules</b>
To ensure that all crypto operations are performed on the hardware.</td></tr>
<tr><td><b>HW / SW preparation</b></td><td>• Operating System: Linux(x64) e.g. Ubuntu 16.04 and above
• Processor: 2 GHz, 2 cores or higher.
• Memory: 8 GB RAM or higher
• HDD: 5 GB of free disk space
<b>*Network interface</b>.</td></tr>
<tr><td><b>Test inputs</b></td><td>Test vectors are prepared as the outputs of PRIGM’s TRNG. Plain data and its encrypted forms.</td></tr>
<tr><td><b>Test procedure</b></td><td>Step 1: The TRNG randomness test is implemented by a test software that is developed by ERARGE according to NIST 800-22 test standard.
Step 2: AES-ECB encryption and decryption performance tests (throughput and latency) are implemented by POSTMAN-based HSM API via a proper network connection.</td></tr>
<tr><td><b>Expected Results</b></td><td><b>Randomness:</b> RNG output must pass the NIST 800-22 randomness test suite
<b>Throughput:</b> The throughput for encryption should be 1500 MBps and decryption 2000 MBps.
<b>Latency:</b> Encryption and decryption latency for the block cypher modes should be approximately 600 µs.</td></tr>
<tr><td><b>Pass/Fail</b></td><td>Passed
<b>Randomness:</b> RNG test results example (a snapshot from the evaluation software developed by ERARGE):

<table>
<tr><th>Name of Test</th><th>P-Value</th><th>Status</th></tr>
<tr><td>Frequency Test (Monobit)</td><td>0.48766835345893056</td><td>Pass</td></tr>
<tr><td>Frequency Test within a Block</td><td>0.1978984664507106</td><td>Pass</td></tr>
<tr><td>Run Test</td><td>0.40852367448379057</td><td>Pass</td></tr>
<tr><td>Longest Run of Ones in a Block</td><td>0.026902915319806618</td><td>Pass</td></tr>
</table>

<b>Throughput: AES ECB - Encription ~1700MBps ; AES ECB - Decryption ~1950MBps</b>
<b>Latency: AES ECB - Encription ~650µs ; AES ECB - Decription ~620µs</b></td></tr>
<tr><td><b>Deviation Encountered</b></td><td>Only a minor deviation is observed in AES EBC decryption performance but this had not caused any serious problem.</td></tr>
<tr><td><b>Problems</b></td><td>-</td></tr>
<tr><td><b>Comments</b></td><td>-</td></tr>
<tr><td><b>Problems</b></td><td>-</td></tr>
<tr><td><b>Comments</b></td><td>-</td></tr>
</table>

Test.-ID	PRIGM_TR_02
Addressed Requirement	PRIGM _02 **PRIGM must have a standardized API to connect to a computer** To communicate with PRIGM via OpenCryptoki and use all of its cryptographic functions
HW / SW preparation	PRIGM API runs on a virtual server with the following configuration: • Machine Type: Virtual Machine \w Ubuntu (64-bit) • OS: Ubuntu 18.04.4 LTS • CPU: Intel(R) Xeon(R) CPU E5-2620 v3 @ 2.40GHz Cores: 2 • RAM: 4GB Storage: 23GB
Test inputs	-
Test procedure	Step 1: Test vectors are implemented by a user via the PRIGM API.
Expected Results	The test vector's expected results matched exactly with the executed test results.
Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.
Problems	-
Comments	-
Problems	-
Comments	-

Test.-ID	PRIGM_TR_03
Addressed Requirement	PRIGM _03 **PRIGM should be connected to the end user's central control unit** Successful installation of PRIGM in the end user's control centre or any remote server acting like the end-users control centre
HW / SW preparation	PRIGM connects to the end users' server via Ethernet or PCIe interfaces. The connected server must have the following minimum HW/SW configuration: • Operating System: Linux(x64) Ubuntu 16.04 and above, • Processor: 2 GHz, 2 cores or higher. • Memory: 8 GB RAM or higher • HDD: 5 GB of free disk space • Network interface.
Test inputs	-
Test procedure	Step 1: The tester physically connects the PRIGM to the server Step 2: The device initialization procedure is applied. Step 3: A control test vector is used to check whether the cryptographic functions operate properly or not via the PRIGM config interface API
Expected Results	The test vector's expected results matched exactly with the control test results.
Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.

Problems	-
Comments	-
Problems	-
Comments	-

Test.-ID	PRIGM_TR_04
Addressed Requirement	PRIGM _04 **PRIGM should give service to end nodes and create outputs for end users** Verify that PRIGM is communicating with end nodes Provide secure data that the end-user can use in their daily services or for secure storage
HW / SW preparation	HW: PRIGM, Senstation Server PC that connects to PRIGM, Test computer to sniff the network, Ethernet LAN.
Test inputs	Any plain data. i.e. reading data from a sensor
Test procedure	Step 1: Plain data is sent by the server PC Step 2: PRIGM encrypts the plain data and sends the encrypted data to the end node Step 3: Senstation decrypts the received data and sends it back to the endpoint test computer Step 4: Original and decrypted texts are compared by a test engineer
Expected Results	Plain data on the server side must exactly be the same as the one on the test computer side.
Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.
Problems	-
Comments	-
Problems	-
Comments	-

Test.-ID	PRIGM_TR_05
Addressed Requirement	PRIGM _05 **PRIGM should work as a utility for the management of certification and IoT device authentication** Certify and authenticate the IoT devices, sensors or data collectors at nodes
HW / SW preparation	PRIGM, Server PC, Senstation (equipped with an IoT device, i.e. sensor(s))
Test inputs	-
Test procedure	Step 1: An IoT device mounted on Senstation tries to connect to any endpoint and sends its certificate and encrypts it by its private key Step 2: The endpoint having the Senstation’s certificate asks PRIGM to verify this certificate. Step 3: PRIGM returns to the endpoint as Senstation’s certificate is legit or not.
Expected Results	The certificate is validated, and the IoT end node device authentication procedure is completed successfully

Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.
Problems	
Comments	
Problems	
Comments	

Test.-ID	PRIGM_TR_06
Addressed Requirement	PRIGM _06 **PRIGM operations must be GDPR-compliant** The protection of any personal data is a fundamental right. The provided solution should encrypt the collected data if there is any personal data is transmitted.
HW / SW preparation	PRIGM, Server PC, IoT device (Senstation)
Test inputs	-
Test procedure	Step 1: A generic personal data is created that is supposed to be GDPR sensitive Step 2: The data is encrypted and sent to an endpoint. Step 3: The encrypted data is assumed to be stolen Step 4: An expert tries to find any meaningful information from the encrypted data.
Expected Results	Any GDPR-sensitive cannot be extracted from the secure channel between PRIGM and Senstation as the transmission channel is fully encrypted. Moreover, both PRIGM and Senstation meet the relevant security standards mentioned in Section 2.8.2
Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.
Problems	-
Comments	-
Problems	-
Comments	-

Test.-ID	PRIGM_TR_07
Addressed Requirement	PRIGM _07 **Conformity with overarching S4RIS platform-specific requirements**
HW / SW preparation	HW: PRIGM, ServerPC SW: KAFKA, RAM2
Test inputs	-
Test procedure	Step 1: A test data (i.e. sensory data) is generated by Senstation Step 2: Test data is assumed to be processed by any service over S4RIS Step 3: A posted message is sent by PRIGM and ServerPC in JSON format. Step 4: The JSON post message is received by the KAFKA tool then it propagates the message to RAM2 Step 3: RAM2 visualises the message on its online console.
Expected Results	The message is successfully sent from PRIGM to RAM2 tool and then visualized with proper messages on the RAM2 console.

Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.
Problems	-
Comments	-
Problems	-
Comments	-

3.9 RAM2

3.9.1 Overview

RAM², a Risk Assessment Monitoring & Management platform is an industrial-tailored Security Orchestration, Automation and Response (SOAR) platform. It offers a comprehensive, centralized, and automated industrial cyber risk management solution. RAM^2 platform delivers online relevant insights and mitigation procedures for the railway system operators.

The platform easily tracks a variety of production floor data sources (e.g., OT, IT, security logs and network data) and provides actionable views of operational network assets and alerts, based on powerful machine analytics. The operational team and operations security teams can use RAM^2 to effectively carry out day-to-day proactive risk mitigation tasks and respond to detected threats.

RAM² allows users to do the following:

- Manage all cyber-physical assets within the operational environment across operational processes, through an easily navigable hierarchical structure.
- Discover, identify and manage asset inventory within the context of the operational processes.
- Assess the cyber security posture and vulnerabilities, security gaps and exposures.
- Detect critical changes in the network in near real time.
- Perform intelligent risk prioritization to better handle threats by calculating the risk level from the single asset to the entire network.
- Automatically generate alerts when abnormal events and vulnerabilities are found in assets.
- Handle risks based on clear recommended mitigation

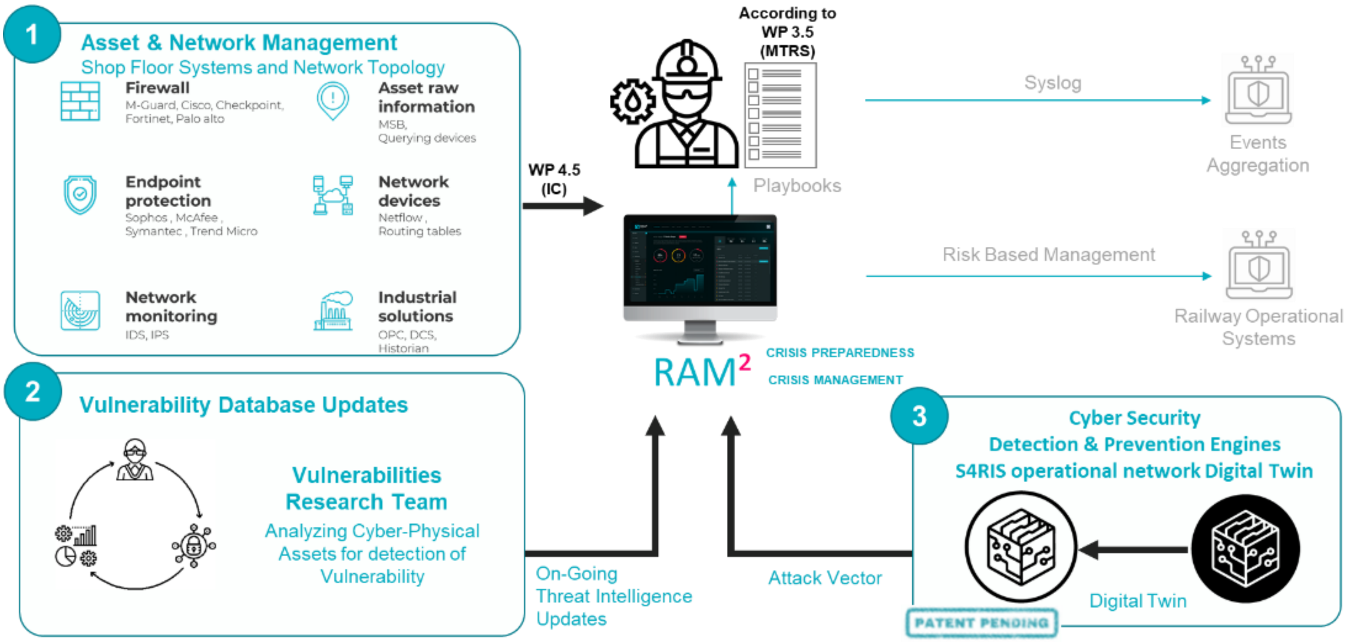

1
Asset & Network Management
Shop Floor Systems and Network Topology
Firewall
M-Guard, Cisco, Checkpoint, Fortinet, Palo alto
Asset raw information
MSB, Querying devices
Endpoint protection
Sophos , McAfee , Symantec , Trend Micro
Network devices
Netflow , Routing tables
Network monitoring
IDS, IPS
Industrial solutions
OPC, DCS, Historian
2
Vulnerability Database Updates
Vulnerabilities Research Team
Analyzing Cyber-Physical Assets for detection of Vulnerability
WP 4.5 (IC)
According to WP 3.5 (MTRS)
Playbooks
Syslog
Events Aggregation
Risk Based Management
Railway Operational Systems
RAM²
CRISIS PREPAREDNESS
CRISIS MANAGEMENT
On-Going Threat Intelligence Updates
Attack Vector
3
Cyber Security
Detection & Prevention Engines
S4RIS operational network Digital Twin
Digital Twin
PATENT PENDING

FIGURE 8: RAM² CAPABILITIES (REFERENCE – S4RIS D5.5 P.11)

3.9.2 Development and Quality standards adopted

RAM2 system was developed according to most advanced quality standards (ISO 9001, ISO 27001, etc.), and configuration management. RAM2 dedicated plugins for S4RIS monitoring tools, were developed and tested during the project, using similar methods.

3.9.3 Data used for tests

RAM2 system was tested using data requested to tool providers for the Simulation Exercises. For each SE at least three rehearsal sessions have been performed.

The data type is in JSON format. Examples of data used for test are reported in ANNEX III JSON messsages for RAM2 .

3.9.4 Test Data Report

This section reports the tests executed for RAM2, based on requirements described in D1.4 par. 2.3.9-

Test.-ID	RAM^2_TR_01
Addressed Requirement	RAM^2 _01 **RAM^2 should provide risk assessment and prioritization**
HW / SW preparation	Link RAM2 server to S4RIS DMS (kafka) Define assets list and mitigation procedures
Test inputs	Various types of events
Test procedure	Various types of JSON messages related to events are pushed to kafka
Expected Results	RAM^2 system enables efficient decision making based on smart prioritization of risks detected
Pass/Fail	Pass
Deviation Encountered	Assets list was not provided. A demo assets list was generated for these tests

Test.-ID	RAM^2_TR_02
Addressed Requirement	RAM^2 _02 **RAM^2 should generate correlated insights** • Identify patterns of events that indicate a potential risk • Provide full context of a scenario for decision making • Enable early warning to regarding suspicious events • Support proper prioritization of events
HW / SW preparation	Link RAM2 server to S4IS DMS (kafka) Define assets list and mitigation procedures
Test inputs	Various types of events
Test procedure	Various types of JSON messages related to events are pushed to kafka
Expected Results	RAM^2 system displayed the insights generated from events analysis
Pass/Fail	Pass
Deviation Encountered	Assets list was not provided. A demo assets list was generated for these tests

Test.-ID	RAM^2_TR_03
Addressed Requirement	RAM^2 _03 **RAM^2 should provide alert and insight mitigation steps** Clear mitigation steps for immediate risk mitigation
HW / SW preparation	Link RAM2 server to S4RIS DMS (kafka) Define assets list and mitigation procedures
Test inputs	Various types of events
Test procedure	Various types of JSON messages related to events are pushed to kafka
Expected Results	RAM^2 system provides relevant mitigation steps display, according to the operator's procedures
Pass/Fail	Pass
Deviation Encountered	Demo operator's procedures were created

Test.-ID	RAM^2_TR_04
Addressed Requirement	RAM^2 _04 **RAM^2 should provide an operational hierarchy context** • Display of assets and alerts within operational hierarchy • Calculation and display of risk according to the operational hierarchy. • Identify patterns of events based on operational context • Improve efficiency of decision making
HW / SW preparation	Link RAM2 server to S4RIS DMS (kafka) Define assets list and mitigation procedures
Test inputs	Various types of events
Test procedure	Various types of JSON messages related to events are pushed to kafka
Expected Results	RAM^2 system displays the relevant assets list (which can be received e.g. from S4RIS risk assessment and/or assets management tools), for the event detected, calculates the risk status and identifies patterns within the detected events to indicate correlated insights, for an efficient decision-making
Pass/Fail	Pass
Deviation Encountered	Assets list was not provided

Test.-ID	RAM^2_TR_05
Addressed Requirement	RAM^2 _05 **RAM^2 Dashboard** • Simple understanding of top KPIs • Immediate focus on source of greatest risks • Operational context
HW / SW preparation	Link RAM2 server to S4RIS DMS (kafka) Define assets list and mitigation procedures
Test inputs	Various types of events

Test procedure	Various types of JSON messages related to events are pushed to kafka
Expected Results	RAM^2 intuitive dashboard enable the operator to focus on alerts with greatest risks and the mitigations as the operational context outcomes
Pass/Fail	Pass
Deviation Encountered	RAM^2 dashboard access wasn't enabled from S4RIS portal

Test.-ID	RAM^2_TR_06
Addressed Requirement	RAM^2 _06 **RAM^2 integration for input data and export to additional systems** Digestion of assets information and events data. Communicating generated alerts and insights generated by RAM2 to external systems
HW / SW preparation	Link RAM2 server to S4IS DMS (kafka) Define assets list and mitigation procedures
Test inputs	Various types of events
Test procedure	Various types of JSON messages related to events are pushed to kafka
Expected Results	RAM^2 was the 1st S4RIS tool to perform integration with other tools (CuriX and Kafka) for receiving JSON events messages. RAM^2 interface dataset turns to be S4RIS standard JSON format for events. Insights and alerts data export was done through file sharing
Pass/Fail	Pass
Deviation Encountered	

Test.-ID	RAM^2_TR_07
Addressed Requirement	RAM^2 _07 **RAM^2 Conformity with overarching and S4RIS platform specific requirements** Ensure that any work connected with this tool conforms to the overarching and S4RIS platform specific requirements
HW / SW preparation	Link RAM2 server to S4RIS DMS (kafka) Define assets list and mitigation procedures
Test inputs	Various types of events
Test procedure	Various types of JSON messages related to events are pushed to kafka
Expected Results	RAM^2 is a TRL7 tool, found to align with most of D1.4 section 2.2 relevant requirements, covering all S4RIS aspects.
Pass/Fail	Pass
Deviation Encountered	

3.10 SARA

3.10.1 Overview

The aim of SARA tool is to analyze a station from a security point of view, with reference to the individual equipment (e.g., ventilation, communication, power supply, etc.). 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 man-made attack and/or natural threat. The analysis of the station gives as outputs 3KPIs.

In this context, 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.

The process is based on the fact that the equipment is modeled and studied with an analysis of vulnerability and availability aimed to identify the critical components and to rank their importance. The balance between investments to limit the vulnerability and the reduction of the consequences of the failure is a typical “decision making” process derived by economical and technical factors.

In the current methodology the equipment considered is related to the functioning of the building and is not related to the operational of the transport service. Therefore, the functional analysis and the definition of the missions of the station are oriented to be developed considering the station building.

Although many activities are hosted in modern complex stations, such as commerce, social interaction, recreation etc., in order to simplify the problem in this context, only the main functions related to the transport system have been taken into account.

KPIs description

The evaluation analysis of a station in the emergency and post-emergency phases can be approached defining a series of mission that a station is expected to perform:

- Mission 1: accessibility of the passengers from outside the building to platforms, and from the platforms to the outside, on the basis of the surviving structure/equipment;
- Mission 2: restoration of the integrity of the damaged equipment back to fully functioning;
- Mission 3: emergency procedures to be put in place during the emergency phase (e.g. evacuation and search and rescue activities).

A specific KPI has been assigned to each mission as reported in the following:

- Mission 1: functioning during the post emergency phase (INDIRECT LOSS).
  KPI1 - measurement of the effectiveness of the station in the post-emergency phase related to service availability (indicator: accessibility to platform on the basis of working structure/equipment in terms of time needed);
- Mission 2: restoration of the integrity of the damaged equipment (DIRECT LOSS).
  KPI2 - measurement of the direct economic damage related to the disruption of the equipment (indicator: cost of replacement of the LDUs/equipment disrupted);
- Mission 3: emergency procedures (PEOPLE LOSS).
  KPI3 - measurement of the efficiency of emergency procedure (indicator: variation of number of fatalities due to the unavailability of some equipment).

3.10.2 Development and Quality standards adopted

RINA adopts the following Quality Standards:

- ISO 31000 - The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome).

- ISO Guide 73:2009 - Risk can be defined as the combination of the probability of an event and its consequences.
- NFPA 130 - Standard for Fixed Guideway Transit and Passenger Rail Systems.

No specific software development and/or quality standard adopted.

3.10.3 Data used for tests

The following methods can be considered for gathering data:

- Types:
  - Planimetry of the different storeys of the station, with the addition of some partially artificial data derived from an on-site survey. The data were given both in pdf and cad format.
  - People flow is defined by a combination of given input and some consideration of literature information.
  - The cost of mitigation, rehabilitation, and duration was defined based on the current RINA know-how.
- Sources: The planimetries were given by RFI and Milan Municipality, while the information on the people flow was derived by RFI input. The cost of mitigation, rehabilitation, and its duration was defined on the basis of an internal DB built-up during a previous project with similar scope of work.
- Amounts:
  - 11 RFI planimetries in pdf (3.61MB).
  - 13 Milan Municipality in pdf (8.15MB).
  - RFI yearly passenger inside the station.

Number of times tests performed: The presented results are based on the definition of two different scenarios (flooding occurring in different areas). These two scenarios were analysed three times, for the first one the analysis was directly related to the current status and scenario effects on the station; secondly, the analyses were performed by introducing a certain amount of budget to evaluate the possible beneficial effect of the mitigation action; and the third analysis was driven by and higher amount of budget to perform a sort of prioritization among the different actions

3.10.4 Test Data Report

This section reports the tests executed for SARA, based on requirements described in D1.4 par. 2.3.10

Test.-ID	SARA_TR_01
Addressed Requirement	SARA _01 **Securestation Attack Resilience Assessment (SARA)** • 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 to reduce the effects of a terrorist attack. • The effects considered are related to the loss of elements and the 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).
HW / SW preparation	
Test inputs	Milan test case

Test procedure	Step 1: Analysis of the station from the physical point of view, considering the architectural aspect and the equipment related to the functioning of the building itself; Step 2: Definition of one or more hazard scenarios in terms of damages of building and equipment; Step 3: Evaluation of the consequences of the defined attacks in term of: Functional consequences; Direct economic losses; Consequences for human life; Step 4: Definition of a set of countermeasures, each of them characterized by their impact (reduction) on the vulnerability and consequences of attacks and their cost; Step 5: Ranking the set of remedial measures in order to define a sub-set able to fulfill the constraints or to reach the goals previously defined.
Expected Results	Two different kinds of results: • Loss due to the current asset situation; • Different losses related to different kind of countermeasure that can be implemented.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	SARA tool was used for the Milan test case, the results obtained by SARA were shown during the Milan test case workshop
Problems	
Comments	

3.11 SecaaS

3.11.1 Overview

Intracom Telecom development of Cloud Computing Service (CCS) aids businesses in designing and implementing a private, public or hybrid cloud. Intracom Telecom offers its multi-vendor technological proficiency and high-standard security methods to enable any organization to provide best-in-class, revenue-generating, cloud-based services. Through CCS it delivers customized cloud solutions that serve the specific business needs of each customer (small & medium businesses, enterprises, and telecom or service providers). The **Security as a Service (SecaaS)**[16] product is a part of Intracom's **Cloud Computing Services** (**CCS**)[17]. It corresponds to innovative security services offered to Cloud customers. They are intended to provide enhanced protection to corporate assets, covering a wide range of requirements. The SecaaS portfolio encompasses dedicated virtual firewalls and web application firewalls. It can also assist organizations in strengthening their virtual private Clouds with controls applicable to their business. A part of the CCS portfolio includes also **Disaster Recovery as a Service (DRaaS**)[18], potentially offering added benefits to SAFETY4RAILS tools portfolio.

3.11.2 Development and Quality standards adopted

Intracom Telecom is the first system integrator in the South East Europe having designed, built and operate a Public Cloud infrastructure which has received numerous distinctions, the most significant being:

- **ISO 27001:2013** certification that guarantees structured and organized information security management system governing the Cloud Services lifecycle. Moreover, Intracom Telecom is listed in Cloud Security Alliance's (CSA) "Security, Trust and Assurance Registry" (STAR), thereby fulfilling the first CSA certification level.
- **Cisco Cloud and Managed Services Advanced Certification** that assures robust, flexible and scalable cloud services and acknowledges excellence in service delivery and support.

3.11.3 Data used for tests

The SecaaS tool is practically a cloud service front end to various products offered by Intracom Telecom. As such, its testing is primarily oriented on evaluating service interfacing to connected products, rather than the actual data analysis. Therefore, types of data refer to compliance tests of such service interfaces.

TABLE 8: CLOUD SERVICE INTERFACING DATA

Type	WEB service request(s) and response(s)
Source	UNIMS, SymbIoTe, SISC2
Amount	Once set of request/response per end point of the connected service(s)
Number of time tests performed	Three tests per interface/end-point Pass result determined by majority results from three tests

3.11.4 Test Data Report

This section reports the tests executed for SecaaS, based on requirements described in D1.4 par. 2.3.11.

Test.-ID	SecaaS_TR_01
Addressed Requirement	SecaaS _01 **Monitoring of network traffic for signs of abnormality** • Abnormality detection • Correlation with known cyber-attack modus of operandi
HW / SW preparation	SecaaS is a WEB service application layer to SISC2 and UniMS applications. Hence, deployment requires installation/deployment of either of the two products. Since they are both physically located at Intracom, opening company firewall and exposing end points to SecaaS is required.

[16] https://intracom-telecom.com/en/products/ict_services_solutions/cloud/SecaaS.htm
[17] https://intracom-telecom.com/en/products/ict_services_solutions/cloud/cloudOverview.htm
[18] https://intracom-telecom.com/en/products/ict_services_solutions/cloud/DRaaS.htm

	Subsequently, to integrate with SAFETY4RAIL system, link to S4RIS Dashboard is required for exposing its GUI interfaces as well as subscription to SAFETY4RAILS Message Broker (Kafka).
Test inputs	SecaaS is directly integrated with Intracom telecommunications systems, such as WiBAS, though it offers also capabilities to link with network management consoles of service operators. Since this has NOT been offered in SAFETY4RAILS, the capabilities of the SecaaS have been limited to demonstrated capabilities of monitoring internal Intracom network and identification of real time abnormalities. The identified incidents may be transmitted to SAFETY4RAILS, though none offers capabilities of integrating such information, while several ones offer similar capabilities.
Test procedure	**Step 1:** Detection of abnormalities within Intracom network **Step 2:** Attempt to identify common attack profiles
Expected Results	**Step 1:** Detect abnormality(ies) and/or unauthorised type of traffic **Step 2:** Flag possible threat by detecting known/suspected abnormal traffic pattern
Pass/Fail	**Step 1:** SUCCESS Analysis of traffic indicated possible network investigation pattern **Step 2:** SUCCESS Analysis of network usage pattern identified insight threat, correlated with forbidden
Deviation Encountered	N/A
Comments	N/A

Test.-ID	SecaaS_TR_02
Addressed Requirement	SecaaS _02 **Interfaces to comply with S4RIS WEB service methodology** Communicating with central C&C console in standardised manner.
HW / SW preparation	Deployment of SAFETY4RAILS Dashboard and Kafka Message Broker Exposure of SecaaS WEB service interfaces by ICOM
Test inputs	N/A
Test procedure	**Step 1:** Integration with SAFETY4RAILS WEB browser interface (new tab or iFrame) **Step 2:** Integration with SAFETY4RAILS Kafka Message Broker
Expected Results	**Step 1:** Ability to display SecaaS WEB interface in SAFETY4RAILS Dashboard **Step 2:** Subscription to SAFETY4RAILS Kafka Message Broker
Pass/Fail	**Step 1:** Not integrated at CDM trials **Step 2:** Not integrated at CDM trials
Deviation Encountered	Integration has NOT been completed in time for CDM trials and contribution not provided for inclusion of ICOM tools in CDM exercises.
Comments	The demo of SecaaS along with other tools will be scheduled for the final event due Sep-2022

Test.-ID	SecaaS_TR_03
Addressed Requirement	SecaaS _03 **Conformity with overarching and S4RIS platform specific requirements** Ensure that any work connected with this tool conforms to the overarching and S4RIS platform specific requirements.
HW / SW preparation	Similarly to all of ICOM products, to facilitate the integration with other SAFETY4RAILS tools and the integrated SAFETY4RAILSDashboard, additional developments had to be made to adapt REST WEB service interfaces to cater for JSON message content agreed to be exchanged among SAFETY4RAILS tools. Considering that SecaaS accommodates alternative Message Broker (Google pub/sub) to SAFETY4RAILS (Kafka), additional development was necessary to enable translation and exchange of message ques among the two brokers.
Test inputs	N/A
Test procedure	**Step 1:** Integration with SAFETY4RAILS Dashboard **Step 2:** Integration with SAFETY4RAILSKafka Message Broker
Expected Results	**Step 1:** SecaaS integrated as a separate tab or iFrame within the SAFETY4RAILS Dashboard **Step 2:** Subscription and consumption of messages from SAFETY4RAILS Kafta message broker
Pass/Fail	**Step 1:** Deviation **Step 2:** Deviation
Deviation Encountered	The integration with SAFETY4RAILS Dashboard could not have been practically tested since SecaaS could not be directly connected neither to the SAFETY4RAILSDashboard not the Kafka Message Broker. The practical test showing potential for integration with SAFETY4RAILS adopted methodology has been successfully validated using synthetic internal benchmarking and demos of those test will be made available to partners for the final meeting in September 2022.
Comments	Refer to section “**Deviations Encountered**” for details.

3.12 SecuRail

3.12.1 Overview

SecuRail is the tool developed by Stam within SAFETY4RAILS project. It is the improved version of a tool developed in a ISF project called Rampart. SecuRail allows the user to create its railway network topology and infrastructure model and compute the risk for various threats. SecuRail is a desktop web application deployed on cloud.

Although the tool was an upgrade of the existing tool, this version of SecuRail has been developed from scratch to allow the usage of a new (and more advanced) development stack.

3.12.2 Development and Quality standards adopted

The process which has been followed for the development of SecuRail is called Agile, specifically Scrum. Agile methodology has been introduced for the first time in 2001. It aimed to have approach less structed to other methodology, like the Waterfall model, and more focused on the objective to deliver the final product to the client in short time and frequently. Agile methodology allows to be always ready to adapt to new and diverse requirements, and to be able fulfil the desires of the client.

Scrum is an Agile methodology specifically created for the management of software development. This approach is based on the team member capacity to interact with one another and to readily respond to changes. A Scrum team is composed by Developers, Scrum Master and Product Owner. Each of them knows exactly which are their role inside the team and work in order to achieve the end goal. The Product Owner have the role to give priorities to the developers and to keep track on how the development is progressing. On the other hand, the Scrum Master, have the role of coaching the team members on the methodology to follow, to remove obstacles in the development process and support the Product Owner.

In order to be sure to follow the right approach and standards, in STAM we have three Product Owners and one Scrum Master certified by Scrum Alliance (www.scrumalliance.org).

The versioning of the software has been made using GitLab in order to enable the possibility of making the team working together on the same code and also to restore previous versions in case of need.

Every piece of the software has been tested before release. Two kind of tests have been carried out:

- Unit tests: all the units of the back-end of the application have been covered with unit tests executed in the pipeline when the code is saved. Any time a new version of the application is released, tests are repeated and the new version is deployed online only if all the tests are passed.
- Functional tests: The Product Owner has defined and conducted a series of functional acceptance tests to verify that the application is working properly. The tests have been repeated any time a new version is deployed online.

3.12.3 Data used for tests

In order to test all the functionalities of SecuRail diverse types of data has been used.

During the development and implementation phases of the functionalities that characterize this tool, the tool has been deeply tested with ad-hoc synthetic data created for this purpose.

While, in order to verify the behaviour of the tool with real data, before each demonstration, with the exception of the one in Rome where this tool has not been applied, there have been an exchange of information with each use-case owner. All the case study owners were capable of providing useful and reliable data thanks to which it was possible to create a detailed network infrastructure and test it in diverse types of scenarios with various threats.

Moreover, it has been tested, both with synthetic data and real data, the commutation to the others tool by publishing diverse Json messages to the broker Kafka. Thanks to the communication with the broker, it is also possible for SecuRail to receive information about the network infrastructure and assets generated by other tools present within the S4RIS platform.

Here are presented the main types of data which have been used in the testing phases.

TABLE 9: CROWDING DATA INFORMATION

Type	Crowding
Source	Use-case owner
Amount	Values for each time slot of the day for a day of the week, Saturday and Sunday
Number of time tests performed	At least 10 for each use-case

TABLE 10: NETWORK DATA INFORMATION

Type	Network
Source	Use-case owner
Amount	Information for each station and section that was need in the Use-case (Also including the areas present inside the stations)
Number of time tests performed	At least 10 for each use-case

TABLE 11: ASSET DATA INFORMATION

Type	Assets
Source	Use-case owner
Amount	Information for each asset present inside the stations and sections (also including the area in which they are located and their economic value)
Number of time tests performed	At least 10 for each use-case

TABLE 12: THREAT DATA INFORMATION

Type	Message reporting an occurring threat
Source	Detection tool
Amount	One message for each threat detected by the tool
Number of time tests performed	5 times

Thanks to these types of data used during the testing process it was possible to verify that all the functionalities of SecuRail work as intended.

3.12.4 Test Data Report

This section reports the tests executed for SecuRail, based on requirements described in D1.4 par. 2.3.12.

Test.-ID	SecuRail_TR_01
Addressed Requirement	SecuRail _01 **Creation of libraries of the Railway environment to create and model the railway infrastructure to be analysed with the tool** ▪ Allow the user modelling its own infrastructure and network ▪ Allow the definition of features of the infrastructure ▪ Facilitate the modelling by providing pre-defined railway items such as assets and countermeasures.
HW / SW preparation	NA
Test inputs	Information regarding the assets inside a station
Test procedure	Step 1: Selection of the station in the map Step 2: Creation of the area inside the station

	Step 3: Creation of the asset in the areas
Expected Results	The station created in the software should have all the assets present in the real station
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	SecuRail_TR_02
Addressed Requirement	SecuRail _02 **Localization on the Map** Visualize the railway network on a map to facilitate exploration and visualization of the model.
HW / SW preparation	NA
Test inputs	Selection of two stations
Test procedure	Step 1: Open the map present in SecuRail Step 2: Selection of the stations on the map Step 3: Creation of a section among the two sections
Expected Results	The user should be able to visualize the stations chosen and the section between them on the map present in the tool
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	SecuRail_TR_03
Addressed Requirement	SecuRail _03 **Computation of Risk** ▪ Perform Risk assessment ▪ Evaluate damages to people, infrastructure and services ▪ Assess likelihood and impact of threats ▪ Definition and quantitative estimation of the Security Risk Assessment Index.
HW / SW preparation	NA
Test inputs	Information regarding the network (stations, section, assets, …), the geographical area considered (VSL, probabilities, …) and impacts (lethality, …)
Test procedure	Step 1: Creation of the network Step 2: Choice of countermeasures present Step 3: Choice of threats considered
Expected Results	The system should display the results of the risk computation in a dashboard and an excel file, containing a detailed description of the scenarios computed, should be generated

Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	SecuRail_TR_04
Addressed Requirement	SecuRail _04 **Real-time automatic risk assessment** Risk assessment in real-time triggered automatically by warning from monitoring tools
HW / SW preparation	Connection to the S4RIS platform broker
Test inputs	Alerts generated by other tools present in the platform and a railway network created on SecuRail
Test procedure	Step 1: Generation of alert in another tool Step 2: Communication of the alert to SecuRail Step 3: Selection by the user to compute the risk assessment based on the values provided by the other tools
Expected Results	The system should display the results of the risk computation in a dashboard and an excel file, containing a detailed description of the scenarios computed, should be generated
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	SecuRail_TR_05
Addressed Requirement	SecuRail _05 **Multilinguality** Provide the tool to the user in its native language
HW / SW preparation	NA
Test inputs	NA
Test procedure	Step 1: Selection by the user to change to another language
Expected Results	The UI should change all the textual contents to another language
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	SecuRail_TR_06
Addressed Requirement	SecuRail _06 **Cost-Benefit Analysis** Evaluation of the overall costs of countermeasures compared to the reduction of risk
HW / SW preparation	NA
Test inputs	Having a list of countermeasures with relative useful information
Test procedure	Step 1: Creation of a scenario with some countermeasures Step 2: Creation of an identical scenario but with other countermeasures Step 3: Computation of the risk of the two scenarios
Expected Results	The application of diverse countermeasures should reflect on the result of the risk computation
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	SecuRail_TR_07
Addressed Requirement	SecuRail _07 **Conformity with overarching and S4RIS platform specific requirements** Ensure that any work connected with this tool conforms to the overarching and S4RIS platform specific requirements
HW / SW preparation	Having a functional and active broker, having another tool connected to the broker, having a common S4RIS platform
Test inputs	Message sent from a tool connected to the broker
Test procedure	Step 1: Receive message from a tool connected to the broker Step 2: Send message to a tool connected to the Step 3: Visualize SecuRail on the S4RIS platform
Expected Results	The software should send and receive messaged form the broker and it should also be visible on the S4RIS platform
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

3.13 Senstation

3.13.1 Overview

Senstation was developed as a backend IoT device which operates as a secure gateway. Senstation can be used as a multipurpose IoT gateway that was strengthened with cryptographic functions in SAFETY4RAILS As is demonstrated in Madrid and Ankara simulations and also at the laboratory scale, Senstation enables the encryption at edge nodes and assists the end-to-end secure communication and data exchange over S4RIS in close coordination with PRIGM (See Section 2.8 for more details about PRIGM). Senstation operates at the client side enabling the encryption and decryption of data where the data is generated, e.g. sensory data collected from the endpoints or any service data gathered from the SCADA system. Senstation has interfaces for both analogue and digital sensors enabling secure transmission of multimodal data over a cyber-physical data acquisition backbone.

3.13.2 Development and Quality standards adopted

Senstation relies on the following standards and test criteria which are accepted as de facto in any information system:

1. The Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 1540814[14]) for computer security certification. This standard is the widely adopted security standard for IoT backend devices that are enriched with cryptographic capabilities.
2. NIST 800-22[15]: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST 800-22 is the widely adopted test criteria used for ensuring the key generation scheme that is built on truly random numbers (not the pseudorandom numbers which can easily be hacked). Since Senstation relies on end-to-end cryptography, NIST-800-22 is also an indispensable criterion in Safety4Rails.

3.13.3 Data used for tests

Data used in Secure end-to-end IoT data transmission:

- type(s): numeric sensory data
- source(s): sensors connected to the Senstation digital interfaces
- amount(s): ~3-day data stream collected at every 5 seconds (per sensor)
- number of times test(s) performed: 2

3.13.4 Test Data Report

This section reports the tests executed for Senstation, based on requirements described in D1.4 par. 2.3.13.

Test.-ID	Senstation_TR_01
Addressed Requirement	Senstation _01 **Interfaces of Senstation should be compatible with the interfaces of sensors and the data network of the end-user compliant with industrial conditions aligned with CE standards** Communicating with sensors through appropriate interfaces
HW / SW preparation	HW: Senstation
Test inputs	-
Test procedure	Step 1: The Ethernet interface of Senstation is checked by a test engineer by connecting it to a network.

	Step 2: Serial Communication interface of Senstation is checked by a test engineer by connecting it to a serial end point device or sensor.
Expected Results	Senstation gets IP and responds to proper ping requests. Senstation communicates with a serial device over a serial communication protocol.
Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.
Problems	-
Comments	-
Problems	-
Comments	-

Test.-ID	Senstation_TR_02
Addressed Requirement	Senstation _02 **The resilience of the alternative secure data channel must be improved by end-to-end and hardware-based security** ▪ Ensure that the secure alternative channel transfers data in an encrypted form. ▪ Prevent man-in-the-middle attacks.
HW / SW preparation	HW: PRIGM, Senstation, Test PC SW: Wireshark
Test inputs	-
Test procedure	Step 1: A data communication channel is created between Senstation and PRIGM Step 2: The connection is sniffed by Wireshark.
Expected Results	Data sniffed from the secure channel must be in encrypted form.
Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.
Problems	-
Comments	-
Problems	-
Comments	-

Test.-ID	Senstation_TR_03
Addressed Requirement	Senstation _03 **Senstation must encrypt sensory data on the communication channel.** Ensure providing encrypted sensory data output to the end user's network.
HW / SW preparation	HW: PRIGM, Senstation, Test PC, a sample sensor (e.g. temperature sensor) SW: Wireshark
Test inputs	-

Test procedure	Step 1: A temperature sensor is connected to Senstation via RS485 (ModbusRTU) Step 2: A data communication channel is created between Senstation and PRIGM Step 3: The connection is sniffed by Wireshark.
Expected Results	Data sniffed from the secure channel must be in encrypted form. In the case of the secure channel captured, an attacker cannot extract the temperature value that flows in the secure channel.
Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.
Problems	-
Comments	-
Problems	-
Comments	-

Test.-ID	Senstation_TR_04
Addressed Requirement	Senstation _04 **Temperature, smoke, acceleration and velocity data should be collected through the Senstation tool and used for anomaly detection.** ▪ Measuring relevant environmental values with the help of the connected sensors. ▪ Applying statistical analysis techniques to identify anomalies within the observed series of sensor measurements.
HW / SW preparation	HW: PRIGM, Senstation, Test PC, Temperature Sensor SW: Wireshark
Test inputs	Confidence intervals (predefined or pre-computed confidence intervals by applying bootstrapping technique) + sample anomaly data
Test procedure	Step 1: Sensors are connected Senstation via RS485 over ModbusRTU protocol. Step 2: A data communication channel is created between Senstation and PRIGM Step 3: Check whether the observed data is in the confidence interval Step 4: Alert when the anomaly occurs (an observation that is out of the confidence interval for a certain period)
Expected Results	Data is collected and logged. Anomaly cases detected and logged.
Pass/Fail	Passed
Deviation Encountered	Field tests could not be implemented as timely as planned due to the inconsistencies that occurred as a result of COVID-19 restrictions. However, lab-scale tests have resulted in great success and field tests applied in controlled areas.
Problems	-
Comments	-
Problems	-
Comments	-

Test.-ID	Senstation_TR_05
Addressed Requirement	Senstation _05 **Conformity with overarching and S4RIS platform-specific requirements** Ensure that any work connected with this tool conforms to the overarching and S4RIS platform-specific requirements
HW / SW preparation	HW: PRIGM, Senstation, Test PC SW: Wireshark
Test inputs	-
Test procedure	Step 1: A data communication channel is created between Senstation and PRIGM Step 2: The connection is sniffed by Wireshark.
Expected Results	Data sniffed from the secure channel must be in encrypted form.
Pass/Fail	Passed
Deviation Encountered	No deviation had been reported.
Problems	-
Comments	-
Problems	
Comments	

3.14 SISC2

3.14.1 Overview

Intracom Telecom SISC2 is a CIP & Border Surveillance platform[19], a modular and scalable software integration platform for surveillance, collaboration, coordination and administration of diverse security and operations management related events. It is a comprehensive solution that gathers, processes, classifies and analyzes information received from several types of detection sensors and 3rd party applications to produce meaningful intelligence. 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.

Its key characteristics include:

- Highly-intuitive human machine interfaces
- Superior situational awareness providing 2D/3D dynamic maps and sensor data displays
- Authentication & authorization with Role Based Access Control (RBAC)
- Multilingual user interface
- Fully customized screen layouts with support for multi-monitor workstations
- Modular design and extensive use of open protocols allows system to scale horizontally
- High Availability ensures 24/7 operation and avoids single point of failure
- Seamless integration with a variety of third party systems

The list of main Functions & Features includes:

- Multiple source data presentation in list views, tree views, table views and custom views.
- GIS integration and mapping tools
  - 2D and 3D rendering capabilities for maps and sensor data
  - Video stream projection on the map
  - Seamless retrieval and projection of raster/vector data either directly or from geographical databases.
  - Measurement tools such as distance, area, angle, line of sight etc.
  - Insertion and management of POIs, areas of interest/jurisdiction, alarm areas and boundaries etc.
- User and role management.
- Resource management including humans and assets.
- Rule-based alarm management from a graphical rule editor:
  - Integration of multiple alarm sources (geo-fencing areas and boundaries, BMS etc.).
  - Alarm detection, prioritization, filtering and suppression.
  - Alarm notifications and programmable actions.
- Incident management with programmable standard operation procedures.
- Operator collaboration tools, such as Chatting, Mobile SMS, E-mail, VoIP, Radio over IP (RoIP)
- Rich set of customized reports in various document formats such as PDF, EXCEL, TXT, etc.
- Key performance indicators (KPI) and statistics.
- CPU and/or hardware accelerated video analytics:
  - Static or moving object detection, classification and identification.
  - Left and foreign object detection.
  - License plate recognition (LPR).
  - Face detection and identification.
- Multi-Sensor data fusion and track management integrating a wide variety of sensors and technologies (radar, EO/IR, CCTV, laser range finder, AIS tracks etc.) to enhance real-time situational awareness.

3.14.2 Development and Quality standards adopted

As all of Intracom Telecom products, also SISC2 complies with industry standard approaches, including incident management based on customized standard operating procedures and rules of engagement, with

[19] https://intracom-telecom.com/en/products/ict_services_solutions/sis/cip.htm

automatic escalation process and follow-up watchdogs, as well as in adopting programmable standard operation procedures as part of its Incident management process.

3.14.3 Data used for tests

In order to test the functionalities of SISC2 platform various types of data has been used. Since the development and implementation have been mostly performed remotely and in separation from other SAFETY4RAILS tools, in order to test and validate the functionalities of SISC2, the real data from cameras and motion detection sensors installed at Intracom premisses have been used. Such an approach has been preferable from using synthetic data that might be more prompt to disassociation from "real" situations that might be faced in relevant environments.

Since SISC2 could not have been demonstrated in SAFETY4RAILS trials, including the last one in Milan, in order to verify the behaviour of the tool with data as much as possible resembling possible situation faced in railway environments, the parking lot at Intracom was used as a physical test site thus creating the most realistic situations that might be faced at railway stations and immediate transport access areas. In addition, data provided by SAFETY4RAILS pilot hosts, such as those from Rome and Milan, have been used to advantage. This allowed recreation of most relevant and useful data types thus creating detailed environment to test with various threats.

Although integration with other tools in SAFETY4RAILS have not been completed in time for Milan tests, the SISC2 has been geared to seamlessly integrate with Kafka services provided by the project, by deploying a proprietary version of a similar messaging broker, thus easing subsequent effort in passing messages between SISC2 and SAFETY4RAILS integrated platform.

Here are presented the main types of data which have been used in the testing phases.

TABLE 13: SURVEILLANCE CAMERA FEEDS

Type	Several individual camera audio-visual feeds (real-time). Data included persons, vehicles and foreign objects as possible detectable threats.
Source	Use-case owner – in our case test site host (i.e., Intracom)
Amount	Persistent streaming of camera audio-visual data for AI threat analysis.
Number of time tests performed	Continuously (24x7) over the period of 10 days

TABLE 14: MOTION SENSOR DEV ICE DATA

Type	Motion sensor data (event-based) over the network
Source	Use-case owner – in our case test site host (i.e. Intracom)
Amount	Data from sensors was captured and analysed over the same period of 10 days, as in the case of camera feed analysis.
Number of time tests performed	Continuously (24x7) over the period of 10 days

TABLE 15: THREAT DATA INFORMATION

Type	Both alert messages and tracking data produced by the SISC2 machine learning algorithms, offering unique threat detection, identification, tracking and threat level analysis.
Source	Inherent SISC2 Machine Learning algorithms
Amount	One Detection message (on 1st intrusion) Multiple messages corresponding to threat tracking and classification
Number of time tests performed	Continuously (24x7) over the period of 10 days

3.14.4 Test Data Report

This section reports the tests executed for SISC2, based on requirements described in D1.4 par. 2.3.14.

Test.-ID	SISC_TR_01

Addressed Requirement	SISC _01 **Software integration platform for surveillance, collaboration, coordination and administration of security and operations management events** ▪ Gathering, processing, classifying and analysing info from sensors ▪ Producing meaningful intelligence out of diverse sensor info ▪ Simple installation and no complex setup is required ▪ Surveillance with physical control of access to the site ▪ Authentication & authorization with Role Based Access Control (RBAC) ▪ Multilingual user interface ▪ Fully customized screen layouts with support for multi-monitor workstations ▪ Modular design and use of open protocols ▪ High availability ensuring 24/7 operation and avoiding single points of failure. ▪ Seamless integration with a variety of third party systems
HW / SW preparation	The SISC2 is currently deployed as a WEB service platform at Intracom premises, thus necessitating exposure to external access. Subsequently, to integrate with SAFETY4RAILS system, link to S4RIS Dashboard is required for exposing its GUI interfaces as well as subscription to SAFETY4RAILS Message Broker (Kafka).
Test inputs	Surveillance data from cameras and in-situ access control sensors
Test procedure	**Step 1:** Collection of surveillance data from multiple cameras for threat detection and identification **Step 2:** Gathering, processing, classifying and analysing info from sensors **Step 3:** Reducing dales positives by determining threats, common to diverse surveillance sources **Step 4:** Producing meaningful intelligence out of diverse sensor info **Step 5:** Surveillance with physical control of access to the site **Step 6:** Authentication & authorization with Role Based Access Control (RBAC) **Step 7:** High availability ensuring 24/7 operation and avoiding single points of failure. **Step 8:** Seamless integration with a variety of third party systems
Expected Results	**Step 1:** Surveillance data from multiple cameras collected **Step 2:** Data classifying and analysed with threat detected and identified **Step 3:** False positives mitigated, individual threat successfully detected **Step 4:** Intelligence provided threat identification with continous tracking **Step 5:** Physical access control to the site offered **Step 6:** Authentication & authorization with Role Based Access Control (RBAC) achieved **Step 7:** Availability at 24/7 with avoidance of single points of failure demonstrated **Step 8:** Capabilities of integrating custom and third party sensors demonstrated
Pass/Fail	**Step 1:** SUCCESS **Step 2:** SUCCESS

	Step 3: SUCCESS **Step 4:** SUCCESS **Step 5:** SUCCESS **Step 6:** SUCCESS **Step 7:** SUCCESS **Step 8:** SUCCESS
Deviation Encountered	Integration with SAFETY4RAILS Dashboard could be practically tested since SISC2 could not be directly connected either to the SAFETY4RAILS Dashboard nor the Kafka Message Broker. Hence, tests have been performed at ICOM premises to simulated scenarios from SAFETY4RAILS CDM trials with videos of the demos captured.
Comments	Demo videos of tests will be made available to partners for the final meeting in September 2022.

Test.-ID	SISC_TR_02
Addressed Requirement	SISC _02 **Conformity with overarching and S4RIS platform specific requirements.** Ensure that any work connected with this tool conforms to the overarching and S4RIS platform specific requirements
HW / SW preparation	The SISC2 is currently deployed as a WEB service platform at Intracom premises, thus necessitating exposure to external access. Subsequently, to integrate with SAFETY4RAILS system, link to S4RIS Dashboard is required for exposing its GUI interfaces as well as subscription to SAFETY4RAILS Message Broker (Kafka).
Test inputs	N/A
Test procedure	**Step 1:** Integration with SAFETY4RAILS Dashboard **Step 2:** Integration with SAFETY4RAILS Kafka Message Broker
Expected Results	**Step 1:** SISC2 integrated as a separate tab or iFrame within the S4R Dashboard **Step 2:** Subscription and consumption of messages from SAFETY4RAILS Kafta message broker
Pass/Fail	**Step 1:** Deviation **Step 2:** Deviation
Deviation Encountered	The integration with SAFETY4RAILS Dashboard could not be practically tested since SISC2 could not be directly connected either to the SAFETY4RAILS Dashboard not the Kafka Message Broker. Due to recent upgrade to security policies, such an access could not be provided. Alternative packaging of the complete system has been investigated and is expected to be successfully completed by the final event in Sept-2022.
Comments	The practical test showing potential for integration with SAFETY4RAILS adopted methodology has been successfully validated using synthetic internal benchmarking and demos of those test will be made available to partners for the final meeting in September 2022.

3.15 TISAIL

3.15.1 Overview

TISAIL (Threat Intelligence Service for the rAILway sector) is a platform based on the open-source platform MISP (Malware Information Sharing Platform). The aim of TISAIL is to provide a platform for gathering, analysing and sharing relevant Threat Intelligence for the railway sector. According to Gartner[20], Threat Intelligence is evidence-based knowledge (e.g., context, mechanism, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets.

Additionally, TISAL has an automated process for gathering emerging threats, IoCs (Indicator of Compromise) and vulnerabilities from different sources. The alerts are filtered by a Threat Intelligence analyst in order to reduce the number of false positives and to adapt the alerts to the stakeholders. After this step, the alerts are sent to other SAFETY4RAILS tools for enriching their data and helping decision-makers at the prevention and detection stages.

The format used by TISAIL is based on MISP (Malware Information Sharing Platform) standard, a flexible and customisable data model based on JSON that is a reference within the Threat Intelligence field. TISAIL will also provide rail specific taxonomy for threats to help decision-makers to identify and classify threats and actions quicker.

3.15.2 Development and Quality standards adopted

The MISP platform used by TISAIL is an open-source project with a large community. There has been software development for the creation of automated processes for gathering information from different sources such as malware repositories, threat intel feeds and social media. Python has been the programming language used and all the software processes have been implemented with unit tests in order to check that the source code was working properly.

3.15.3 Data used for tests

The data used for building TISAIL was mainly open-source data available, related to reported vulnerable devices, and previous threats encountered in the railway sector. Besides, some questions were made to our end-users in SAFETY4RAILS, who sent some information about the devices they use in their infrastructures, which could be a target to a cybersecurity attack.

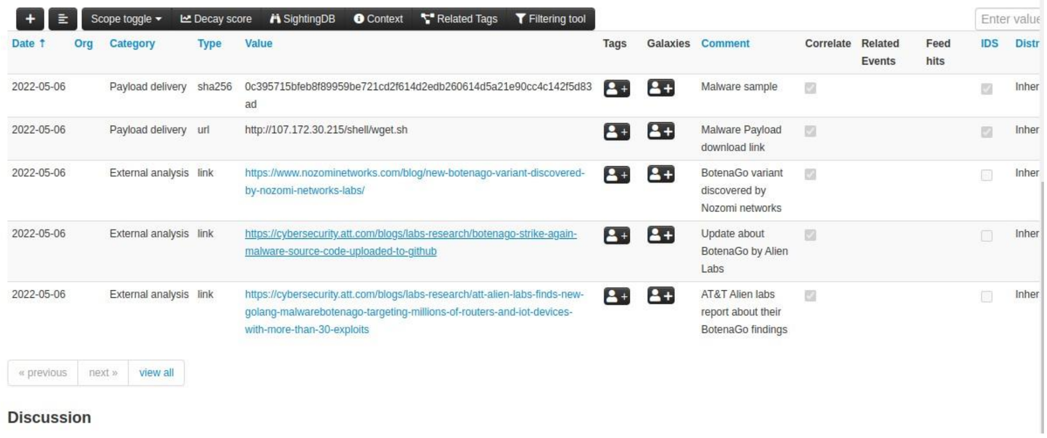
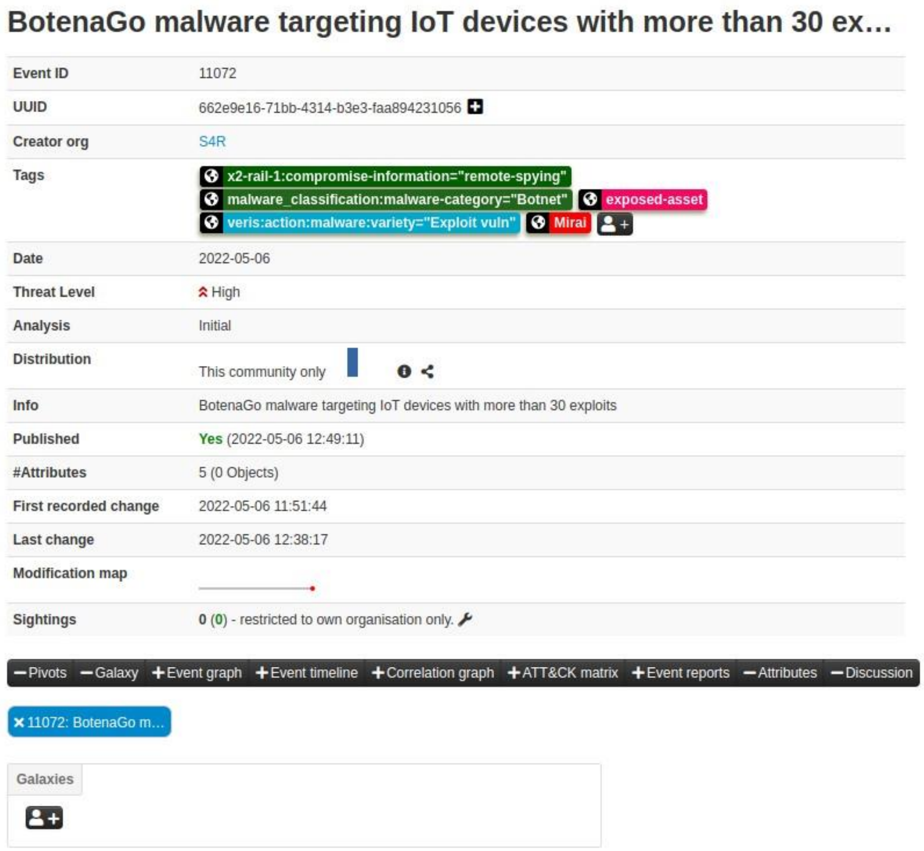
Then, we made tests during our simulation exercises (Madrid, Ankara and Rome), and TISAIL gathered data collected during the exercises days. The tool was tested across the development cycle and tested and demonstrated live in simulation exercises. All the test cases were performed multiple times on different systems to confirm the results.

3.15.4 Test Data Report

This section reports the tests executed for TISAIL, based on requirements described in D1.4 paragraph 2.3.15.

Test.-ID	TISAIL_TR_01
Addressed Requirement	TISAIL _01 **Detection of cyber-threats related to the railway sector: Malware** •Detect malware targeting ICS infrastructures (e.g.EKANS) •Detect malware targeting transportation sector, in particular the railway sector
HW / SW preparation	A properly configuration of “search terms” is needed such as: • Keywords such as “railway”, “metro”, “train”

[20] Gartner: Security Threat Intelligence Products and Services

	- Names of threat actors targeting ICS infrastructures (e.g. Energetic Bear, Dragon Fly, Xenotime, etc) - Malware families known for targeting ICS (e.g. Triton, Industroyer)
Test inputs	
Test procedure	Step 1: Configure the automated processes (e.g., crawlers) with the above keywords, malware families and threat actors. Step 2: Run the crawlers and send the alerts to TISAIL. Step 3: Check if any of the threats collected is relevant for the SAFETY4RAILS stakeholders.
Expected Results	A significant number of threats related to ICS, since the attacks and breaches to ICS has been increased during the last 3 years.  

Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distr
2022-05-06		Payload delivery	sha256	0c395715bfeb8f89959be721cd2f614d2edb260614d5a21e90cc4c142f5d83ad			Malware sample	☑			☑	Inher
2022-05-06		Payload delivery	url	http://107.172.30.215/shell/wget.sh			Malware Payload download link	☑			☑	Inher
2022-05-06		External analysis	link	https://www.nozominetworks.com/blog/new-botenago-variant-discovered-by-nozomi-networks-labs/			BotenaGo variant discovered by Nozomi networks	☑			☐	Inher
2022-05-06		External analysis	link	https://cybersecurity.att.com/blogs/labs-research/botenago-strike-again-malware-source-code-uploaded-to-github			Update about BotenaGo by Alien Labs	☑			☐	Inher
2022-05-06		External analysis	link	https://cybersecurity.att.com/blogs/labs-research/att-alien-labs-finds-new-golang-malwarebotenago-targeting-millions-of-routers-and-iot-devices-with-more-than-30-exploits			AT&T Alien labs report about their BotenaGo findings	☑			☐	Inher

BotenaGo malware targeting IoT devices with more than 30 ex…

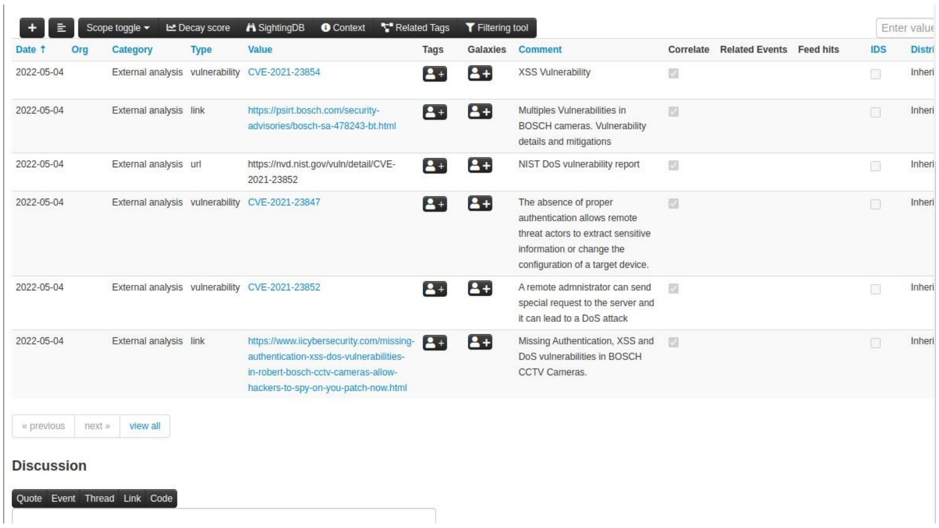
Event ID	11072
UUID	662e9e16-71bb-4314-b3e3-faa894231056
Creator org	S4R
Tags	x2-rail-1:compromise-information="remote-spying" malware_classification:malware-category="Botnet" exposed-asset veris:action:malware:variety="Exploit vuln" Mirai
Date	2022-05-06
Threat Level	High
Analysis	Initial
Distribution	This community only
Info	BotenaGo malware targeting IoT devices with more than 30 exploits
Published	Yes (2022-05-06 12:49:11)
#Attributes	5 (0 Objects)
First recorded change	2022-05-06 11:51:44
Last change	2022-05-06 12:38:17
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Pass/Fail	Pass
Deviation Encountered	None
Problems	None identified
Comments	

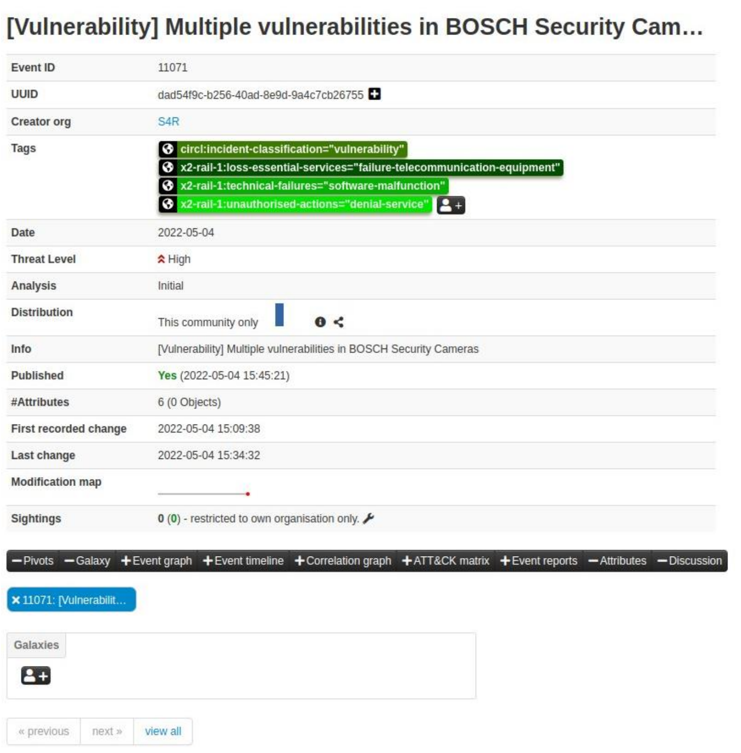
Test.-ID	TISAIL_TR_02
Addressed Requirement	TISAIL _02 **Detection of cyber-threats related to the railway sector: Internet-Exposed Assets and credential leaks** ▪ Detect sensitive IT/OT assets used in the railway industry exposed to the Internet. ▪ Detect data leaks such as emails, usernames or passwords related to railway companies.
HW / SW preparation	A properly configuration of "search terms" is needed such as: • IT/OT assets used by railway stakeholders (e.g., wind sensors, CCTV cameras, etc) • Domain names of railway stakeholders (e.g., metrodemadrid.es, tcdd.gov.tk)
Test inputs	
Test procedure	Step 1: Configure the automated processes (e.g., crawlers) with the above keywords. Step 2: Run the crawlers and send the alerts to TISAIL. Step 3: Check if any of the threats collected is relevant for the SAFETY4RAILS stakeholders.
Expected Results	At least one device (e.g. server, CCTV camera, IoT) exposed to the Internet.
Pass/Fail	Pass
Deviation Encountered	None identified
Problems	There was not real data from SAFETY4RAILS stakeholders about the products (e.g., manufacturer, model, etc) used by them, due to security reasons. This was solved by using well-known manufacturers such as AXIS or BOSCH for Surveillance cameras.
Comments	Internally tested several times

Test.-ID	TISAIL_TR_03
Addressed Requirement	TISAIL _03 **Detection of cyber-threats related to the railway sector: Threat Intel feeds and Social Media** •Detect common malware (crimeware) threats that are becoming relevant. •Provide Indicators of Compromise (IoCs), details and context about these threats
HW / SW preparation	A properly configuration of "search terms" is needed such as: • Keywords such as "railway", "metro", "train" • Names of threat actors targeting transportation sector or large companies (Carbon Spider, TA2541,etc) • Malware and Ransomware families used for targeting the transportation sector or large companies (e.g. Ryuk, Emotet, Blackcat, Revil)
Test inputs	None
Test procedure	Step 1: Configure the automated processes (e.g., crawlers) with the above keywords, malware families and threat actors. Step 2: Run the crawlers and send the alerts to TISAIL.

	Step 3: Check if any of the threats collected is relevant for the SAFETY4RAILS stakeholder
Expected Results	A significant number of threats related to ransomware, since these attacks has increased during the last 3 years.
Pass/Fail	Pass
Deviation Encountered	None.
Problems	None identified
Comments	Internally tested several times

Test.-ID	TISAIL_TR_04
Addressed Requirement	TISAIL _04 **Detection of cyber-threats related to the railway sector: Vulnerabilities** •Detection of vulnerabilities on ICS devices used in the railway sector. •Detection of vulnerabilities in IT software used in the railway sector (e.g. RDP)
HW / SW preparation	A properly configuration of “search terms” is needed: • A list of software products (e.g., AXIS Q16) that you want to monitor in order to know if there is any new vulnerability disclosed.
Test inputs	None
Test procedure	Step 1: Configure the automated processes (e.g., crawlers) with the above keywords. Step 2: Run the crawlers and send the alerts to TISAIL. Step 3: Check if any of the threats collected is relevant for the SAFETY4RAILS stakeholder
Expected Results	A significant number of vulnerabilities, since during the last years the number of vulnerabilities disclosed has increased. 

Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distri
2022-05-04		External analysis	vulnerability	CVE-2021-23854			XSS Vulnerability	☑			☐	Inheri
2022-05-04		External analysis	link	https://psirt.bosch.com/security-advisories/bosch-sa-478243-bt.html			Multiples Vulnerabilities in BOSCH cameras. Vulnerability details and mitigations	☑			☐	Inheri
2022-05-04		External analysis	url	https://nvd.nist.gov/vuln/detail/CVE-2021-23852			NIST DoS vulnerability report	☑			☐	Inheri
2022-05-04		External analysis	vulnerability	CVE-2021-23847			The absence of proper authentication allows remote threat actors to extract sensitive information or change the configuration of a target device.	☑			☐	Inheri
2022-05-04		External analysis	vulnerability	CVE-2021-23852			A remote admnistrator can send special request to the server and it can lead to a DoS attack	☑			☐	Inheri
2022-05-04		External analysis	link	https://www.iicybersecurity.com/missing-authentication-xss-dos-vulnerabilities-in-robert-bosch-cctv-cameras-allow-hackers-to-spy-on-you-patch-now.html			Missing Authentication, XSS and DoS vulnerabilities in BOSCH CCTV Cameras.	☑			☐	Inheri

<table>
<tr><td></td><td>
[Vulnerability] Multiple vulnerabilities in BOSCH Security Cam…
<table>
<tr><td>Event ID</td><td>11071</td></tr>
<tr><td>UUID</td><td>dad54f9c-b256-40ad-8e9d-9a4c7cb26755</td></tr>
<tr><td>Creator org</td><td>S4R</td></tr>
<tr><td>Tags</td><td>circl:incident-classification="vulnerability"
x2-rail-1:loss-essential-services="failure-telecommunication-equipment"
x2-rail-1:technical-failures="software-malfunction"
x2-rail-1:unauthorised-actions="denial-service"</td></tr>
<tr><td>Date</td><td>2022-05-04</td></tr>
<tr><td>Threat Level</td><td>High</td></tr>
<tr><td>Analysis</td><td>Initial</td></tr>
<tr><td>Distribution</td><td>This community only</td></tr>
<tr><td>Info</td><td>[Vulnerability] Multiple vulnerabilities in BOSCH Security Cameras</td></tr>
<tr><td>Published</td><td>Yes (2022-05-04 15:45:21)</td></tr>
<tr><td>#Attributes</td><td>6 (0 Objects)</td></tr>
<tr><td>First recorded change</td><td>2022-05-04 15:09:38</td></tr>
<tr><td>Last change</td><td>2022-05-04 15:34:32</td></tr>
<tr><td>Modification map</td><td></td></tr>
<tr><td>Sightings</td><td>0 (0) - restricted to own organisation only.</td></tr>
</table>
</td></tr>
<tr><td><b>Pass/Fail</b></td><td>Pass</td></tr>
<tr><td><b>Deviation Encountered</b></td><td>None.</td></tr>
<tr><td><b>Problems</b></td><td>There was not real data from SAFETY4RAILSs stakeholders about the products (e.g., manufacturer, model, etc) used by them for security reasons. This was solved by using well-known manufacturers such as AXIS or BOSCH for Surveillance cameras.</td></tr>
<tr><td><b>Comments</b></td><td>Internally tested several times</td></tr>
</table>

Test.-ID	TISAIL_TR_05
Addressed Requirement	TISAIL _05 **Detection of cyber-threats related to the railway sector: Spear Phishing**. Detect potential phishing campaigns masquerading as railway companies
HW / SW preparation	Configuration of the domain name to monitor (e.g., metrodemadrid.es)
Test inputs	None
Test procedure	Step 1: Configure the automated processes with the domain name to monitor Step 2: Run the crawlers Step 3: Confirm if any of the domain names collected is a potential fraudulent domain.
Expected Results	
Pass/Fail	Pass
Deviation Encountered	None
Problems	None identified
Comments	Internally tested several times

Test.-ID	TISAIL_TR_06
Addressed Requirement	TISAIL _06 **Integrate alerts related to cyber-threats in the railway sector with a MISP repository** Provide alerts to other tools for further exploitation.
HW / SW preparation	Configuration in the crawler of the MISP instance for sending alerts to it.
Test inputs	None
Test procedure	Step 1: Configure the automated processes with the URL and the API KEY of the MISP instance Step 2: Send the alerts
Expected Results	Alerts identifying spear phishing campaigns.
Pass/Fail	PASS
Deviation Encountered	None
Problems	None identified
Comments	

3.16 uni|MSTM

3.16.1 Overview

UniMS is a Planning and Operations (P&O) software, integrated with WiBAS, which includes:

- Network Lifecycle Management[21]
- Radio Planner[22]
- Connected Site[23]

3.16.2 Development and Quality standards adopted

Intracom Telecom's uni|MS™ platform embeds a fully-featured RF planning tool that closes the loop by automating WiBAS™ radio network's planning, rollout, optimization and maintenance stages under a single pane-of-glass. The WiBAS adopts the latest standards and most advanced technologies to deliver wireless solutions that best fit customer current and future needs, specifically concerning:

- Support for standardised formats of 3D buildings and 3D maps
- Export of coverage maps in standard formats (Google Earth / ASCII, etc.)
- Easy project migration from other radio planning tools (through standard-compliant .csv files)
- Support for standard DEM/DSM formats (ASCII Grid and BIL)
- Support for standard radio and antenna equipment files
- ITU standards and digital maps included
- Multi-vendor equipment files for improved inter-operability (industrial standards compliance)

Specific standards include:

- RFC 793 Transmission Control Protocol (DARPA Internet Program Protocol Specification).
- RFC 1155 Structure and Identification of Management Info for TCP/IP-based Internets.
- RFC 1157 A Simple Network Management Protocol (SNMP).
- RFC 1212 Concise MIB definitions.
- RFC 1213 Management Info Base for Network Management of TCP/IP-based Internets: MIBII.
- RFC 1215 A Convention for Defining Traps for Use with the SNMP.

3.16.3 Data used for tests

In order to test the functionalities of UNIMS platform various types of data has been used. Since the development and implementation have been mostly performed remotely and in separation from other SAFETY4RAILS tools, in order to test and validate the functionalities of UNIMS, the real data from infrastructures owned by Intracom and most relevant to SAFETY4RAILS project have been used. In order to enhance the perception of advanced functionalities of the platform, additional synthetic data have been also added. This way, Intracom was able to create a more "interesting" situations mimicking "real" ones that might be (possibly/likely) faced in relevant environments.

As UNIMS could not have been demonstrated in SAFETY4RAILS trials, including the last one in Milan, an attempt was made to align the data from pilot sites with actual/real data from Intracom infrastructures in the demonstrations built at Intracom premisses (as foreseen to be shown in recordings of demos presented at the final project event in Paris at the end of September 2022). This allowed recreation of most relevant and useful data types thus creating a detailed environment to test it in with various threats.

Although integration with other tools in SAFETY4RAILS have not been completed in time for Milan tests, similarly to other tools from Intracom, also UNIMS offers capabilities of integrating with Kafka message brokering services in SAFETY4RAILS project. The UNIMS hosts its own message broker, as part of its

[21] https://intracom-telecom.com/en/products/wireless_network_systems/netw_manag_systems/NetworkLifecycleMgmt.htm
[22] https://intracom-telecom.com/en/products/wireless_network_systems/netw_manag_systems/RadioPlanner.htm
[23] https://intracom-telecom.com/en/products/wireless_network_systems/netw_manag_systems/RadioPlanner.htm

internal message exchange mechanism among its diverse components. This offers capabilities of subsequently linking directly with Kafka message broker of the SAFETY4RAILS integrated platform.

Here are presented the main types of data which have been used in the testing phases.

TABLE 16: NETWORK TRAFFIC DATA

Type	Agent-based network traffic data.
Source	Use-case owner – in our case test site host (i.e., Intracom)
Amount	Complete (isolated) intranet traffic data.
Number of time tests performed	One (1) day worth of data – test period

TABLE 17: ENERGY INFRASTRUCTURE DATA

Type	Data from switches/controllers of energy backup generators Data from client devices including consumption data access control
Source	Use-case owner – in our case test site host (i.e., Intracom)
Amount	Complete data from infrastructure components, subject to testing.
Number of time tests performed	One (1) day worth of data – test period

TABLE 18: ACCESS CONTROL DATA

Type	Access control data from entries/exits, motion sensors, control access etc
Source	Use-case owner – in our case test site host (i.e. Intracom)
Amount	All available data from areas subject to tests.
Number of time tests performed	One (1) day worth of data – test period

TABLE 19: THREAT DATA INFORMATION

Type	Alert messages with threat types determined, location and forensic data
Source	Inherent Artificial Intelligence algorithms operating on integrated data Rule-based engine output (corresponding to correlated data analytics)
Amount	One to several message (per simulated threat) depending on whether it was a detection or persistent intrusion(s)
Number of time tests performed	One (1) day worth of data – test period

3.16.4 Test Data Report

This section reports the tests executed for uni|MS^{TM}, based on requirements described in D1.4 par. 2.3.15.

Test.-ID	uni|MS^{TM} _TR_01
Addressed Requirement	uni|MS^{TM} _01 **Unified management for networks, infrastructure and systems**. • Simple installation and no complex setup is required • Info about degrading of network conditions • Avoidance of service-affecting problems • Surveillance with physical control of access to the site
HW / SW preparation	Since it has been ultimately infeasible to demonstrate the UniMS system in any of the SAFETY4RAILS piloting events, a self-contained demo system has been built and populated with synthetic data originating from systems deployed in the Intracom premises in Athens (Greece). The deployment of the UniMS is at Intracom premises in Athens. Considering that its instance is currently used for commercial applications, there has been a security imposed limitation for opening its services to prototype-grade services from SAFETY4RAILS, considered by IT security of Intracom as an excessive high security risk for company's commercial operations. Therefore, provisions for integration with SAFETY4RAILS tools have been implemented, though access to such services has been so far limited. Therefore, synthetic data and some of the past records have been

	used to produce demo videos, which will be made available to partners during the final event in September 2022.
Test inputs	UniMS accommodates a range of sensors, including network traffic monitors from hardware network controllers, surveillance feeds, environments sensor data, physical access sensors and management data for energy devices
Test procedure	**Step 1**: Management of multiple technology domains from a single platform (wireless backhaul / transport, wireless broadband access, FWA access, etc.) with unified user interface that is modern, simple and convenient to use. Highly-effective service fulfilment & assurance ensure improved user experience and reduced NOC costs. **Step 2:** Unified North Bound Interfaces (NBIs) thereby reducing the OSS integration workload **Step 3:** Continuous monitoring of doors, motion detectors and cameras (CCTV) with infrared capabilities, greatly improving the security of telecom sites. **Step 4:** Remote and schedule maintenance of battery cells to improve reliability and prolong their lifetime. **Step 5:** Improving efficiency & operational cost of power generators via continuous automatic monitoring. **Step 6:** Improving reliance on power from generators & minimized fuel theft through fuel tank monitoring.
Expected Results	**Step1:** Improved reliability of the overall telecommunications network **Step 2:** Improved operational reliability of the Unified North Bound Interfaces (NBIs) **Step 3:** Improved physical security **Step 4:** Increased lifetime of batteries **Step 5:** Avoiding power generator malfunctioning **Step 6:** Increased backup power reliability
Pass/Fail	All tests successful
Deviation Encountered	N/A
Problems	N/A
Comments	N/A

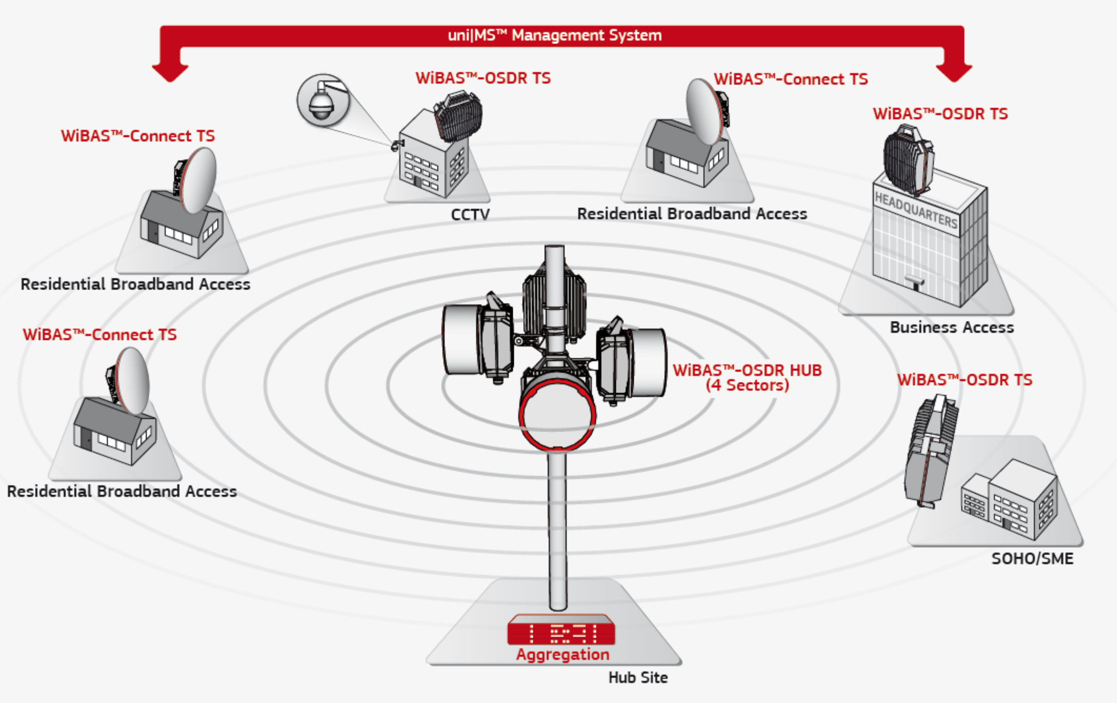
Test.-ID	uni|MS^{TM} _TR_02
Addressed Requirement	uni|MS^{TM} _02 **Conformity with overarching and S4RIS platform specific requirements**. Ensure that any work connected with this tool conforms to the overarching and S4RIS platform specific requirements included in section 2.2
HW / SW preparation	To facilitate the integration with other SAFETY4RAILS tools and the integrated SAFETY4RAILS Dashboard, additional developments have been made to adapt its REST WEB service interfaces to cater for JSON message content agreed to be exchanged among SAFETY4RAILS tools. Furthermore, considering that UniMS accommodates alternative Message Broker (Google pub/sub) to SAFETY4RAILS

	(Kafka), additional development was necessary to enable translation and exchange of message ques among the two brokers.
Test inputs	N/A
Test procedure	**Step 1:** Integration with SAFETY4RAILS Dashboard **Step 2:** Integration with SAFETY4RAILS Kafka Message Broker
Expected Results	**Step 1:** UniMS integrated as a separate tab or iFrame within the S4R Dashboard **Step 2:** Subscription and consumption of messages from SAFETY4RAILS Kafta message broker
Pass/Fail	**Step 1:** FAIL **Step 2:** FAIL
Deviation Encountered	The integration with SAFETY4RAILS Dashboard could not have been practically tested since SecaaS could not be directly connected neither to the SAFETY4RAILS Dashboard not the Kafka Message Broker. The practical test showing potential for integration with SAFETY4RAILS adopted methodology has been successfully validated using synthetic internal benchmarking and demos of those test will be made available to partners for the final meeting in September 2022.
Problems	Lack of practical feasibility to evaluate UniMS in SAFETY4RAILS pilots
Comments	Refer to section “**Deviations Encountered**” for details.

3.17 WIBAS

3.17.1 Overview

WiBAS™, a state-of-the-art Point-to-MultiPoint (PtMP) native Ethernet microwave product line, perfectly fits demanding operator needs. Specially designed for high-speed multi-service applications, WiBAS™ offers a wide service area footprint reaching distant underserved areas and locations lacking telecommunications infrastructure. WiBAS™ optimally addresses today's requirements for ultrabroadband Fixed Wireless Access (FWA) and smooth migration to networks with 5G speeds. With a powerful core engine and field-proven reliability, WiBAS™ provides significant CapEx & OpEx savings to operators requiring to deploy and provision their network quickly and effectively while maintaining a low-enough TCO to achieve viable service pricing levels. WiBAS™ opens up new horizons in reaching underserved residential as well as business customers. Employing today's most advanced technologies, WiBAS™ enables a wide range of profitable business plans, providing a key differentiator of operator success. A typical architecture contains:



WiBAS is best used for:

Ultra-broadband FWA for sub-urban and rural residential areas

- Competitive Service Providers planning to develop business with high-end customers to offer legacy and broadband access services (telephony, Web/IP services, metro Ethernet connectivity, etc.)
- Public sector organizations, utility companies, banks, etc. needing to deploy own resilient & backup networks in underserved areas, or in areas lacking wireline infrastructure
- Government authorities for secure private networks (CCTV, LAN, info-kiosk)
- Network access providers planning to offer bit-stream services to WISPs

WiBAS is a family of solutions, includes: G5 Connect Plus , G5 DualBS , G5 SmartBS , evoBS , micro-BS , OSDR and Connect .

3.17.2 Development and Quality standards adopted

The management and automations of WiBAS™ radio network's planning, rollout, optimization and maintenance stages is performed under a single pane-of-glass using the integrated Intracom Telecom's uni|MS™ platform that embeds a fully-featured RF planning tool for WiBAS. Regarding the range of applicable standards that the combined Intracom telecom's wireless solutions comply with, please refer to section 3.16.2 earlier.

3.17.3 Data used for tests

Since WiBAS system is NOT a threat detection system per-se, but more of a threat prevention infrastructure by employing a secure and less-intrusion-prompt telecommunication infrastructure, its testing methodology in SAFETY4RAILS project has been to integrate it with UNIMS system mentioned in section 3.16 above. Therefore, data used in evaluating the added value of WiBAS system have been generally network traffic passed to the abnormality and intrusion detection components embedded into the UNIMS platform.

NOTES:

- UNIMS is included by default with WiBAS when deploying it in operational environments
- Data used in tests have been offered on complimentary bases by one of Intracom commercial partners (confidential) as part of the pre-purchase demonstration in the relevant operational railway environment

Here are presented the main types of data which have been used in the testing phases.

TABLE 20: NETWORK TRAFFIC DATA

Type	Network traffic data (in case of WiBAS, over microwave links)
Source	Use-case owner – in our case test site host (i.e., Intracom)
Amount	Complete (isolated) microwave network traffic data.
Number of time tests performed	One (1) day worth of data (commercial railway partner) – test period

TABLE 21: THREAT DATA INFORMATION

Type	Alert messages with threat types determined, location and forensic data
Source	Inherent Artificial Intelligence algorithms operating on integrated data Rule-based engine output (corresponding to correlated data analytics)
Amount	One to several message (per simulated threat) depending on whether it was a detection or persistent intrusion(s)
Number of time tests performed	One (1) day worth of data (commercial railway partner) – test period

3.17.4 Test Data Report

This section reports the tests executed for WIBAS, based on requirements described in D1.4 par. 2.3.16.

Test.-ID	WIBAS_TR_01
Addressed Requirement	WIBAS _01 **Advanced Wireless Broadband Access for Enterprise Users**. L1 Throughput (net) per Terminal (Mbit/s) (Downlink / Uplink): • 730 / 85 (TDD @ 100 MHz) (8:1 DL/UL TDD Split Ratio.) • 930 / 630 (FDD @ 112 MHz) Max achieved throughput per direction. Supported channel bandwidths: • FDD: 56/112 MHz • TDD: 40/50/75/100 MHz Less than 3.5 Kg (radio and antenna) Operation at area-licensed frequencies: 24.25-29.50 GHz Auto-Polarization feature Slim form-factor radio units Compatibility with a 30 cm or 60 cm parabolic antenna. Range extending to 10 km.
HW / SW preparation	The WiBAS infrastructure has NOT been deployed in the SAFETY4RAILS project. The real deployment requires: • installation of WiBAS microwave transmitters

	• installation of UniMS network management platform at Intracom • integration of UniMS controller with local mobile operator’s network infrastructure
Test inputs	Network traffic from local mobile network operator’s infrastructure
Test procedure	**Step 1:** Verification of connection via WiBAS using UniMS network management platform
Expected Results	Peer-to-Peer (P2P) line of sight transmission of high-bandwidth traffic in excess of 300gbps verified via UniMS network management platform
Pass/Fail	N/A
Deviation Encountered	The WiBAS system is a telecommunications hardware infrastructure and its form as well as use has been misunderstood in the SAFETY4RAILS project preparation. Since it contains a set of large microwave hardware base stations for which the connection to mobile network operator network is a pre-requisite, the deployment in trials as defined in SAFETY4RAILS was infeasible. Therefore, following an agreement with project coordinator in early 2021, the WiBAS system was NOT expected to be physically demonstrated, instead presentations to users with remote demos were conducted.[24]

Test.-ID	WIBAS_TR_02
Addressed Requirement	WIBAS _02 **Conformity with overarching and S4RIS platform specific requirements** (Ensure that any work connected with this tool conforms to the overarching and S4RIS platform specific requirements).
HW / SW preparation	Refer to WIBAS_TR_01
Test inputs	Refer to WIBAS_TR_01
Test procedure	**Step 1:** Validation of secure transmission over WiBAS – NOT feasible to be intercepted, hence
Expected Results	**Step 1:** DEFAULT compliance with over-reaching objective of SAFETY4RAILS project in providing long-range secure means of communication to railway network operators.
Pass/Fail	N/A
Deviation Encountered	Refer to WIBAS_TR_01

[24] Comment by Fraunhofer as coordinator, as stated in the Periodic Report 1 (project period October 2020-September 2021), page 61: “The deliverable D1.4 included WiBAS as one of the contributory tools of the S4RIS platform (D1.4, section 2.3.17). ICOM did however indicate during the production of D1.4 that it would be unlikely that it could be deployed during the simulation exercises because of: cost, restrictions on travel due to the pandemic and access to end-user data which was unexpected to be provided. At the same time, ICOM proposed that the tools SecaaS and UniMS could be useful additional contributory tools for the S4RIS and they are included as such (D1.4 sections 2.3.11 and 2.3.16).” The tools SecaaS and UniMS are reported on in this present report in sections 3.11 and 3.16.

3.18 WINGSPARK

3.18.1 Overview

The WINGSPARK platform is dedicated to detecting abnormal events (anomaly detection). It offers a monitoring functionality and abnormalities identification in measurements from various sources and sensors. Through its analytics-mechanisms delivers insights, to better understand past and current issues and generate insights that can help predict and optimize the current and future actions, enabling faster, more efficient, and reliable decision making.
In the context of the project, the provided functionality is focused primarily on train speed, energy consumption and crowd concentration monitoring exploiting the capabilities of AI and deep learning, which are described with details in the deliverable D4.1. In summary the components provided under SAFETY4RAILS project are:

- Time-series based anomaly detection utilizing train speed measurements
- Time-series based anomaly detection utilizing energy consumption measurements
- Overcrowded situations in the monitored railway infrastructure, based on video acquired through closed-caption cameras.

3.18.2 Development and Quality standards adopted

For the development of the services the stack listed below was used:

- Django, as Object-Relational Mapper (ORM)
- Django Rest Framework JSON:API + HATEOAS, as the REST framework and API specification
- Postgresql as the database development tool
- uWSGI as the host service
- Nginx as Web Server and Reverse Proxy
- python open source statistical packages (numpy, scikit-learn, pandas) for the timeseries anomaly identification
- PyTorch deep learning library for the crowd concentration estimation module

The API also comes with API Documentation Swagger and Redoc.

Regarding the quality standards, all the processes followed were compliant with ISO international standards, ensuring the soundness of all operations. In particular:

- The quality management was compliant with ISO9001:2015
- The information security management was compliant with ISO27001:2013

3.18.3 Data used for tests

Types of data

Position

- Id: uuid
- Name: character varying
- Latitude: double precision
- Longitude: double precision

Trains

- Id: uuid
- Train name: character varying
- Timestamp: timestamp with time zone
- Departure stations: character varying

- Departure time: timestamp with time zone
- Arrival station: character varying
- Arrival time: timestamp with time zone

Velocitysensor (Sensors' velocity measurements) related to the position and the train

- Id: uuid
- serial number: character varying
- name: character varying
- timestamp: timestamp with time zone
- velocity: double precision
- units: character varying (default km/h)
- train_id: uuid
- position_id: uuid

Velocitystatistics (velocity statistics from sensors' measurements) related to the velocitysensor

- id: uuid
- type: character varying
- subtype: character varying
- classification: character varying
- is_event: boolean
- message: text
- anomaly value: double precision
- event severity: character varying
- velocitysensor_id: uuid

Camerasensors (Camera sensors' measurements) related to a position

- id: uuid
- serial number: character varying
- name: character varying
- timestamp: timestamp with time zone
- resolution: character varying
- framerate_fps: integer
- image name: character varying
- image: character varying
- density heat map: character varying
- position_id: uuid

Note the image and density heat map show the path to the image file and density heat map file which are stored in the file system of the server and not in the database.

Camera statistics (Statistics from the camera) each one related to the one camera sensor

- id: uuid
- type: character varying
- subtype: character varying
- classification: character varying
- is_event: Boolean
- message: text
- max_people: integer
- no_people: integer
- severity: character varying

- camera_id: uuid

Annotations

- id: uuid
- serial number: character varying
- asset_name (velocity or camera sensor): character varying
- timestamp: timestamp with time zone
- type: character varying
- subtype: character varying
- classification: character varying
- is_event: boolean
- message: text
- name: character varying
- status: character varying
- event_severity: character varying
- value: double precision

Events

- id: uuid
- data_source: character varying
- source_IP: character varying
- destination_IP: character varying
- asset_ID (velocity or camera sensor): character varying
- source_event_time: timestamp with time zone
- source_event_id: character varying
- _comment: character varying
- event_category: character varying
- type: character varying
- subtype: character varying
- descriptrion: character varying
- name: character varying
- severity: character varying\

Sources

- Positions: data from the internet
- Trains: fictional names with fictional schedules - related to the Positions
- Data velocities provided from data acquisition by provided by Rete Ferroviaria Italiana S.p.A. (RFI) at the location of a Rome train station for the length of a day; extrapolation to fit a duration of approximately a month for each position (see Note 1* at the end of the script)
- Anomaly scores calculated from the prediction model of the tool
- Cameras video streams provided by Rete Ferroviaria Italiana S.p.A. (RFI) at the location of a Rome train station on the 13th May of 2022 (see Note 2* at the end of the script)
- Camera statistics calculated from the statistic's visual algorithm of the tool
- Events, Annotations and Kafka messages are created
    - for velocity every time there is an event
    - for every camera image

Amounts

- Locations: 2 (Rome train station and Milan train station)
- Trains:

    - for Rome: 4927
    - for Milan: 2260

- Trains schedules: as many as trains
- Velocity Measurements: 5013
    - Rome: 2753
    - Milan: 2260

- Timestamps as many as sensor measurements:
    - Romei:
        - from 2022-05-02 21:30:00+00
        - to 2022-06-01 11:50:00+00
        - with 15 minutes interval (almost everywhere)
    - Milan:
        - from 2022-06-12 00:15:00+00
        - to 2022-07-06 10:05:00+00
        - with 15 minutes interval (almost everywhere)

- Velocitystatistics
    - as many as the velocity measurements for each position
- Camera Sensors measurements: 16
    - Rome: 11
    - Milan: 5

- Camera statistics
    - As many as the images for each location

- Events:
    - Velocity:
        - Romei: 23
        - Milan: 76
    - Cameras: as many as camera sensors measurements

- Annotations:
    - Velocity sensors: as many as events
    - Cameras: as many as cameras

- Kafka
    - As many as event (plus some more for the tests)

Number of tests performed

Tests in Rome and Milan exercises

- Velocity:

For the tests we gave some velocities that could match the scenarios at both Rome and Milan train stations for the Rome and Milan exercises respectively:

Number of velocity inputs

- Rome: 5
- Milan: 5

The scores predicted anomalies as for the usual cases, events annotation and kafka messages were created appropriately

Camera: the same images provided for the development where also used for the tests

NOTES[25]

1* Data for Train speeds

- "Generate partially artificial data: from a small sample of real data, which can be acquired from the above three methods, artificial data can by generated by sampling methods e.g. bootstrap method, this can be done individually per tool and needs to be synchronized amongst tool providers"

2* Video data

- "Share collected data: using data which was collected before by end-users (and acquired by consortium partner or external stakeholder interactions), i.e. realistic data but from an earlier time period. Where necessary, this data can be pseudonymised or anonymised. Alternatively, other sources of data can be considered such as open data."

3.18.4 Test Data Report

This section reports the tests executed for WINGSPARK, based on requirements described in D1.4 par. 2.3.18.

Test.-ID	WINGS_TR_01
Addressed Requirement	WINGS _01 **Data ingestion from devices.** Acquisition of input data
HW / SW preparation	HW was not provided. Used the alternative solution / variant of offline data
Test inputs	Data acquisition for a day and extrapolation to fit a duration of approximately a month for each position
Test procedure	Step 1: Creation of data, using python population scripts Step 2: Persistence in the database Step 3: Retrieve and visualise data in the GUI or for analytics purposes
Expected Results	The train speed data, camera images and event annotations shown in the GUI Analytics provide insights using data persisted in the database.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

Test.-ID	WINGS_TR_02
Addressed Requirement	WINGS _02 **Data Management/Analysis** Management and analysis of data
HW / SW preparation	HW was not provided so no Websockets are used REST APIs are created to enable the user to communicate with the database - For the analytics algorithms - For the GUI Analytics are applied on the fly for each new data item in the database using Django Signals, so no cronjobs where necessary

[25] Methods for collecting data as amongst those described in D1.4 Specification of the overall technical architecture, p.189.

Test inputs	A. Train Speed anomaly detection mechanism New train speed values - one which triggers the analytics, and - one who does not B. Crowd concentration estimation mechanism New image: analytics for camera is triggered
Test procedure	A. Train Speed anomaly detection mechanism Step 1: Enter new speed Step 2: Calculate the anomaly score from the analysis on the fly B. Crowd concentration estimation mechanism Step 1: the image is saved in the database and the image analysis starts
Expected Results	A. Train Speed anomaly detection mechanism If the anomaly score is at the limit to called as an event an annotation is created and the event is sent to the Kafka B. Crowd concentration estimation mechanism For the camera, if the analysis leads to an overcrowded situation then an annotation is created and the event is sent to the Kafka
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	A. Train Speed anomaly detection mechanism All anomaly scores are shown in the GUI with a red marker: when an event is identified the score is highlighted with a bigger marker B. Crowd concentration estimation mechanism All images from the cameras are shown in the GUI regardless of if an event is identified

Test.-ID	WINGS_TR_03
Addressed Requirement	WINGS _03 **Support of A.I. techniques (train speed case)** Usage of A.I. for enhanced prevention, detection, response
HW / SW preparation	A. Train Speed anomaly detection mechanism The analytics algorithms have all been implemented using python and they use REST APIs to retrieve and save the input and the output data respectively. As it regards the train speed modality, the required mechanism has been implemented supporting any univariate time-series signal as input, describing the speed of the investigated train.
Test inputs	As in step 2
Test procedure	A. Train Speed anomaly detection mechanism Step 1: Provide the initially collected time-series signal and fit the anomaly detection mechanism on that Step 2: Compute dynamically the threshold based on the statistical properties of the provided data. Step 3: Annotate each incoming instance / speed through the fitted mechanism. Step 4: Evaluate the model's performance based on useful metrics, if annotated data have been provided
Expected	A. Train Speed anomaly detection mechanism

Results	i) High anomaly detection rate and low false alarm indications. ii) Great response on both fitting the provided data and annotating the unknown instances.
Pass/Fail	Pass
Deviation Encountered	
Problems	Train speed anomaly detection: Our data were artificially created by benchmarks or by extrapolating the few provided ones.
Comments	

Test.-ID	WINGS_TR_04
Addressed Requirement	WINGS _03 **Support of A.I. techniques – crowd concentration case** Usage of A.I. for enhanced prevention, detection, response
HW / SW preparation	B. Crowd concentration estimation mechanism The analytics and deep learning approach have all been implemented using python and respective statistics, computer vision and deep learning packages (mainly "opencv", "sklarn", "pytorch") and they use REST-API architecture to retrieve and save the input and the output data respectively.
Test inputs	Camera feed -either live stream ("rtsp" - protocol) or recorded video (*.mp4)- from which the frame to be processed is extracted
Test procedure	B. Crowd concentration estimation mechanism Step 1: Provide the live stream or the recorded video file to the service which starts running. Step 2: The service runs and calculates the density heatmap from which it infers the people count. Step 3: The count is compared to an approximate count calculated by a human annotator
Expected Results	Low normalized mean absolute error (MAE) of the crowd count, compared to count provided by the human annotator
Pass/Fail	Pass
Deviation Encountered	
Problems	The data acquired for the testing purposes was mainly gathered from open sources and the ones that were actually from the trial scene was very limited
Comments	

Test.-ID	WINGS_TR_05
Addressed Requirement	WINGS _04 **User-friendly GUI** Provision of a user-friendly GUI for interfacing with users
HW / SW preparation	Frontend has been implemented in Angular 12, using REST API consumption. The application is shared to the user through a nginx web server with client side rendering.
Test inputs	New train speed notifications New camera images

Test procedure	Step 1: New train speed records and images (raw and annotated) in the database Step 2: The client sends requests to the server to receive new data from the database (notifications and images) through REST APIs Step 3: The client receives the responses from the server and the received data are shown in the dashboard
Expected Results	All the requested data sent by the server are shown in the dashboard. If there is a new entry in the database, the relevant dashboard elements are updated with the new data.
Pass/Fail	Pass
Deviation Encountered	
Problems	
Comments	

4. Conclusions

This deliverable D6.4 presented the results related to the validation and evaluation of the tools included in the S4RIS platform obtained by the technical developmental (i.e. none end-user) partners and the most advanced S4RIS platform (with its contributory tools) reached at the end of the development cycle in the SAFETY4RAILS project.

Each contributory tool (identified in D1.4 section 2.3) and a sub-set of the overarching requirements and specifications placed on the S4RIS platform (identified in D1.4 section 2.2) have been subject to validation tests in laboratory following the test report schema proposed and agreed in task T6.4 (having as reference the technical requirements and specifications described in section 2.2 and 2.3 of D1.4, identified for a product). The S4RIS platform component providers and the contributory tool providers were advised to focus on those requirements and specifications which included both new developments (compared to established solutions) and which have a strong impact on the reliability of results. Almost all of the tests had a positive outcome (*Pass*). Minor deviations were highlighted only for some tests (*Pass with deviations*) for which a justification has been provided.

The Annex IV provides a good faith evaluation by the T6.4 of which of the D1.4 requirements/specifications were tested in the T6.4 and how far they were met, while acknowledging that the Technology Readiness Level (TRL) is in most cases still below TRL9. The evaluation relies on the results reported by the individual contributory tool providers.

As stated in D8.5: "In the D1.4, altogether 277 requirements with priority of essential (168), essential/conditional (6), conditional (54), optional (14) and not specified (35) were defined for the S4RIS platform with its contributory tools."[26] 70 essential, 1 essential/conditional and 7 conditional requirements were tested in the T6.4.

Table 8 provides information on the number of tools requirements/specifications as well as the number of the tested requirements/specifications as assessed by tests.

TABLE 22: SAFETY4RAILS GOOD FAITH ASSESSMENT OF D1.4 REQUIREMENTS/SPECIFICATIONS TEST COVERAGE IN T6.4

Requirement	Priorities and tests							
Specification type	Essential	Tested	Conditional	Tested	Optional	Tested	No specific	Tested
S4RIS platform specific	24		1		1			
Knowledge / Usability	1							
Graphical User Interface - GUI	16	14	10	1	2			
Standards	34 [1)]		21					
Data Protection	1							
Open-source intelligence technologies for the S4RIS	4		1					
Blockchain technology	3				1			
Railways in the Smart City	2		2				6	

[26] D8.5 Final version of evaluation report, page 58.

Requirement	Priorities and tests							
Specification type	**Essen tial**	**Tested**	**Condi tional**	**Tested**	**Optio nal**	**Tested**	**No specific**	**Tested**
Crisis Management	1						29	
Communication with the public	5		2		1			
Cost	1							
BB3d (RINA-C)	6	4						
CaESAR (Fraunhofer)	7	6	1	1				
CAMS (RMIT)	9	4	2					
CuriX (CuriX)	6	5	3		2	1		
DATAFAN (Fraunhofer)	9	6						
Ganimede (LDO)	5	3	1	1				
iCrowd (NCSRD)	3	2	1	1	3	3		
PRIGM (ERARGE)	6	5	1	1				
RAM^2 (ELBIT)	7	6						
SARA (RINA-C)	2 [2)]	1						
SecaaS (ICOM)	2	1	1					
SecuRail (STAM)	3	2	3	2	1	1		
Senstation (ERARGE)	4	1	1					
SISC2 (ICOM)	1	1	1					
TISAIL (TREE)	5	4			3	2		
uni|MS™ (ICOM)	1	1	1					
WIBAS (ICOM)	1	1	1					
WINGSPARK (WINGS)	5	4						

1) includes five essential/conditional requirements
2) includes one essential/conditional requirement, which has been tested

Also, in Annex IV:

- The “S4RIS platform specific” and “Knowledge / Usability” requirements and specifications (D1.4, section 2.2. requirements/specifications P01-P024 and EU+U01) have been evaluated based on design and observation.
- For the requirements/specifications of the contributory tools (contributory tools as identified in D1.4 section 2.3) not directly tested under T6.4 an evaluation has been provided based design, observation and test (where relevant) from other tasks in WP3-6 and WP7.

The standards (55), data protection (1), Open source intelligence technologies for the S4RIS (5), Blockchain technology (4), Railways in smart city (10), crisis management (30), communication with the public (8) and costs (1) were not evaluated in Annex IV and as such are not evaluated in this report.

On the basis of the above evaluation and methods, Annex IV provides the overall evaluation on how far the 277 requirements/specifications were met:

- Achieved: 90
- Partially achieved: 54
- Not achieved: 10
- Not known to date (of extent of achievement): 123 (incl. the 114 requirements not evaluated in this report):

ANNEXES

ANNEX I Glossary and acronyms

TABLE 23 GLOSSARY AND ACRONYMS

Term	Definition/description
AQAP	Allied Quality Assurance Publications
CAMS	Central Assest Management System
CCTV	Closed-circuit television
CO	Confidential
DMS	Distributed Message System
DoA	Description of the Action (Annex 1 to the Grant Agreement)
EC	European Commission
FPS	Frame Per Second
GUI	Graphical User Interface
GDPR	General Data Protection Regulation
IED	Improvised Explosive Device
IoCs	Input Output Control Systems
IRS	Interface Requirement Specification
ISO	International Standards Organization
KPIs	Key Performance Indicators
LTE	Long Term Evolution
MISP	Malware Information Sharing Platform
S4RIS	SAFETY4RAILS Information System
SARA	Securestation Attack Resilience Assessment
SAS	Software As a Service
SDD	Software Design Description
SSDD	System /Subsystem Design Description
SRS	System Requirement Specification
SE	Simulation Exercise
SIEMs	Security information and event management

STR	Software Test Report
TRL	Technology Readiness Level
UC	Use-Case
WP	Work-Package

ANNEX II Input test data for CaESAR

For completeness, in tabular form, example of Network input file and configuration file is presented.

Node file:

TABLE 24: AN EXAMPLE OF INPUT NODE FILE WITH DIFFERENT ATTRIBUTES FOR NETWORK COMPONENTS[27]

ID	Grid Type	Type	Latitude	Longitude	Repair Time	Name	Capacity	lines
3601	0	3	[redacted]	[redacted]	255	via vittorio veneto prima di via pascoli (ponte autostrada)	1	B708, B166, B83
46	0	3	[redacted]	[redacted]	108	Via Buozz 102 prima di Via Alfieri	1	B328, B220
2435	0	0,3	[redacted]	[redacted]	237	v.le f.test 300 prima di via bignami	1	B728, T31
37	0	3	[redacted]	[redacted]	168	V.le Milanofiori prima di V.le Gran S.Bernardo	1	B328
1056	0	3	[redacted]	[redacted]	273	via mazzolari fronte 19 prima di via campari	1	B74
255	0	3	[redacted]	[redacted]	157	Via Madonna Pellegrina prima di Via Giovanni XXIII	1	B431, B424
0	0	3	[redacted]	[redacted]	153	C.so Sempion 83 prima di Via E. Filiberto	1	B57 B43, B48
484	0	3	[redacted]	[redacted]	134	Via Sauro prima via Manzoni	1	B566
219	0	0,3	[redacted]	[redacted]	206	C.so Milano dopo P.za Panceri (VAREDO DEPOSITO)	1	T179, B165

Edge file:

TABLE 25: AN EXAMPLE OF INPUT EDGE FILE WITH CONNECTIONS BETWEEN NODES AND ROUTE PROPERTY

GridType	Source	Target	Route
0	661	4208	EMI_M_M3
0	661	4309	EMI_M_M3
0	1755	4643	EMI_M_M3
0	1755	4593	EMI_M_M3
0	1758	1760	EMI_M_M3
0	1758	4201	EMI_M_M3
0	1759	1763	EMI_M_M3
0	1759	1760	EMI_M_M3
0	1760	1759	EMI_M_M3
0	1760	1758	EMI_M_M3
0	1763	4673	EMI_M_M3
0	1763	1759	EMI_M_M3
0	1845	1853	EMI_M_M3
0	1845	1847	EMI_M_M3

Config file:

```
{
   "sep": ";",
   "decimal": ".",
   "crs": "epsg:4326",
   "Group": "M4",
   "columns_to_drop": [
      "nodeAttr"
   ],
```

[27] Latitude and longitude redacted.

```
    "velocity": 400,
    "vehicle_start_positions": [0.0, 0.5],
    "timestep_duration": 10,
    "max_passengers": 1000,

    "nodes": {
        "files": [
            {
                "filename": "MDM_M4_GridNode.csv"
            }
        ],
        "column_mapping": {
            "Lon": "x_pos",
            "Lat": "y_pos"
        }
    },
    "edges": {
        "files": [
            {
                "filename": "MDM_M4_GridArcs.csv"
            }
        ],
        "column_mapping": {
            "Source": "source_ID",
            "Target": "target_ID"
        }
    },
    "impacts": [
        {
            "node_IDs": [3, 194],
            "impact_timestep":2000,
            "restore_duration":1000
        }
    ],
    "_impacts": [
        {
            "node_IDs": [145, 131],
            "impact_timestep": 0,
            "restore_duration": 10
        }
    ]
}
```

ANNEX III JSON messsages for RAM2 tests[28]

```
{Ankara:
    "events": [
        {
            "value": {
                "asset_ID": "25bdaa8f-b1d54bf1-89df-3309da492d89",
                "data_source": "Ganimede",
                "event_type": "Abandoned Object",
                "event_subtype": "Abandoned Bag",
                "event_category": "Railway Station",
                "event_severity": "SEVERE",
                "source_event_time": 1643908977,
                "source_event_id": "9fe73e9-75ff-48ec-b453-2ba953e6894b"
            }
        },
        {
            "value": {
                "asset_ID": "e0d4a35d-16e3-4079-828f-f0ca2a58c49c",
                "data_source": "Senstation",
                "event_category": "Host Security",
                "event_type": "Physical intrusion",
                "event_subtype": "Unexpected Physical Enterance",
                "event_description": "Unexpected Physical Enterance into the
Electronic Equipment Room ",
                "event_severity": "HIGH",
                "source_event_time": "1645797552",
                "event_name": "Physical_Intrusion in unexpected time",
                "source_event_id": "4db3c562-9873-4456-91ff-dee424092607",
                "event_info": {
                    "AnomalyName": "Abnormal Change Both in Light in [redacted] and
Acceleration in Door Movings",
                    "AnomalyType": "Physical Intrusion",
                    "EventId": "eb7ff366-1b8a-4cb7-b48b-5795e23ffc16",
                    "AnomalyHandled": "True"
                },
                "extra_fields": {
                    "sensors": [
                        {
                            "sensor_value": "245 lx",
                            "sensor_id": "ID066",
                            "sensor_name": "BP#03 (ambient light sensor)",
                            "threshold": "200 lx",
                            "min_val": "0 lx",
                            "max_val": "245 lx"
                        },
                        {
                            "sensor_value": "-395 x,-322 Y,449 Z",
                            "sensor_id": "ID067",
                            "sensor_name": "BP#04 (three-axis
accelerometer)",
                            "threshold": "-395 x,-322 Y,500 Z",
```

[28] Specific details redacted.

```
                            "min_val": "-395 x,-322 Y,449 Z",
                            "max_val": "-395 x,-322 Y,849 Z"
                        }
                    ]
                }
            }
        },
        {
            "value": {
                "asset_ID": "09bfec23-1a58-4224-a73e-30e2d69979a2",
                "data_source": "Senstation",
                "event_category": "Host Security",
                "event_type": "Physical intrusion",
                "event_subtype": "Physical Damage",
                "event_description": "Attacker Damages and burns the [redacted]
system",
                "event_severity": "HIGH",
                "event_name": "Physical Damage",
                "source_event_time": "1645797505",
                "source_event_id": "37a5e510-0f93-4001-b773-ddfa28cd824e",
                "event_info": {
                    "AnomalyName": "Abnormal Heat and Vibration observed in the
[redacted]",
                    "AnomalyType": "Physical Damage",
                    "EventId": "e9f54808-f23f-4161-a567-1d11b78872a6",
                    "AnomalyHandled": "True"
                },
                "extra_fields": {
                    "sensors": [
                        {
                            "sensor_value": "-395 x,-322 Y,449 Z",
                            "sensor_id": "ID067",
                            "sensor_name": "BP#04 (three-axis
accelerometer)",
                            "threshold": "-395 x,-322 Y,500 Z",
                            "min_val": "-395 x,-322 Y,449 Z",
                            "max_val": "-395 x,-322 Y,849 Z"
                        },
                        {
                            "sensor_value": "55.2 C°",
                            "sensor_id": "ID064",
                            "sensor_name": "Tibbo BP#01 (ambient
temperature sensor)",
                            "threshold": "55 C°",
                            "min_val": "-3 C°",
                            "max_val": "55.2 C°"
                        }
                    ]
                }
            }
        },
        {
            "value": {
                "asset_ID": "780fb26e-5910-4995-9860-bf1ee9d8e5fa",
                "data_source": "Senstation",
                "event_category": "System Event",
                "event_type": "Cyber Intrusion",
                "event_subtype": "Authentication Failure",
                "event_description": "Attacker tries to Authenticate him/herself into the
Control Pc Physically Appears in the □",
                "event_severity": "HIGH",
                "source_event_time": "1645872476",
                "source_event_id": "2dbb488f-245d-41e4-9174-ff74638a0d91",
                "event_info": {
                    "AnomalyName": "Unauthorized Access",
                    "AnomalyType": "Cyber Intrusion",
                    "EventId": "a8fcab2c-d71a-4b0f-8600-735acda12862",
                    "AnomalyHandled": "Finished"
                },
                "extra_fields": {
                    "Log": "/7.29.238.177 - - HTTP/1.1 200 2687 - Mozilla/5.0
(Windows NT 10.0: Win64: x64) AppleWebKit/537.36 (KHTML. like Gecko)
Chrome/96.0.4664.110 Safari/537.36 Edg/96.0.1054.62[05 / Jan / 2022: 14: 59: 06 + 0100] POST
/auth/realms/test/login-actions/required-
action?session_code=V1DZ140_r41JXEvgZYSo8khYhlmSWh16DzeNPV/6ktsäexecution=CONFI
GURE_TOTP&client_id=account-console&tab_id=CTA6aFq-vF0"
                }
            }
        },
        {
            "value": {
                "asset_ID": "09bfec23-1a58-4224-a73e-30e2d69979a2",
                "data_source": "Senstation",
                "event_category": "Host Security",
                "event_type": "Sensor Malfunction",
                "event_subtype": "Multi-Sensor Inconsistency",
                "event_description": "Inconsistency Between the Humidity and
Temperature Sensors Observed",
                "event_severity": "Medium",
                "event_name": "Multi-Sensor Inconsistency",
                "source_event_time": "1645797505",
                "source_event_id": "37a5e510-0f93-4001-b773-ddfa28cd824e",
                "event_info": {
                    "AnomalyName": "Mismatch between Humidity and
Temperature Sensors",
                    "AnomalyType": "Cyberphysical Attack",
                    "EventId": "e9f54808-f23f-4161-a567-1d11b78872a6",
                    "AnomalyHandled": "True"
                },
                "extra_fields": {
                    "sensors": [
                        {
                            "sensor_value": "%28",
                            "sensor_id": "ID065",
                            "sensor_name": "BP#02 (ambient temperature
and humidity sensor)",
                            "threshold": "%30",
                            "min_val": "%30",
						"max_val": "%60"
					},
					{
						"sensor_value": "55.2 C°",
						"sensor_id": "ID064",
						"sensor_name": "Tibbo BP#01 (ambient
temperature sensor)",

						"threshold": "55 C°",
						"min_val": "-3 C°",
						"max_val": "55.2 C°"
					}
				]
			}
		}
	},
	{
		"value": {
			"asset_ID": "09bfec23-1a58-4224-a73e-30e2d69979a2",
			"data_source": "Senstation",
			"event_category": "Host Security",
			"event_type": "Physical intrusion",
			"event_subtype": "Physical Damage",
			"event_description": "Attacker Damages and burns the [redacted]
system",
			"event_severity": "HIGH",
			"event_name": "Physical Damage",
			"source_event_time": "1645797505",
			"source_event_id": "37a5e510-0f93-4001-b773-ddfa28cd824e",
			"event_info": {
				"AnomalyName": "Abnormal Heat and Vibration observed in the
EER",

				"AnomalyType": "Physical Damage",
				"EventId": "e9f54808-f23f-4161-a567-1d11b78872a6",
				"AnomalyHandled": "True"
			},
			"extra_fields": {
				"sensors": [
					{
						"sensor_value": "-395 x,-322 Y,449 Z",
						"sensor_id": "ID067",
						"sensor_name": "BP#04 (three-axis
accelerometer)",

						"threshold": "-395 x,-322 Y,500 Z",
						"min_val": "-395 x,-322 Y,449 Z",
						"max_val": "-395 x,-322 Y,849 Z"
					},
					{
						"sensor_value": "55.2 C°",
						"sensor_id": "ID064",
						"sensor_name": "Tibbo BP#01 (ambient
temperature sensor)",

						"threshold": "55 C°",
						"min_val": "-3 C°",
						"max_val": "55.2 C°"
```

```
                        }
                    ]
                }
            }
        },
        {
            "value": {
                "data_source": "TISAIL",
                "event_type": "Vulnerability",
                "event_subtype": "Mail server",
                "event_category": "Host Security",
                "event_severity": "Medium",
                "event_description": "There is a mail server exposed to the Internet. This could be exploited by threat actors for initial compromise of the corporate network.",
                "source_event_time": 1647874478,
                "extra_fields": {
                    "exposed asset": "<Asset ID>",
                    "exposed information": "Mail Server may be exploited by threat actors"
                }
            }
        },
        {
            "value": {
                "asset_ID": "90e87773-9994-4ec4-b0c2-69631f090cac",
                "asset_name": "Station_PIS",
                "data_source": "Curix",
                "event_type": "PIS Anomaly",
                "event_subtype": "Unusual number of messages found in PIS",
                "event_category": "Railway Station",
                "event_severity": "SEVERE",
                "source_event_time": "<timestamp>",
                "source_event_id": "60fd6e5e-9344-47db-934b-a5d23da0c506"
            }
        },
        {
            "value": {
                "asset_ID": "C55875B6-98AC-41D4-00AA",
                "data_source": "OSINT",
                "event_category": "Physical Event",
                "event_type": "Public Safety",
                "event_subtype": "Explosion report in social media",
                "event_description": "Social media report of an explosion",
                "event_severity": "HIGH",
                "source_event_time": "2022-03-16 08:02:22.184422",
                "source_event_id": "f238aa0c-82a2-494b-9c42-c395493ad69b",
                "extra_fields": {
                    "messages": [
                        {
                            "text_content": "Just heard about a bomb going off in Ankara at the central train station"
                        }
                    ],
                    "tags": [
                        {
                            "name": "bomb"
                        },
                        {
                            "name": "ankara"
                        },
                        {
                            "name": "centrain train station"
                        }
                    ],
                    "position": {
                        "latitude": "[redacted]
                        "longitude""
                    }
                }
            }
        },
        {
            "value": {
                "source_IP": "127.0.0.1",
                "destination_IP": "127.0.0.1",
                "asset_ID": "Turnstile Gate #1 [redacted],
                "data_source": "DATAFAN",
                "event_category": "Railway Station",
                "event_type": "Crowd Concentration",
                "event_subtype": "Turnstile is blocked",
                "event_severity": "HIGH",
                "source_event_time": 1643642072,
                "source_event_id": "7034de5a21515a8bf167b32cd56bf287",
                "extra_fields": {
                    "Station": "[redacted]",
                    "Capacity_of_turnstile": 0,
                    "Expected_flow_rate_of_turnstile": 999,
                    "Passenger_overload_of_turnstile": 999,
                    "Time_stamp": 1643645672,
                    "Surrounding_stations": [
                        {
                            "Name": "[redacted]",
                            "Free_capacity": 999
                        },
                        {
                            "Name": "[redacted]",
                            "Free_capacity": 999
                        },
                        {
                            "Name": "[redacted],
                            "Free_capacity": 999
                        },
                        {
                            "Name": "[redacted]
                            "Free_capacity": 999
                        }
                    ]
                }
```

```
                        }
                },

{
"records": [
          {
             "value": {
                        "source_IP": "",
                        "destination_IP": "",
                        "asset_ID": "",
                        "data_source": "CaESAR",
                        "_comment": "",
                        "event_category": "Railway Systems",
                        "event_type": "Critical Station Impact",
                        "event_subtype": "Criticality and What-If Simulation results",
                        "event_name": "Critical Stations due to flooding",
                        "event_description": "Flooding of the Seveso river. Event simulation highlights
critical stations to be monitored and resource to be directed for more support and reduction of
impact",
                        "event_severity": "HIGH",
                        "source_event_time": "2022-06-10T10:00:00",
                        "source_event_id": "",
                        "extra_fields":{
                        "link_to_additional information": "https://192.102.163.182:3000",
                        "critical_components": "Porta Garibaldi Station, Zara Station, Isola, Marche"
                        }
                  }
          }
          ]
}

{Rome:
 "asset_ID": "90e87773-9994-4ec4-b0c2-69631f111cac",
 "asset_name": "Station_CCTV",
 "data_source": "Curix",
 "event_type": "CCTV availability",
 "event_subtype": "CCTV service response time increase (D)DoS Attack suspected",
 "event_category": "Cyber-Attack (DoS)",
 "event_severity": "SEVERE",
 "source_event_time": {{$timestamp}},
 "source_event_id": "60fd6e5e-9344-4711-934b-a5d23da0c506"
}
{
   "asset_ID":"25bdaa8f-b1d54bf1-89df-3309da492d89",
   "data_source":"Ganimede",
   "event_type":"Audio detection",
   "event_subtype":"Gun-shot",
   "event_category":"Railway Station",
   "event_severity":"SEVERE",
   "source_event_time":1643908977,

{
   "asset_ID":"25bdaa8f-b1d54bf1-89df-3309da492d89",
   "data_source":"Ganimede",
  "event_type":"Abandoned Object",
  "event_subtype":"Abandoned Bag",
  "event_category":"Railway Station",
  "event_severity":"SEVERE",
  "source_event_time":1643908977,
  "source_event_id":"9fe73e9-75ff-48ec-b453-2ba953e6894b"
}
{
  "source_IP":"xxx",
  "destination_IP":"xxx",
  "asset_ID":"ss1",
  "data_source":"WINGSPARK",
  "_comment":"Event Related Data: ",
  "event_category":"Railway System",
  "event_type":"Speed Anomaly",
  "event_subtype":"Unexpected High Train Speed",
  "event_description":"monitor train's speed and raise alarms in case of anomaly",
  "event_name":"High_Train_Speed",
  "event_severity":"HIGH",
  "source_event_time":"timestamp",
  "source_event_id":"xxx"
}
{
  "asset_ID":"25bdaa8f-b1d54bf1-89df-3309da492d89",
  "data_source":"Ganimede",
  "event_type":"People re-identification",
  "event_subtype":"People detection",
  "event_category":"Railway Station",
  "event_severity":"SEVERE",
  "source_event_time":1643908977,
  "source_event_id":"9fe73e9-75ff-48ec-b453-2ba953e6894b"
}
{
   "records": [
      {
         "value": {
            "source_IP": "127.0.0.1",
            "destination_IP": "127.0.0.1",
            "asset_ID":[redacted]",
            "data_source": "DATAFAN",
            "event_category": "Railway station",
            "event_type": "Crowd concentration",
            "event_subtype": "Abnormal passenger flow",
            "event_description": "Expected number of passengers exceeds the station capacity.
Thus, the station is either closed or the gate and turnstiles are blocked. Consider redirecting the
passenger flow to surrounding stations",
            "event_severity": "HIGH",
            "source_event_time": 1643642072,
            "source_event_id": "7034de5a21515a8bf167b32cd56bf287",
            "extra_fields": {
               "Station":[redacted]",
               "Gate": "xyz",
               "Capacity_of_turnstiles": 0,
               "Expected_flow_rate_of_turnstiles": 999,
          "Passenger_overload_of_turnstiles": 999,
          "event generated time": "<dd/mm/yyyy, xx:yy:zzzz>",
          "Surrounding_stations": [
            {
              "Name"[redacted]
              "Free_capacity": 999
            },
            {
              "Name'[redacted]",
              "Free_capacity": 999
            },
            {
              "Name[redacted]
              "Free_capacity": 999
            },
            {
              "Name[redacted]",
              "Free_capacity": 999
            },
            {
              "Name"[redacted]
              "Free_capacity": 999
            }
          ]
        }
      }
    }
  ]
}

{ Milano:
        "source_IP":"https://s4r.wings-ict-solutions.dev",
        "destination_IP": "https://s4ris-dms.iit.demokritos.gr:8082",
        "asset_ID":"Camera__RFI",
        "data_source": "WINGSPARK",
        "_comment": "Event Related Data: ",
        "event_category": "Railway System",
        "event_type": "Camera",
        "event_subtype": "Overcrowded",
        "event_description": "Overcrowded area, Raise Alarm, Consult WINGSPARK",
        "event_name": "Overcrowded Area 1",
        "event_severity": "HIGH",
        "source_event_time": "2022-07-06 10:30:00+00",
        "source_event_id": "xxx"
}
{
        "source_IP":"https://s4r.wings-ict-solutions.dev",
        "destination_IP": "https://s4ris-dms.iit.demokritos.gr:8082",
        "asset_ID":"Camera__RFI",
        "data_source": "WINGSPARK",
        "_comment": "Event Related Data: ",
        "event_category": "Railway System",
        "event_type": "Camera",
        "event_subtype": "Overcrowded",
        "event_description": "Overcrowded area, Raise Alarm, Consult WINGSPARK",
        "event_name": "Overcrowded Area 1",
        "event_severity": "HIGH",
        "source_event_time": "2022-07-06 10:30:00+00",
        "source_event_id": "xxx"
}
{
"records": [
            {
                "value": {
                            "source_IP": "0.0.0.1",
                            "destination_IP": "",
                            "asset_ID": "",
                            "data_source": "CaESAR",
                            "event_category": "Railway Systems",
                            "event_type": "Critical Station Impact",
                            "event_subtype": "Flooding in station",
                            "event_description": "Flooding in Seveso river. An outlook of expected impact
propagation to different stations in the network.",
                            "event_severity": "HIGH",
                            "source_event_time": "2022-06-10T10:15:00",
                            "source_event_id": "",
                            "extra_fields":{
                                          "link_to_additional information": "https://192.102.163.182:3000",
                                          "critical_components": ""
                            }
                        }
            }
            ]
}
```

ANNEX IV Good faith assessment of D1.4 requirements/specifications test coverage and further evaluation under T6.4 for this report

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✓)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	**T6.4**	**A**	**P**	**NA**	**NK**	
1	S4RIS platform specific	P-01	Platform modularity	Essential	-	-	-	x	-	-		x			Assessable based on design. Message exchange within the S4RIS platform achieved by KAFKA distributed message system (DMS). Modularity in the sense of integration in the S4RIS GUI implemented in two ways: the individual provision of web-based graphical user interfaces for those tools that provide a web-based GUI and being accessed via iframes or new Tabs the web-based S4RIS GUI. Possibility to weakly couple the GUIs of those tools that do not provide a web-based GUI possible e.g. via a link to an executable. Not all toos intergated.
2		P-02	Consolidation of end-user inputs	Conditional	-	-	-	-	-	-		x			Assessable based on design. In principle possible via the Distributed Messaging System (DMS) with publish/subscribe.
3		P-03	End User configuration	Essential	-	-	-	-	-	-		x			Assessable based on design. The indication is that end-users would need support for the delpoyment of the S4RIS platfrom and the (chosen) contributory tools.
4		P-04	Minimum requirements for S4RIS use	Essential	x	x	x	-	x	-	x	x			Assessable based on design. It was possible to identify for the 4 Simulation Exercises the minimum use requirements for the components and contributory tools within the 4 Simualtion Exercises.
5		P-05	Identification of useful S4RIS contributory tool combinations	Essential	-	x	x	-	-	-		x			Assessable based on design. Partially identified for SEs during the project.
6		P-06	Data exchange – end user sources to S4RIS	Essential	-	x	x	-	-	-		x			Assessable based on design. The real-time monitoring tools (e.g. CuriX, WINGSPARK, (SC2/Ganimede)) provide means to observe current values of measured data of physical and cyber sensors.
7		P-07	Data exchange – S4RIS to end-users	Essential	-	-	-	-	-	-		x			Assessable based on design. In principle possible via the Distributed Messaging System (DMS) with publish/subscribe. In addition, some of the real-time monitoring tools (e.g. CuriX) provide means to feedback data to existing end-user systems, e.g. Splunk, Elastic or PRTG via given REST APIs.
8		P-08	Data exchange – Between S4RIS tools	Essential	-	-	-	x	-	-		x			Assessable based on design. Possible via the Distributed Messaging System (DMS) with publish/subscribe. Not tested for all tools.
9		P-09	Synchronisation	Essential	-	-	-	x	-	-		x			Assessable based on design. In principle possible via the Distributed Messaging System (DMS) with publish/subscribe.
10		P-10	Input quality check	Essential	x	x	x	-	x	-		x			Assessable based on design e.g. warning/error messages from individual tools.
11		P-11	Self-diagnostics	Essential	-	-	-	-	-	-			x		Not possible to indentify implementation of this requirement and connected specification in development to date.
12		P-12	Archive	Essential	-	-	-	x	-	-		x			Assessable based on design. In principle possible via the Distributed Messaging System (DMS) for pre-determined lengths of time for messages communicated via DMS. Archiving of processing in contributory tools depends on the individual contributory tools.
13		P-13	Data integrity	Essential	-	x	-	-	-	-		x			Assessable based on design. D1.4 identified the Blockchain solution as a method towards achieving this requirments and connected specification.
14		P-14	Data authenticity	Essential	-	x	-	-	-	-		x			Assessable based on design. D1.4 identified the Blockchain solution as a method towards achieving this requirments and connected specification. The PRIGM/Senstation combination offer a further method.
15		P-15	Manual	Essential	x	x	x	-	x	-		x			Assessable based on observation. The S4RIS GUI and individual contributory tools providing varying degress of manuals and/or on-line help.
16		P-16	Skill / training	Essential	-	-	-	-		-				x	Assessable based on observation. Following the D1.4, there was not the expectation to address / achieve this requirement within the project duration.

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	T6.4	A	P	NA	NK	
17		P-17	Security	Essential	-	-	-	-	-	-		x			Assessable based on design and observation. Following the D1.4, there was not the expectation to address / achieve this requirement fully within the project duration. The security requirements fof the Simulation Exercises were fulfilled.
18		P-18	Public accessibility	Optional	-	-	-	-	-	-		x			Assessable based on design and observation. The basic S4RIS GUI access page is available but there is no detailed information available publicly to date.
19		P-19	Global unique identification of entities	Essential	-	-	-	x	-	-		x			Assessable based on design and observation. Partially achieved for the specific Simulation Exercises where there was communication via the DMS.
20		P-20	Messaging System	Essential	-	-	-	x	-	-	x				Assessable based on design and observation. DMS implemented for multiple tools (but not all).
21		IO-1 (P-08 above)	Data exchange – Between S4RIS tools	Essential	-	-	-	x	-	-	x				See P-08 above.
22		IO-2 (P-09 above)	Synchronisation	Essential	-	-	-	x	-	-		x			See P-09 above.
23		P-21 (IO-3 in D2.3)	Data exchange with end-users' system	Essential	-	-	-	-	-	-		x			See P-07 above.
24		P-22 (IO-4 in D2.3)	Data exchange – Upload already existing data in the S4RIS	Essential	-	-	-	-	-	-		x			Assessable based on design. Achieved through upload to individual contributory tools as relevant
25		P-23 (IO-5 in D2.3)	Data exchange format for the S4RIS	Essential	-	-	-	-	-	-		x			Assessable based on design and observation. Provided thorugh DMS solution and JSON formats agreed for individual Ses
26		P-24 (IO-6 in D2.3)	The S4RIS shall provide a possibility to connect to not specified systems	Essential	-	-	-	-	-	-		x			Assessable based on design and observation. Provided through DMS solution and JSON formats agreed for individual SEs
27	Knowledge / Usability	EU+U01	Usability	Essential	-	-	-	-	-	-		x			As for P-15
28	Graphical User Interface - GUI	GUI-R01	Web-based interface	Essential	-	-	-	x	-	x	x				Achieved for S4RIS GUI (but not for all contributory tools)
29		GUI-R02	Login page	Essential	-	-	-	x	-	x	x				
30		GUI-R03	Single point of access to the tools	Essential	-	-	-	x	-	x		x			Assessable based on design and observation. This functionality has been delivered and demonstrated in the S4RIS GUI for those tools with their own GUI in a web application and the epossibility to download .exe programmes has been demonstrated.
31		GUI-R04	Grouping of tools	Essential	-	-	-	-	-	x		x			Demonstrated for tools used in SEs.
32		GUI-R05	How to launch tools	Essential	-	-	-	-	-	x		x			
33		GUI-R06	Display of tools based on user role	Essential	-	-	-	-	-	x	x				Based on UNEW reported test.
34		GUI-R07	Tools keywords and short descriptions	Essential	-	-	-	-	-	x		x			
35		GUI-R08	Log-out button	Essential	-	-	-	x	-	x		x			Achieved according to UNEW test reports but not visible in actual S4RIS GUI at time of writing (13/09/2022)
36		GUI-R09	Home page button	Essential	-	-	-	x	-	x	x				
37		GUI-R10	Account management	Essential	-	-	-	-	-	x	x				

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	**T6.4**	A	P	NA	NK	
38		GUI-R11	Settings and configuration	Essential	-	-	-	-	-	x		x			As it stands the end-user does not see the settings page.
39		GUI-R12	Language	Essential	-	-	-	-	-	x		x			S4RIS GUI in english. Technically possible to offer further languages. Compared to D1.4 comments on requirement: not each individual tool demonstrated for at least two
40		GUI-R13	Bar with additional functions	Conditional	-	-	-	-	-	x		x			Test demonstrated possibility to access tools grouped under a specific heading e.g. a Simulation exercise location. Full specification not tested.
41		GUI-R14	Opening web-based tools	Essential	-	-	-	-	-	x	x				Demonstrated for tools with web application.
42		GUI-R15	Opening desktop tools	Essential	-	-	-	-	-	x	x				Based of UNEW reported test.
43		GUI-R16	Opening CLI tools	Conditional	-	-	-	-	-	-			x		Not possible to indentify implementation of this requirement and connected specification in development to date.
44		GUI-R16a	Opening CLI tools - BB3d	Conditional	-	-	-	-	-	-			x		Not possible to indentify implementation of this requirement and connected specification in development to date.
45		GUI-R16b	Opening CLI tools - CaESAR	Conditional	-	-	-	-	-	-			x		No longer relevant as CaESAR delivered a web application GUI
46		GUI-R16c	Opening CLI tools - SARA	Conditional	-	-	-	-	-	-			x		Not possible to indentify implementation of this requirement and connected specification in development to date.
47		GUI-R17	User confirmation on certain actions	Essential	-	-	-	-	-	-			x		Not possible to indentify implementation of this requirement and connected specification in development to date.
48		GUI-R18	Font type and size	Conditional	-	-	-	-	-	-		x			Visible in actual S4RIS GUI at time of writing (13/09/2022)
49		GUI-R19	Error display -	Essential	-	-	-	-	-	-			x		Not possible to indentify implementation of this requirement and connected specification in development to date.
50		GUI-R20	S4RIS account creation	Optional	-	-	-	-	-	-	x				Visible in actual S4RIS GUI at time of writing (13/09/2022)
51		GUI-R21	Help and documentation	Conditional	-	-	-	-	-	-		x			See P-15
52		GUI-R22	Frequently/recently used tools	Optional	-	-	-	-	-	-			x		
53		GUI-R23	Dashboard	Conditional	-	-	-	-	-	-		x			Assessable based on design and observation.
54		GUI-R24	Mobile interface	Conditional	-	-	-	-	-	-		x			Assessable based on design and observation.
55		GUI-25	S4RIS public accessible part optimized for mobile devices	Condtional	-	-	-	-	-	-		x			Assessable based on design and observation. The basic S4RIS GUI access page is available but there is no detailed information available publicly to date.
56	Standards	STD-R01	Human user identification and authentication	Essential	-	-	-	-	-	-					Not evaluated under T6.4
57		STD-R02	Human user identification and authentication - multifactor for remote connection	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
58		STD-R03	Human user identification and authentication - multifactor	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
59		STD-R04	Non-human user identification and authentication	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
60		STD-R05	Account management	Essential	-	-	-	-	-	-					Not evaluated under T6.4

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	T6.4	A	P	NA	NK	
61		STD-R06	User account uniqueness	Essential	-	-	-	-	-	-					Not evaluated under T6.4
62		STD-R07	Secure log-on	Essential	-	-	-	-	-	-					Not evaluated under T6.4
63		STD-R08	Secure log-on feature 1	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
64		STD-R09	Secure log-on feature 2	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
65		STD-R10	Secure log-on feature 3	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
66		STD-R11	Secure log-on feature 4	Essential	-	-	-	-	-	-					Not evaluated under T6.4
67		STD-R12	Secure log-on feature 5	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
68		STD-R13	Secure log-on feature 6	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
69		STD-R14	Secure log-on feature 7	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
70		STD-R15	Secure log-on feature 8	Essential	-	-	-	-	-	-					Not evaluated under T6.4
71		STD-R16	Password management	Essential	-	-	-	-	-	-					Not evaluated under T6.4
72		STD-R17	Password management feature 1	Essential	-	-	-	-	-	-					Not evaluated under T6.4
73		STD-R18	Password management feature 2	Essential / Conditional	-	-	-	-	-	-					Not evaluated under T6.4
74		STD-R19	Password management feature 3	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
75		STD-R20	Password management feature 4	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
76		STD-R21	Public Key Infrastructure	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
77		STD-R22	Public Key authentication	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
78		STD-R23	Monitoring of access from untrusted networks	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
79		STD-R24	User access provisioning	Essential	-	-	-	-	-	-					Not evaluated under T6.4
80		STD-R25	Information access restriction	Essential	-	-	-	-	-	-					Not evaluated under T6.4
81		STD-R26	Identification and monitoring of access through wireless connection	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
82		STD-R27	Session lock	Essential	-	-	-	-	-	-					Not evaluated under T6.4
83		STD-R28	Termination of remote sessions	Essential	-	-	-	-	-	-					Not evaluated under T6.4

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	T6.4	A	P	NA	NK	
84		STD-R29	Limit of contemporary sessions	Essential	-	-	-	-	-	-					Not evaluated under T6.4
85		STD-R30	Audit of events related to security	Essential	-	-	-	-	-	-					Not evaluated under T6.4
86		STD-R31	Audit storage	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
87		STD-R32	Alerting of audit process fail	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
88		STD-R33	Timestamp for audit	Essential	-	-	-	-	-	-					Not evaluated under T6.4
89		STD-R34	Non-repudiation of users	Essential	-	-	-	-	-	-					Not evaluated under T6.4
90		STD-R35	Access to audit information	Essential	-	-	-	-	-	-					Not evaluated under T6.4
91		STD-R36	Information classification	Essential / Conditional	-	-	-	-	-	-					Not evaluated under T6.4
92		STD-R37	Information classification scheme	Essential / Conditional	-	-	-	-	-	-					Not evaluated under T6.4
93		STD-R38	Information labelling	Essential / Conditional	-	-	-	-	-	-					Not evaluated under T6.4
94		STD-R39	Information labelling scheme	Essential / Conditional	-	-	-	-	-	-					Not evaluated under T6.4
95		STD-R40	Protection of communications	Essential	-	-	-	-	-	-					Not evaluated under T6.4
96		STD-R41	Dealing with errors in a secure way	Essential	-	-	-	-	-	-					Not evaluated under T6.4
97		STD-R42	Information backup	Essential	-	-	-	-	-	-					Not evaluated under T6.4
98		STD-R43	Recovery and restore	Essential	-	-	-	-	-	-					Not evaluated under T6.4
99		STD-R44	Inventory of assets	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
100		STD-R45	Source code protection	Essential	-	-	-	-	-	-					Not evaluated under T6.4
101		STD-R46	Infrastructure monitoring	Essential	-	-	-	-	-	-					Not evaluated under T6.4
102		STD-R47	Integration of a security incident tracking system form	Essential	-	-	-	-	-	-					Not evaluated under T6.4
103		STD-R48	Overall security event / incident / vulnerability database	Essential	-	-	-	-	-	-					Not evaluated under T6.4
104		STD-R49	Automatic correlation of different incidents detected	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
105		STD-R50	Security incident management system governance	Essential	-	-	-	-	-	-					Not evaluated under T6.4
106		STD-R51	Attributes relevant for security incident management	Essential	-	-	-	-	-	-					Not evaluated under T6.4

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	T6.4	A	P	NA	NK	
107		STD-R52	Collection of evidence before shutdown.	Essential	-	-	-	-	-	-					Not evaluated under T6.4
108		STD-R53	Guidelines to inform who is responsible for internal and external communications	Essential	-	-	-	-	-	-					Not evaluated under T6.4
109		STD-R54	Video Coding and metadata representation	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
110		STD-R55	Alerting protocol for emergencies	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
111	Data Protection	GDPR-R01	GDPR Compliance	Essential	-	-	-	-	-	-					Not evaluated under T6.4
112	Open source intelligence technologies for the S4RIS	OSINT_1	Data acquisition of OSINT	Essential	-	x	-	-	-	-					Not evaluated under T6.4
113		OSINT_2	Pre-Processing and Analytics	Essential	-	x	-	-	-	-					Not evaluated under T6.4
114		OSINT_3	Storage and representation	Essential	-	x	-	-	-	-					Not evaluated under T6.4
115		OSINT_4	Data set analytics	Conditional	-	x	-	-	-	-					Not evaluated under T6.4
116		OSINT_5	Data access and messaging	Essential	-	x	-	-	-	-					Not evaluated under T6.4
117	Blockchain technology	Blockchain_01	Technological requirements for the blockchain	Essential	-	x	-	-	-	-					Not evaluated under T6.4
118		Blockchain_02	Data ingestion	Essential	-	x	-	-	-	-					Not evaluated under T6.4
119		Blockchain_03	Data analytics	Optional	-	x	-	-	-	-					Not evaluated under T6.4
120		Blockchain_04	Data access	Essential	-	x	-	-	-	-					Not evaluated under T6.4
121	Railways in the Smart City	UR-SM-1	Enhanced coordination of the transport services available in the city	Essential	-	-	-	-	-	-					Not evaluated under T6.4
122		UR-SM-2	Adequate coordinated crisis management and support structures	Essential	-	-	-	-	-	-					Not evaluated under T6.4
123		UR-SM-3	Joint risk and threat assessment in transport hub.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
124		UR-SM-4	Early warning procedures between stakeholders of the transport hub to inform about incidents before they have exceeded the threshold for serious security/safety incidents or even crises.	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
125		UR-SM-5	Signalisation in hub with several transportations modes and levels for pas-sengers both under normal circumstances and during a crisis is key ele-ment in the overall system.	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
126		UR-SM-6	Cooperation between security providers in a hub.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
127		UR-SM-7	Fostering communication/reporting about delays/ irregularities and common/coordinated reactions between different stakeholders of a common transport hub.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
128		UR-SM-8	Direct and immediate security/safety incident reporting between different stakeholders of a common transport hub including stakeholders of different countries (multilingual) who operate at a common transport hub (trains, touring coaches).	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
129		UR-SM-9	Provision of predictive information for joint crisis management with various stakeholders	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
130		UR-SM-10	Reliable communication means used by stakeholders.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	T6.4	A	P	NA	NK	
131	Crisis Management	UR-CM-R01	Adequate crisis management and support structures.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
132		UR-CM-R02	Cooperation between stakeholders.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
133		UR-CM-R03	Clear definition of role and responsibilities.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
134		UR-CM-R04	Expert knowledge - a prerequisite for being able to assess both physical and cyber incidents - both with reference to rail traffic.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
135		UR-CM-R05	Training and exercises.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
136		UR-CM-R06	Blast wave impact in case of an explosion.	*not specified*	-	-	-	-	-	-					See BB3d requirements/specifications below.
137		UR-CM-R07	Crowd simulation in case of an incident.	*not specified*	-	-	-	-	-	-					See iCrowd requirements/specifications below.
138		UR-CM-R08	Cascade effect simulation.	*not specified*	-	-	-	-	-	-					See CaESAR requirements/specifications below.
139		UR-CM-R09	Early warning systems to alarm in case of forecast problematic weather conditions to be implemented in all prevention tools.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
140		UR-CM-R10	Threat Intelligence.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
141		UR-CM-R11	Detection of abnormal situation/anomalies regarding sensors, IT systems, assets, behaviour, forbidden objects, suspicious items, etc.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
142		UR-CM-R12	Detection of combined attacks.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
143		UR-CM-R13	Standardised and simplified exchange of information between the Central IT Body for Incident Management/IT SPOC and the Central Security Body.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
144		UR-CM-R14	Harmonised reporting tool for exchanging information.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
145		UR-CM-R15	Ensure that the same degree of concern (slight - medium - severe) is understood by both sides, the Central IT Body and the Central Security Body.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
146		UR-CM-R16	The moment (threshold) must be determined as to what and to whom an incident is reported - and by what communication means.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
147		UR-CM-R17	The threshold must be specified at which the Central IT Body or the Operation Centres report to the Central Security Body.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
148		UR-CM-R18	The reporting from the Central IT Body or the Operation Centres.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
149		UR-CM-R19	Information on the situation to be given to the company staff.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
150		UR-CM-R20	Ensures the standardised and simplified.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
151		UR-CM-R21	Reliable communication and early warning.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
152		UR-CM-R22	Mutual early warning system for the operators of different means of transport.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
153		UR-CM-R23	Mutual early warning system for the operators of different means of transport.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
154		UR-CM-R24	Cross-border exchange with the use of different languages must be considered.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
155		UR-CM-R25	Situational awareness.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
156		UR-CM-R26	Impact and cascading effect simulation.	*not specified*	-	-	-	-	-	-					See CaESAR requirements/specifications below.
157		UR-CM-R27	Crowd management.	*not specified*	-	-	-	-	-	-					See iCrowd requirements/specifications below.

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	T6.4	A	P	NA	NK	
158		UR-CM-R28	Resumption of all operations of the multimodal transport system – complying with mutual interdependencies.	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
159		UR-CM-R29	Evaluation and explanation of common "lessons learned“ to be implemented in the next prediction/prevention phase..	*not specified*	-	-	-	-	-	-					Not evaluated under T6.4
160		UR-CM-R30	Security Risk Assessment Index	Essential	-	-	-	-	-	-					Not evaluated under T6.4
161	Communication with the public	UR-CC-R01	Coordinate with relevant stakeholders.	Essential	-	-	-	-	-	-					Not evaluated under T6.4
162		UR-CC-R02	Create a crisis communication plan.	Essential	-	-	-	-	-	-					Not evaluated under T6.4
163		UR-CC-R03	Communicate about preparedness actions to take when facing potential risks	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
164		UR-CC-R04	Provide timely information.	Essential	-	-	-	-	-	-					Not evaluated under T6.4
165		UR-CC-R05	Provide upstream communication in transportation hub	Optional	-	-	-	-	-	-					Not evaluated under T6.4
166		UR-CC-R06	Continue to update about the situation.	Conditional	-	-	-	-	-	-					Not evaluated under T6.4
167		UR-CC-R07	Specific communication to regain passengers´ confidence for the multimodal approach.	Essential	-	-	-	-	-	-					Not evaluated under T6.4
168		UR-CC-R08	Apply lessons learned.	Essential	-	-	-	-	-	-					Not evaluated under T6.4
169	Costs	C01	Cost benefit balance	Essential	-	-	-	-	-	-					Not evaluated under T6.4
170	BB3d (RINA-C)	BB3d_01	Bomb blast loading	Essential	x	x	x	-	-	x	x				Main contributions in D3.4,D4.5, D5.5
171	BB3d (RINA-C)	BB3d_02	Bomb blast usability	Essential	-	-	x	-	-	x	x				Main contributions in D5.5 in §2.1 and 2.3
172	BB3d (RINA-C)	BB3d_03	Bomb blast damage and casualties	Essential	x	x	x	-	-	x	x				Main contributions in D3.4 (confidential data are not provided because of it is a public deliverable),D4.5, D5.5
173	BB3d (RINA-C)	BB3d_04	Bomb blast computing performance	Essential	-	-	x	-	-	x	x				Main contributi in D5.5 in §2.2
174	BB3d (RINA-C)	BB3d_05	Bomb blast tool integration	Essential	x	-	x	-	-	-		x			Main conrtributions in D3.4 (connection with SecuRail), D5.5 in §5 , D5.2 (connection with iCrowd), D5.7
175	BB3d (RINA-C)	BB3d_06	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				UNEW considered the efforts to create and integrate the BB3d GUI too demanding considering the budget and time available. Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
176	CaESAR (Fraunhofer)	CaESAR_01	CaESAR should estimate how disruptive events impact the infrastruc-ture, its components and their functionalities.	Essential	-	-	x	-	-	x		x			
177	CaESAR (Fraunhofer)	CaESAR_02	CaESAR should identify weak points in the railway/metro system	Essential	-	-	x	-	-	x	x				
178	CaESAR (Fraunhofer)	CaESAR_03	CaESAR should estimate the propagation of a failure caused by disruptive events to/from interdependent infrastructures,	Essential	-	-	x	-	-	x		x			
179	CaESAR (Fraunhofer)	CaESAR_04	CaESAR should apply several strategies to recover from disruptive events and evaluate their impact on the	Conditional	-	-	x	-	-	x	x				
180	CaESAR (Fraunhofer)	CaESAR_05	Implementation and evaluation of mitigation measures	Essential	-	-	x	-	-	x	x				

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	**T6.4**	**A**	**P**	**NA**	**NK**	
181	CaESAR (Fraunhofer)	CaESAR_06	CaESAR should be able to handle the following different types of at-tacks	Essential	-	-	x	-	-	x	x				
182	CaESAR (Fraunhofer)	CaESAR_07	Implementation of What-If-Scenarios and varying disruptive event at-tributes	Essential	-	-	x	-	-	x	x				
183	CaESAR (Fraunhofer)	CaESAR_08	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	x	x	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
184	CAMS (RMIT)	CAMS_01	Prediction of normal deterioration due to aging and degradation of as-sets	Essential	-	-	-	-	-	x	x				Achieved through project developmental validation and evaluation. Items provided: Asset degradation curves due to ageing; Cost of maintenance, repair, renew.
185	CAMS (RMIT)	CAMS_02	Maintenance and repair budget calculation	Essential	-	-	-	-	-	x	x				Achieved through project developmental validation and evaluation. Items provided: Capital value of the elements; Cost of asset maintenance under normal degradation; time allocated for maintenance of the element; Cost of asset repair under normal degradation and hazard event.
186	CAMS (RMIT)	CAMS_03	State-dependent fragility analysis	Essential	-	-	-	-	-	x	x				Achieved through project developmental validation and evaluation. Items provided: Asset fragility.
187	CAMS (RMIT)	CAMS_04	Resilience module	Essential	-	-	-	-	-	x	x				Achieved through project developmental validation and evaluation. Items provided: Resilience index .
188	CAMS (RMIT)	CAMS_05	Risk / Cost Evaluation	Essential	-	-	-	-	-	-		x			Partially acquired from project simulation exercises. (Based on WP8- stated predominantly in D7.5)
189	CAMS (RMIT)	CAMS_06	Backlog estimation	Essential	-	-	-	-	-	-		x			Partially acquired from project simulation exercises. (Based on WP8- stated predominantly in D7.1)
190	CAMS (RMIT)	CAMS_07	Optimization of budget	Essential	-	-	-	-	-	-		x			Partially acquired from project simulation exercises. (Based on WP8- stated predominantly in D7.5)
191	CAMS (RMIT)	CAMS_08	Extension of the framework to IT assets	Conditional	-	-	-	-	-	-		x			Partially acquired from project simulation exercises. (Based on WP8- stated predominantly in D7.1)
192	CAMS (RMIT)	CAMS_09	Analysis of compromise between maintenance, repair, rehabilitation and resilience enhancement efforts	Essential	-	-	-	-	-	-	x				Achieved through project developmental validation and evaluation. Items provided: System components (physical and cyber) and their quantity; Two
193	CAMS (RMIT)	CAMS_10	Assessment of recovery	Conditional	-	-	-	-	-	-	x				Achieved through project developmental validation and evaluation. Items provided: Cost and time of asset rehabilitation under normal degradation and/or hazard event.
194	CAMS (RMIT)	CAMS_11	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
195	CuriX (CuriX)	CuriX_01	Anomaly detection (univariate and multivariate)	Essential	-	x	-	-	-	x	x				
196	CuriX (CuriX)	CuriX_02	Catalogue-Based Outage Prevention	Essential	-	x	-	-	-	x	x				The test did not cover the full requirement. While the test passed, the requirement is only parially achieved.
197	CuriX (CuriX)	CuriX_03	Infrastructure Monitoring (including cyber threats)	Essential	-	x	-	-	-	x	x				
198	CuriX (CuriX)	CuriX_04	CuriX User-Friendly Dashboard	Essential	-	-	-	-	-	x	x				

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	T6.4	A	P	NA	NK	
199	CuriX (CuriX)	CuriX_05	System resource optimization for the Railway infrastructure	Conditional	-	-	-	-	-	-				x	This requirement was not addressed within SAFETY4RAILS
200	CuriX (CuriX)	CuriX_06	CuriX Dashboard to be provided multilingual	Conditional	-	-	-	-	-	-				x	This requirement was not addressed within SAFETY4RAILS
201	CuriX (CuriX)	CuriX_07	CuriX integration (connectors) to S4RIS and interfaces to other tools	Essential	-	x	-	-	-	x	x				
202	CuriX (CuriX)	CuriX_08	Hardening anomaly detection against data interruptions	Optional	-	x	-	-	-	x	x				
203	CuriX (CuriX)	CuriX_09	System intelligence and visualisation.	Optional	-	-	-	-	-	-				x	This requirement was not addressed within SAFETY4RAILS.
204	CuriX (CuriX)	CuriX_10	How to use CuriX (configuration and dashboard)	Conditional	-	-	-	-	-	-				x	This requirement was not addressed within SAFETY4RAILS.
205	CuriX (CuriX)	CuriX_11	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				Connected to DMS, integrated in GUI and demonstrated. Evaluated as achieved based on D1.4 specfciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
206	DATA FAN (Fraunhofer)	DATA FAN-1	Reliable and understandable machine learning (ML)-based results	Essential	-	x	-	-	-	x	x				
207	DATA FAN (Fraunhofer)	DATA FAN-2	High prediction performance of results, e.g. anomaly detection	Essential	-	x	-	-	-	x	x				
208	DATA FAN (Fraunhofer)	DATA FAN-3	Software application with a user-friendly interface	Essential	-	-	-	x	-	x	x				
209	DATA FAN (Fraunhofer)	DATA FAN-4	How to use the software	Essential	-	-	-	x	-	x	x				
210	DATA FAN (Fraunhofer)	DATA FAN-5	Moderate hardware requirements for using the software	Essential	-	-	-	x	-	x	x				
211	DATA FAN (Fraunhofer)	DATA FAN-6	Webservice for computation of expensive ML-algorithms	Essential	-	-	-	-	-	-			x		
212	DATA FAN (Fraunhofer)	DATA FAN-7	Manner of the applied anomaly detection	Essential	-	x	-	-	-	x	x				
213	DATA FAN (Fraunhofer)	DATA FAN-8	Requirements for the used data	Essential	-	-	-	-	-	-			x		
214	DATA FAN (Fraunhofer)	DATA FAN-9	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				Evaluated as achieved based on D1.4 specfciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
215	Ganimede (LDO)	Ganimede_1	Audio pattern detection	Essential	-	-	-	-	-	x	x				
216	Ganimede (LDO)	Ganimede_2	Enhanced abandoned baggage detection	Essential	-	-	-	-	-	x	x				
217	Ganimede (LDO)	Ganimede_3	People re-identification	Conditional	-	-	-	-	-	x	x				
218	Ganimede (LDO)	Ganimede_4	Man down	Essential	-	-	-	-	-	x	x				
219	Ganimede (LDO)	Ganimede_5	Event visualization	Essential	-	-	-	-	-	-		x			Events visualized through SC2

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	**T6.4**	A	P	NA	NK	
220	Ganimede (LDO)	Ganimede_6	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
221	iCrowd (NCSRD)	iCrowd_01	Simulate realistic crowd congestion levels	Essential	-	-	-	-	-	x	x				
222	iCrowd (NCSRD)	iCrowd_02	Simulate an evacuation because of terrorism (bomb, gas release) or natural disaster (fire/flood)	Essential	-	-	-	-	-	x	x				
223	iCrowd (NCSRD)	iCrowd_03	Simulate crowd behaviour considering cyber agents (electronic boards)	Conditional	-	-	-	-	-	x		x			Implemented but not tested
224	iCrowd (NCSRD)	iCrowd_04	Detect blind-spots because of guards' movements and insufficient cameras	Optional	-	-	-	-	-	x	x				
225	iCrowd (NCSRD)	iCrowd_05	Simulate access to a restricted area by cyber-attack (hackage of door) or physical attack (disabling a guard)	Optional	-	-	-	-	-	x	x				
226	iCrowd (NCSRD)	ICrowd_06	Guards' distraction simulation	Optional	-	-	-	-	-	x		x			Implemented but not tested
227	iCrowd (NCSRD)	iCrowd_07	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
228	PRIGM (ERARGE)	PRIGM_01	PRIGM must have hardware encryption and random number generator modules	Essential	-	-	x	x	-	x		x			Description of data used in NIST-800-22 True Randomness Test Suite: type(s): file with binary stream
229	PRIGM (ERARGE)	PRIGM_02	PRIGM must have a standardised API to connect to a Computer	Essential	-	-	-	x	-	x	x				
230	PRIGM (ERARGE)	PRIGM_03	PRIGM should be connected to the end user's central control unit	Essential	-	-	-	x	-	x	x				Description of data used in ned-to-end communication with a generic central control unit:
231	PRIGM (ERARGE)	PRIGM_04	PRIGM should give service for end nodes and create outputs for end-users	Essential	-	-	-	x	-	x	x				
232	PRIGM (ERARGE)	PRIGM_05	PRIGM should work as a utility for the management of certification and IoT device authentication	Conditional	-		x	-	-	x	x				
233	PRIGM (ERARGE)	PRIGM_06	PRIGM operations must be GDPR compliant	Essential	-	x	-	-	-	x	x				
234	PRIGM (ERARGE)	PRIGM_07	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
235	RAM^2 (ELBIT)	RAM2_01	RAM2 should provide risk assessment and prioritization	Essential	x	-	-	x	-	x	x				
236	RAM^2 (ELBIT)	RAM2_02	RAM2 should generate correlated insights	Essential	-	x	-	x	-	x	x				
237	RAM^2 (ELBIT)	RAM2_03	RAM2 should provide alert and insight mitigation steps	Essential	x	x	-	x	-	x	x				
238	RAM^2 (ELBIT)	RAM2_04	RAM2 should provide an operational hierarchy context	Essential	-	x	-	x	-	x		x			Assets lists were not provided in order to develop operational hierarchy
239	RAM^2 (ELBIT)	RAM2_05	RAM2 Dashboard	Essential	-	-	x	-	-	x	x				

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	**T6.4**	**A**	**P**	**NA**	**NK**	
240	RAM^2 (ELBIT)	RAM2_06	RAM2 integration for input data and export to additional systems	Essential	-	x	-	x	-	x	x				
241	RAM^2 (ELBIT)	RAM2_07	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	x	x	-	x	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
242	SARA (RINA-C)	SARA-1	SARA - Securestation Attack Resilience Assessment	Essential / Conditional	-	-	-	-	-	x	x				From D1.4: Essential – xlm file as input; Conditional – png/svg file as output.
243	SARA (RINA-C)	SARA-2	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	-	-					x	
244	SecaaS (ICOM)	SecaaS_01	Monitoring of network traffic for signs of abnormality	Conditional	-	-	-	-	-	x	x				
245	SecaaS (ICOM)	SecaaS _02	Interfaces to comply with S4Rails WEB service methodology	Essential	-	-	-	-	-	-		x			
246	SecaaS (ICOM)	SecaaS_03	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-				x	
247	SecuRail (STAM)	SECURAIL_1	Creation of libraries of the Railway environment to create and model the railway infrastructure to be analysed with the tool	Essential	x	-	-	-	-	x	x				
248	SecuRail (STAM)	SECURAIL_2	Localization on the Map	Conditional	x	-	-	-	-	x	x				
249	SecuRail (STAM)	SECURAIL_3	Computation of Risk	Essential	x	-	-	-	-	x	x				
250	SecuRail (STAM)	SECURAIL_4	Real time automatic risk assessment	Conditional	x	-	-	-	-	x		x			
251	SecuRail (STAM)	SECURAIL_5	Multilinguality	Optional	x	-	-	-	-	x	x				
252	SecuRail (STAM)	SECURAIL_6	Cost-Benefit Analysis	Conditional	x	-	-	-	-	-		x			
253	SecuRail (STAM)	SECURAIL_7	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
254	Senstation (ERARGE)	SENSTATION_01	Interfaces of Senstation should be compatible with the interfaces of sensors and the data network of the end-user	Essential	-	-	-	x	-	-	x				Compliance with common criteria EAL 4+ specifications achieved.
255	Senstation (ERARGE)	SENSTATION_02	The resilience of the alternative secure data channel must be improved by end-to-end and hardware-based security.	Essential	-	x	x	-	-	-	x				
256	Senstation (ERARGE)	SENSTATION_03	Senstation must encrypt sensory data on the communication channel	Essential	-		x	-	-	-	x				
257	Senstation (ERARGE)	SENSTATION_04	Temperature, smoke, acceleration and velocity sensors should be collected through the Senstation tool and used for anomaly	Conditional	-	-	-	-	-	-		x			Discrepancy: new data for wind speed and water level at vents added. Description of data used in Secure end-to-end IoT data transmission:
258	Senstation (ERARGE)	SENSTATION_05	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	-	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
259	SISC2 (ICOM)	SISC2_01	Software integration platform for surveillance, collaboration, coordina-tion and administration of security and operations	Conditional	-	-	-	-	-	x	x				

ID	Status
x	Tested
-	Not tested

ID	Evaluation (✔)
A	Achieved
P	Partially achieved
NA	Not achieved
NK	Not known to date

					TEST CONTENT						EVALUATION				COMMENT
No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	*WP3*	*WP4*	*WP5*	*T6.2 / T6.3*	*WP7*	T6.4	A	P	NA	NK	
260	SISC2 (ICOM)	SISC2_02	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-				x	
261	TISAIL (TREE)	TISAIL_1	Detection of cyber-threats related to the railway sector: Malware	Essential	-	-	-	-	-	x	x				
262	TISAIL (TREE)	TISAIL_2	Detection of cyber-threats related to the railway sector: Internet-Exposed Assets and credential leaks	Essential	-	-	-	-	-	x	x				
263	TISAIL (TREE)	TISAIL_3	Detection of cyber-threats related to the railway sector: Threat Intel feeds and Social Media	Optional	-	-	-	-	-	x	x				
264	TISAIL (TREE)	TISAIL_4	Detection of cyber-threats related to the railway sector: Vulnerabilities	Essential	-	-	-	-	-	x	x				
265	TISAIL (TREE)	TISAIL_5	Detection of cyber-threats related to the railway sector: Spear Phishing	Optional	-	-	-	-	-	x	x				
266	TISAIL (TREE)	TISAIL_6	Integrate alerts related to cyber-threats in the railway sector with a MISP repository	Essential	-	-	-	-	-	x	x				
267	TISAIL (TREE)	TISAIL_7	Use a Railway Threat Taxonomy on TISAIL	Optional	x	-	-	-	-	-		x			
268	TISAIL (TREE)	TISAIL_8	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."
269	uni|MS^{TM} (ICOM)	UNIMS_01	Unified management for networks, infrastructure and systems	Conditional	-	-	-	-	-	x	x				
270	uni|MS^{TM} (ICOM)	UNIMS_02	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-				x	
271	WIBAS (ICOM)	WiBAS_01	Advanced Wireless Broadband Access for Enterprise Users	Conditional	-	-	-	-	-	x		x			
272	WIBAS (ICOM)	WiBAS_02	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-				x	
273	WINGSPARK (WINGS)	WINGS_01	Data ingestion from devices	Essential	-	-	-	-	-	x	x				
274	WINGSPARK (WINGS)	WINGS_02	Data Management/Analysis	Essential	-	-	-	-	-	x	x				
275	WINGSPARK (WINGS)	WINGS_03	Support of A.I. techniques	Essential	-	-	-	-	-	x	x				
276	WINGSPARK (WINGS)	WINGS_04	User-friendly GUI	Essential	-	-	-	-	-	x	x				
277	WINGSPARK (WINGS)	WINGS_05	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	-	-	-	x	-	-	x				Evaluated as achieved based on D1.4 specifciation: "No development should be carried out in SAFEYT4RAILS which would negate the possibility or even make it extremely hard to fulfil 1 or more of the requirements determined as essential for the S4RIS product(s)."

SAFETY4RAILS

Partners:

Fraunhofer EMI
UIC
Metro
Metro de Madrid
EGO
EGO Genel Müdürlüğü
RFI
RETE FERROVIARIA ITALIANA
GRUPPO FERROVIE DELLO STATO ITALIANE

LEONARDO
ceis
avisa partners
STAM
MASTERING EXCELLENCE
TCDD

IC 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

IN Innova Integra
LAU REA
AMMATTIKORKEAKOULU
University of Applied Sciences
CyberServices
MADE IN EUROPE
FGC
Ferrocarrils
de la Generalitat
de Catalunya
erarGE

MTRS
INTRACOM
TELECOM
UNIVERSITAS
Miguel Hernández

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.