SAFETY4RAILS

Final version of evaluation report

Deliverable 8.5

Lead Author: LAU

Contributors: ETRA, UIC, Fraunhofer, MdM, CdM, RFI, EGO, UNEW

Dissemination level: PU - Public

Security Assessment Control: passed

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

D8.5 Final version of evaluation report	
Deliverable number:	8.5
Version:	1.2
Delivery date:	21/03/2023
Dissemination level:	PU - Public
Nature:	Report
Main author(s)	LAU
Contributor(s) to main deliverable production	ETRA UIC LDO Fraunhofer MDM CDM RFI EGO UNEW RMIT
Internal reviewer(s)	Fraunhofer MdM CdM RFI MTRS CS
External reviewer(s)	UIC (individual not directly involved in project)

Document control			
Version	Date	Author(s)	Change(s)
0.1	05.05.2022	LAU	Draft structure.
0.2	17.05.2022	LAU	ToC for review
0.3	22.06.2022	LAU	Deliverable structure according to review comments
0.4	29.06.2022	LAU	First initial draft for consortium review
0.5	19.07.2022	LAU	Version for consortium and formal review
0.6	27.07.2022	LAU	Updated version according to review feedback
0.71	29.08.2022	LAU	Updated according to coordinator and UIC feedback
0.72	09.09.2022	LAU	Updated according to PC feedback
0.73	09.09.2022	LAU	Updated according to internal review feedback
0.8	16.09.2022	LAU	Updated according to further internal and external review feedback
1.0	19.09.2022	Fraunhofer	Creation of 1.0 from 0.8. Update of this table. Minor editing and formatting.
1.1	13.12.2022	LAU, Fraunhofer	Explanation for a low number of replies to evaluation questionnaires added in 3.2, 4.2, 5.2 and 6.2
1.2	21.03.2023	LAU, UIC, ETRA, Fraunhofer	Additional chapter (chapter 8) added to the deliverable to explain end-users' evaluation results strengthening in post-project phase. Inclusion of reference to new chapter in section 1.2 and reflection of it in last paragraph in chapter 10. Update of Bibliography. Update of this table and footers. Main inputs from LAU, UIC, ETRA and Fraunhofer.

DISCLAIMER AND COPYRIGHT

ABOUT SAFETY4RAILS

SAFETY4RAILS is the acronym for the innovation project: **Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILwaynetworkS**. 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 onrush 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

ABOUT SAFETY4RAILS 3
Executive summary 8
1. Introduction 9
1.1 Overview 9
1.2 Structure of the document 10
2. Description of S4RIS 11
3. Exercise 1 (Madrid Spain; MdM) 14
3.1 Use scenario summary and S4RIS capabilities tested 14
3.2 Results of the exercise 1 17
3.2.1 Prevention phase 17
3.2.2 Detection phase 18
3.2.3 Response phase 19
3.2.4 Recovery phase 20
3.2.5 S4RIS Graphical User Interface 21
3.2.6 S4RIS platform 21
3.2.7 MdM exercise evaluation 22
3.2.8 Overall questions 22
3.3 Analysis of the results of the exercise 1 23
4. Exercise 2 (Ankara Turkey;TCDD&EGO) 24
4.1 Use scenario summary and S4RIS capabilities tested 24
4.2 Results of the exercise 2 26
4.2.1 Prevention phase 27
4.2.2 Detection phase 28
4.2.3 Response phase 29
4.2.4 Recovery phase 30
4.2.5 S4RIS Graphical User Interface 31
4.2.6 S4RIS platform 31
4.2.7 TCDD&EGO exercise evaluation 32
4.2.8 Overall questions 32
4.3 Analysis of the results of the exercise 2 33
5. Exercise 3 (Rome Italy; RFI) 35
5.1 Use scenario summary and S4RIS capabilities tested 35
5.2 Results of the exercise 3 36
5.2.1 Prevention phase 37
5.2.2 Detection phase 37
5.2.3 Response phase 38
5.2.4 Recovery phase 39
5.2.5 S4RIS Graphical User Interface 40

5.2.6 S4RIS platform 40
5.2.7 RFI exercise evaluation 41
5.2.8 Overall questions 41
5.3 Analysis of the results of the exercise 3 41
6. Exercise 4 (Milan Italy; CdM) 42
6.1 Use scenario summary and S4RIS capabilities tested 43
6.2 Results of the exercise 4 44
6.2.1 Prevention phase 45
6.2.2 Detection phase 45
6.2.3 Response phase 46
6.2.4 Recovery phase 47
6.2.5 S4RIS Graphical User Interface 47
6.2.6 S4RIS platform 47
6.2.7 CdM exercise evaluation 48
6.2.8 Overall questions 48
6.3 Analysis of the results of the exercise 4 49
7. Nominal Group Technique evaluation 51
7.1 Focus group discussions 1 51
7.1.1 Results of the focus group discussions 1 52
7.2 Focus group discussions 2 53
7.2.1 Results of the focus group discussions 2 54
8. Strengthening of end users' feedback from the S4RIS during post-project phase 55
9. S4RIS influence for railway companies Business Continuity Management and Crisis Management. 59
10. Conclusion 61
Bibliography 66
ANNEXES 67
ANNEXI Glossary and Acronyms 67
ANNEX II Madrid (MdM) exercise schedule 69
ANNEX III Results of the MdM exercise 71
ANNEX IV Assessment of how far the MdM scenario objectives were met based on end-users' evaluation 111
ANNEX V Ankara (TCDD&EGO) exercise schedule 118
ANNEX VI Results of the TCDD&EGO exercise 120
ANNEX VII Assessment of how far the TCDD&EGO scenario objectives were met based on evaluation 181
ANNEX VIII Rome (RFI) exercise schedule 186
ANNEX IX Results of the RFI exercise 188
ANNEX X Assessment of how far the RFI scenario objectives were met based on evaluation 233
ANNEX XI Milan (CdM) exercise schedule 238
ANNEX XIIResults of the CdM exercise 239
ANNEX XIII Assessment of how far the CdM scenario objectives were met based on evaluation 292

ANNEX XIV Good faithassessment of D1.4 requirements/specifications test coverage in SEs..... 297

List of tables

Table 1 S4RIS Tools 12
Table 2 Tools involved in simulation exercise 1 14
Table 3 Tools involved in Simulation Exercise 2 25
Table 4 Tools involved in simulation exercise 3 35
Table 5 Tools involved in simulation exercise 4 43
Table 6 Tools participation in simulation exercises 62
Table 7 SAFETY4RAILS Good faith assessment of D1.4 requirements/specifications test coverage in SEs 63
Table 8 Glossary and Acronyms 67

List of figures

Figure 1 Domain Intersection of Tools in the S4RIS platform 11
Figure 2 The concept of S4RIS Platform Concept System Architecture 12
Figure 3 MdM exercise prevention phase – average rates for different tools 18
Figure 4 MdM exercise detection phase – average rates for different tools 19
Figure 5 MdM exercise response phase – average rates for diffetent tools 20
Figure 6 MdM exercise recovery phase – average rates for different tools 21
Figure 7 MdM exercise S4RIS GUI – average rates for statements 21
Figure 8 MdM exercise S4RIS – average rates for statements 22
Figure 9 MdM exercise evaluation – average rates for statements 22
Figure 10 MdM exercise overall feedback of S4RIS – average rate for statement 22
Figure 11 TCDD&EGO exercise prevention phase – average rates for different tools 28
Figure 12 TCDD&EGO exercise detection phase – average rates for different tools 29
Figure 13 TCDD&EGO exercise response phase – average rates for different tools 30
Figure 14 TCDD&EGO exercise recovery phase – average rate for tool 31
Figure 15 TCDD&EGO exercise S4RIS GUI – average rates for statements 31
Figure 16 TCDD&EGO exercise S4RIS platform – average rates for statements 32
Figure 17 TCDD&EGO exercise evaluation – average rates for statements 32
Figure 18 TCDD&EGO exercise overall feedback of S4RIS – average rate for statement 33
Figure 19 RFI exercise prevention phase – average rates for different tools 37
Figure 20 RFI exercise detection phase – average rates for different tools 38
Figure 21 RFI exercise response phase – average rates for different tools 39
Figure 22 RFI exercise recovery phase – average rate for tool 39
Figure 23 RFI exercise S4RIS GUI – average rates for statements 40
Figure 24 RFI exercise S4RIS platform – average rates for statements 40
Figure 25 RFI exercise evaluation – average rates for statements 41
Figure 26 RFI exercise overall feedback of S4RIS – average rate for statement 41

Figure 27 CdM exercise prevention phase – average rates for different tools 45
Figure 28 CDM exercise detection phase – average rates for different tools 46
Figure 29 CdM exercise response phase – average rates for different tools 46
Figure 30 CdM exercise recovery phase – average rate for tool 47
Figure 31 CdM exercise S4RIS GUI – average rates for statements 47
Figure 32 CdM exercise S4RIS platform – average rates for statements 48
Figure 33 CdM exercise evaluation – average rates for statements 48
Figure 34 CdM exercise overall feedback of S4RIS – average rate for statement 49
Figure 35 SAFETY4RAILS objectives designed to deliver capabilities to support the characteristics of resilient systems. Left image (DEPARTMENT OF COMMUNICATIONS, August 2019) p.8 and p. 22, Right Image (European Comission, June 2021) p. 32 59
Figure 36 BCM and Resilience Cycles 60

Executive summary

The Task T8.3 Evaluation – end-user and developer feedback for improvements- aim is to provide conclusions on the applicability, feasibility and success of the developed SAFETY4RAILS Information System (S4RIS) platform. This document is the deliverable D8.5 – Final Version of Evaluation Report– of SAFETY4RAILS, aiming at presenting the evaluation results of the S4RIS platform. This report summarises the evaluation results of all four simulation exercises and two Nominal Group Technique evaluation events that were carried out in the timeframe of M17 (February 2022) – M22 (July 2022).

The basis for the implementation of the evaluation was the deliverable D8.1 - Evaluation Methodology, end-user requirements and derived specifications detailed in D1.4 - Specification of the overall technical architecture, D8.2 - First draft of the blueprint exercise handbook, and D8.3 - Final draft of the blueprint exercise handbook. The deliverable builds on and extends the D8.4 First version of the evaluation report. The evaluation focused on 2 main aspects:

- The organisation of the exercise.
- The performance of the S4RIS against pre-defined objectives related to:
  - Usability.
  - Specific requirements laid out by the end-users in SAFETY4RAILS Deliverable D1.4.
  - Scenario-based requirements/objectives identified in SAFETY4RAILS Deliverable D8.2, and in SAFETY4RAILS Deliverable D8.3 (referenced back to e.g. tool the specific requirements/specifications identified in D1.4).

The S4RIS was evaluated in four Simulation Exercises and feedback was collected with altogether 17 online questionnaires. Overall, the respondents valued most the developing integration between the different information sources and systems as well as detection capabilities. The platform gives the opportunity of collecting information and updating it, obtaining a simulation of different choices and giving back a decision support system for security purposes. The benefit of support in decision-making and combined alert from different tools were also highlighted. The detection tools, which demonstrated early detection of anomalies or vulnerabilities, were appreciated for anticipating situations and preventing or mitigating the consequences of cyber and physical attacks

1. Introduction

1.1 Overview

This deliverable presents the evaluation/validation results including evaluation-based lessons learnt from the SAFETY4RAILS Information System (S4RIS) simulation exercises. This report concentrates on optimization potentials for technical aspects of the S4RIS. The evaluation results of the S4RIS are also useful input for demonstrating and identifying potential improvements in railway and metro crisis business continuity management.

The evaluation methodology is described in SAFETY4RAILS Deliverable D8.1 and this deliverable should be read simultaneously. In this deliverable, the methodology is described briefly and how the process and questionnaires changed according to feedback and observations in each exercise. Moreover, the simulation exercises scenarios and the tool capabilities that can be provided either through the S4RIS platform or as a standalone (in the first exercises) are described in D8.2 and D8.3[1] (D8.2 first version and D8.3 final version– development of a blueprint exercise handbook). To avoid duplication, in this deliverable only the summary of used scenarios and participated tools are presented.

Four simulation exercises, which represent four scenarios, were organised within the project to test and evaluate the S4RIS platform. The first simulation exercise (MDM exercise) was carried out in February (project month 17), the second exercise (EGO, Ankara) in April (project month 19), the third exercise (RFI, Rome) in June (project month 21) and the last exercise (CDM, Milan) in July (project month 22). Within the time between the simulations, the identified proposals for improvement of the solution and further evaluation were taken into consideration where possible. The exercises were carried out using online and on-site possibilities to attend the exercises due to COVID-19 restrictions. As primary evaluators of the exercises, representatives of eight end-user companies were involved: CDM (City of Milan in Italy), MDM (Metro De Madrid), EGO (Ankara Metro), RFI (Rail Infrastructure Manager in Italy), PRORAIL (Rail Infrastructure Manager in the Netherlands), TCDD (State Railway in Turkey), FGC (Ferrocarrils de la Generalitat de Catalunya) and UIC (the Worldwide Railway Organisation).

The main output of the SAFETY4RAILS project is the SAFETY4RAILS Information System (S4RIS) platform. S4RIS is an integrated platform that offers and combines risk assessment, monitoring, simulation, and decision support capabilities as well as “visualisation means to prevent, forecast, detect, defuse, respond and mitigate the impact of cyber and physical threats in a holistic methodological and operational approach resulting in a collaboration between cyber-physical security technologies and actors”[2]. The SAFETY4RAILS project aimed at a prototype of the S4RIS, which could be demonstrated and validated in an operational environment. The overall philosophy was to bring different technologies together and combine these with the S4RIS, to provide various functionalities towards supporting the end-users in the railway and metro sector in the handling of cyber, physical, and combined cyber-physical threats.[3]

The evaluation focused on two main aspects:

- The organisation of the exercise (as carried out).
- The performance of the S4RIS against pre-defined objectives related to:
  - Usability.
  - Specific requirements laid out by the end-users in SAFETY4RAILS Deliverable D1.4.
  - Scenario-based requirements/objectives to be identified in SAFETY4RAILS Deliverable D8.2and in SAFETY4RAILS Deliverable D8.3.

[1] SAFETY4RAILS Deliverable D8.2 and deliverable D8.3.

[2] SAFETY4RAILS Grant Agreement, version 2.0.

[3] SAFETY4RAILS Deliverable D1.4.

Feedback from all participants was collected during the evaluation of the simulation exercise in order to improve the preparations for the next simulation exercise as well as future exercises. The focus was on what can be done differently for the next exercises or what improvements need to be made.

The evaluation of the S4RIS was based on almost 300 requirements and connected specifications (not counting directly those high-level requirements in the Annex of the D1.4[4]) that have been identified as the basis for the development of the S4RIS platform considering the resilience of metro and rail infrastructure with the Smart City concept of multi-modality broadly.

All these requirements are documented and the specification in answer to each requirement is provided in SAFETY4RAILS Deliverable D1.4. As stated in D1.4, "*The requirements and specifications are input into both the S4RIS development cycle in SAFETY4RAILS and also future evaluation and validation cycles. The requirements and specifications have been formulated for a future S4RIS product.*"As stated in D8.1: *"As part of the usability, the Graphical User Interface (GUI) will be evaluated.Most of the requirements identified in D1.4 are technical and will validated within WP6 in the technical validation.The evaluation from the end-users performed within WP8 will focus on the ease of use (for all technical requirements), relevance (GUI-R06, GUI-R07, GUI-R17, GUI-R23) and the overall end-user satisfaction.*[5]"

The usability was evaluated as part of the user experience. As stated in D8.1 Evaluation Methodology the review of existing methodologies ISO 9241-11 (for ergonomic of human-system interaction) defines usability as the "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specifiied context of use".[6] As part of the usability, the Graphical User Interface (GUI) has been evaluated.

The main objective of scenario-based requirements evaluation was to provide feedback to the solution providers on the possible improvement of the tools. This supports the evaluation of the overall requirements and specifications, by evaluating the application of the S4RIS and its contributory tools against the specific scenario(s). The scenario-based requirements are presented in SAFETY4RAILS D8.3 "Final version – Development of a blueprint exercise handbook exercise handbook". It includes the description of the tool capabilities (i.e. specifications in answer to requirements) that were tested for each resilience stage of the scenario with the specific objectives of the simulation and the expected performance to be evaluated.

1.2 Structure of the document

The deliverable is structured so that the main and overall results of the evaluation are presented in the main body and the detailed results will be found in the relevant annexes.

This deliverable is structured in detail as follows:

- Section 1 introduces the deliverable.
- Section 2 introduces the S4RIS
- Section 3 reports on the exercise 1 (Madrid) including the main results.
- Section 4 reports the exercise 2 (Ankara) including the main results.
- Section 5 reports the exercise 3 (Rome) including the main results.
- Section 6 reports the exercise 4 (Milan) including the main results.
- Section 7 introduces the Nominal Group Technique (NGT) evaluation, including the results.
- Section 8 explains strengthening of the results of exercises evaluations in post-project phase
- Section 9 provides analysis of how the S4RIS solution can influence railway companies' Business Continuity Management and Crisis Management.
- Section 10 provides the conclusions of the S4RIS evaluation.

[4] SAFETY4RAILS Deliverable D1.4.

[5] SAFETY4RAILS Deliverable D8.1, page 21.

[6] International Organisation for Standardisation Ergonomics of human-system interaction: part 11:usability: definitions and concepts (ISO/DIS 9241-11.2:2016).

2. Description of S4RIS

The detailed architecture and system specifications are described in deliverable D1.4 in detail and with confidential information and in D2.3[7] in a public version. In this section, the SAFETY4RAILS is described briefly to give an overall picture of tools and functionalities.

The S4RIS platform is an online platform for cyber-physical security implemented into the SAFETY4RAILS project. It is designed to enable the integration of providers' capabilities in a single architecture supported by the platform. The platform specifically enhances end-user usability by enabling access to individual software tools through the platform (when they are integrated in it) and the combination of results from different tools. The combination of results from different tools can lead to an overall higher level of insight to support decision making within the resilience cycle for all phases.

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

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

The tools inside the platform are able to offer functionalities under one of those domains although it is more often the case that a tool will provide an intersection of functionalities across these domains. The following Venn diagram shown in Figure 1 depicts this concept by visualizing the intersection of tools across the different domains in the S4RIS platform. The diagram presented aims to provide a broad understanding with regards[8]

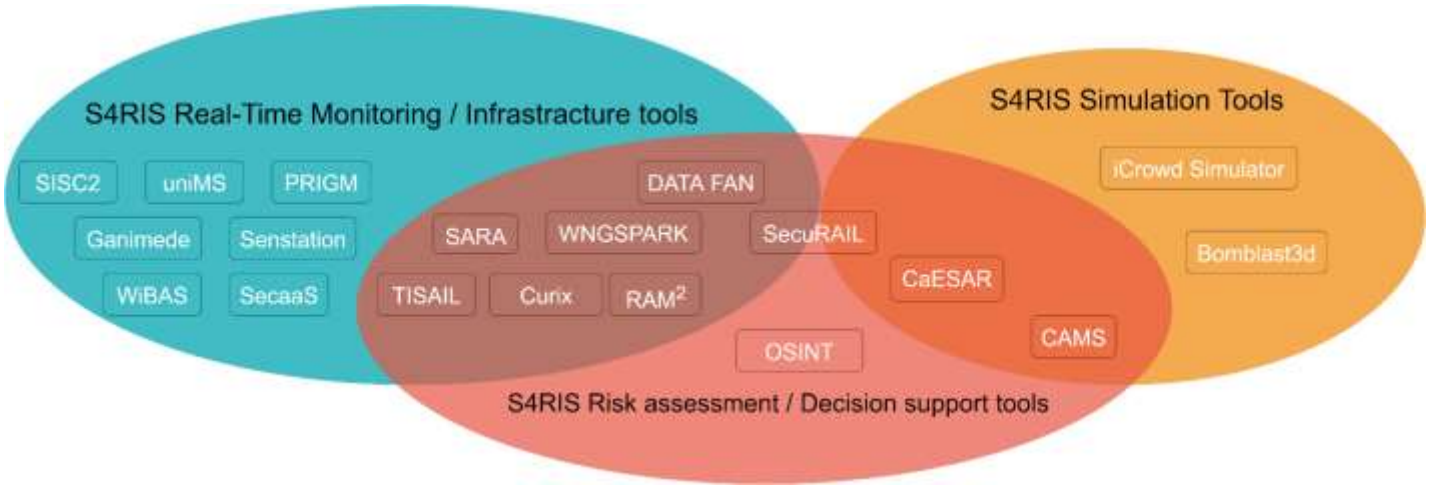


FIGURE 1 DOMAIN INTERSECTION OF TOOLS IN THE S4RIS PLATFORM

The S4RIS main components include [1] Graphical User Interface (GUI) to enable end-users to view individual software tools' (where integrated) GUIs either within the S4RIS itself or through opening a new "Tab", [2] 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 Figure 2 from D2.3 presents the SAFETY4RAILS architecture[9].

[7] SAFETY4RAILS Deliverable D2.3, System specification and concept architecture.

[8] SAFETY4RAILS Deliverable D2.3, System specification and concept architecture, page 9.

[9] SAFETY4RAILS Deliverable D2.3, System specification and concept architecture, page 40.

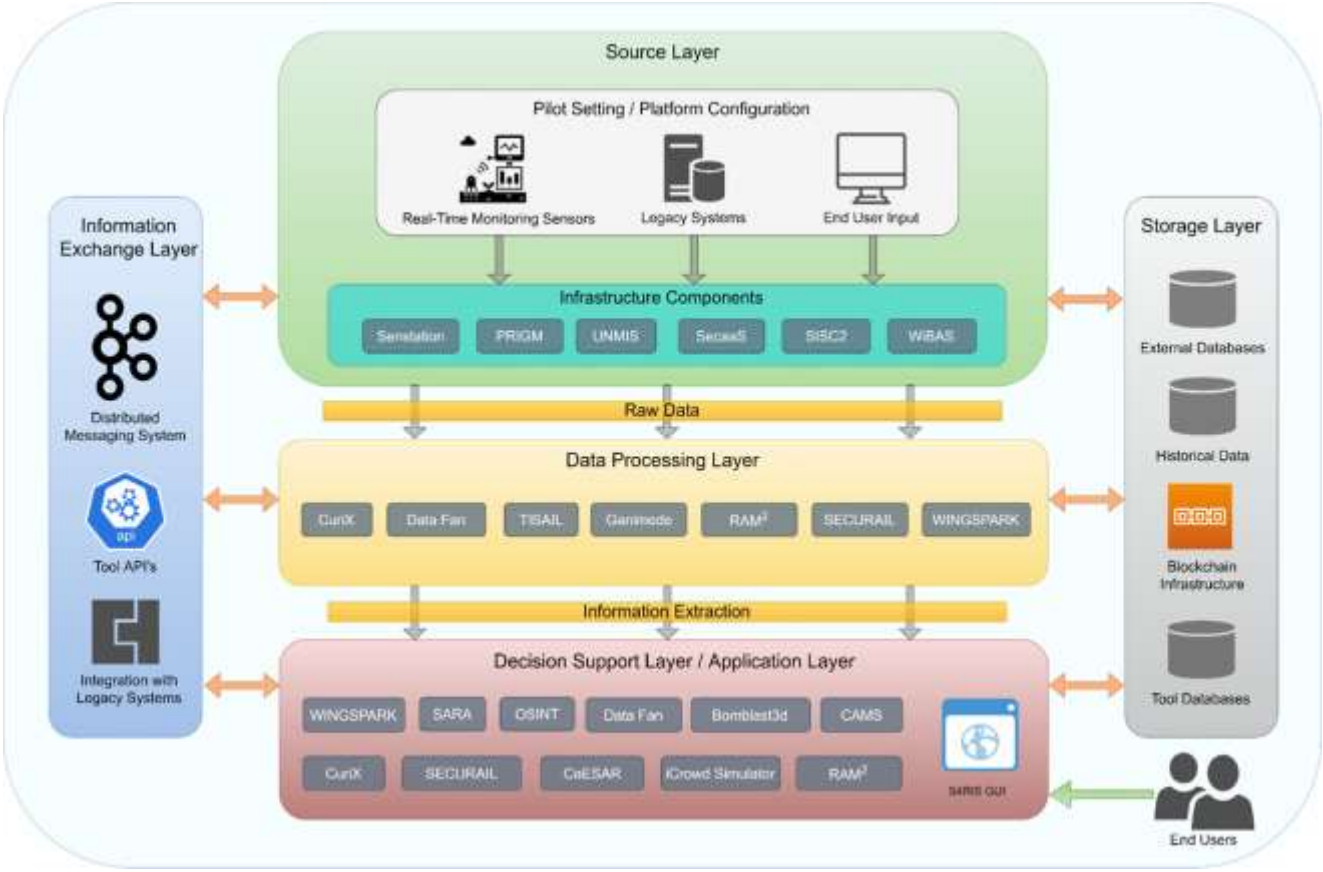


FIGURE 2 THE CONCEPT OF S4RIS PLATFORM CONCEPT SYSTEM ARCHITECTURE

Table 1 presents the targeted functionalities of the contributory S4RIS tools modified from the D2.3 original text.

TABLE 1 S4RIS TOOLS

Tool	Tool description
BomBlast3d	BB3d is a tool capable to fast predict blast loading due to high-explosive bomb attack and the consequent damage on people and structures. Experimental data is its basis
iCrowd	iCrowd is a general purpose, agent-based modelling platform that provides an abstract, domain-agnostic simulation framework. It can for example simulate large-scale crowds in indoor and outdoor areas, focusing on behaviour modelling, and be used for evaluation of potential blind spots in applied surveillance measures.
CAMS	CAMS provides an innovative approach to long-term asset management of infrastructure systems. With the understanding of the range of deterioration scenarios for the systems, asset condition data is captured to support risk identification and budget allocation forecasting. In the cases of the sudden damage or destruction to assets it can also be applied to understand the budgetary need and priorities for repair and/or replacement.
SecuRail	SecuRail is a quantitative risk assessment tool for analysis of cyber-physical threats in railway and metro network. SecuRail enables facility and security managers to model their own railway infrastructure and conduct a tailored risk analysis to evaluate likelihood and potential impact of a set of possible threat scenarios, including impacts caused by the cascading effect and the potential benefits of implementing further mitigation measures.
TISAIL	TISAIL is a threat intelligence platform for the railway sector. TISAIL incorporates three different stages as part of the threat intelligence process: i) uses automated processes for

	discovering potential threats using threat intelligence feeds, malware repositories, vulnerability reports and detection rules; ii) Carries out malware analysis processes; and iii) Extracts Indicators of Compromise (IoC) and enriches the gathered information in order to generate threat data and notifications for use by other S4RIS tools.
OSINT	OSINT is a platform for gathering, analysing and sharing potential threats to railway infrastructure for cyber, physical and combined cyber-physical threats. The main objective of the platform is to channel relevant threats to operators as soon as information becomes available in open sources in order to enable operators to prevent continuing exposure to those threats
PRIGM and SENSTATION	PRIGM and SENSTATION present a point-to-point secure channel between edge nodes where data is generated (e.g. by sensor measurements) and the central systems where the railway infrastructure and services are managed (e.g. Operational Control Centre - OCC). Unexpected patterns in the data can also be used as a method for anomaly detection.
DATAFAN	DATAFANenables the user to analyse sequential data such as time series using machine-learning algorithms to generate specifically in this project a prognosis of passenger load in stations, including spare capacity, based on historical data, together with a measure of a reliability of the results. This has the aim of assisting end-users in redirecting passengers to alternative stations (for the situation that a station is closed), based on their predicted capacity.
CaESAR	CaESAR evaluates the impact of disruptions on single, or coupled critical infrastructures. The tool identifies critical components, and investigates mitigation strategies, providing a ranked list as well as performance time curves. The focus in SAFETY4RAILS was for the situation in which a station is closed.
WINGSPARK	WINGSPARK is a platform, which provides active monitoring, forecasting and anomaly detection mechanisms, delivering insights to the operational condition of the environment it supervises. Currently, WINGSPARK has three primary components: i) Time-series based anomaly detection utilizing train speed measurements retrieved from IoT sensors, ii) Time-series based anomaly detection utilizing energy consumption measurements; and iii) Detection of overcrowded situations in the monitored railway infrastructure, based on video acquired through CCTV cameras.
CuriX	CuriX is a commercial tool to monitor technical devices (e.g., IT, OT) in real-time. It monitors the system behaviour, learns normal behaviour based on statistical and machine learning methods, and informs the users about deviations.
RAM2	RAM2 is an industrial digital and cybersecurity platform for risk monitoring, assessment and management. It integrates with a wide variety of security and industrial systems to collect and correlate data and events, to provide complete asset inventory visibility, identify vulnerabilities, evaluate the security posture, and detect suspicious patterns. RAM2 prioritizes and alerts on risks and provides clear risk mitigation steps, which are feasible within the operational constraints.
SARA	SARA (SECURESTATION Attack Resilience Assessment) aims to analyse a station and its equipment from a security point of view. The results of the analyses will enable the user to define, evaluate, rank and select possible countermeasures to be applied to the equipment of the station in order to reduce the effects of a terrorist attack.
SecaaS	SecaaS is a software platform that enables for monitoring of network traffic for signs of abnormality. The platform also provides Security as a Service though virtual firewalls and web application firewalls enhancing the security of the network.
WIBAS	WIBAS is a state-of-the-art Point-to-MultiPoint (PtMP) native Ethernet microwave product line. It provides access to broadband fixed wireless access. It is especially designed for

	high-speed multi-service applications, WiBAS offers a wide service area footprint reaching distant underserved areas and locations lacking telecommunications infrastructure.
uniMS	uni|MS (Unified Management Suite) serves the concept of simple and unified management for networks, infrastructure and systems. uni|MS. The platform automates management and monitoring tasks to eliminate error-prone and time-consuming manual efforts. uni|MS platform automates decision-making and augments operators' responsiveness, throughout all phases of the network lifecycle.
Ganimede	Ganimede is a platform for the large-scale analysis of live and recorded data streams based on Deep Learning. Ganimede is implemented exploiting Video Analysis techniques, in IT platforms and security, supported by competence centres specialized in artificial vision and deep learning. Ganimede Video Content Analysis platform enhances situational awareness and transforms threat detections from a manual, resource-intensive operation into an efficient and automated process [15].

3. Exercise 1 (Madrid Spain; MdM)

This section describes the Metro de Madrid (MdM) exercise and how the methodology was applied to it. In short, the S4RIS and the contributory tools included in the MdM exercise based on their development status at that time were successfully demonstrated. However, not all tools in S4RIS were applicable to all simulation exercises and this was the case with the MdM exercise as well. The simulation exercises were primarily based on the user scenarios that the individual host end-users were most interested. This means that this report (and accordingly this section) does not take into account every single tool within the S4RIS project scope. The methodology enabled feedback for the planning of future exercises and for development iterations.

During the second week of February 2022 (8th-11th), the first SAFETY4RAILS Simulation Exercise (SE) was performed at the Metro de Madrid facilities. It was co-organised by MdM and ETRA, who provided the technical leadership. The exercise was performed in a hybrid mode, due to the COVID-19 incidence rate in Europe during the selected days and connected limitations regarding travel.

The event brought together around 60 representatives from the SAFETY4RAILS consortium, participating physically in Madrid and online. As mentioned, representatives from eight end-users attended: CdM (Comune di Milano in Italy), MdM (Metro de Madrid), EGO (Ankara Metro), RFI (Rail Infrastructure Manager in Italy), PRORAIL (Rail Infrastructure Manager in the Netherlands), TCDD (State Railway in Turkey), FGC (Ferrocarrils de la Generalitat de Catalunya) and UIC (the Worldwide Rail Organisation).

For a full schedule of the simulation exercise, please refer to Annex II.

3.1 Use scenario summary and S4RIS capabilities tested

The objective of the Madrid simulation exercise was to evaluate both the first version of the S4RIS platform in the context of a cyber-physical attack in connection with a sporting event and the individual tool capacities. The scenario was developed in T8.1 and reported in detail in D6.2 Annexes – as a confidential deliverable, while the overall organisation is described in D8.3.

The simulation exercises involved several S4RIS capabilities to cover each resilience stage in the context of the scenario: prevention, detection, response, recovery.

In this simulation exercise, 11 tools were deployed to provide some of their functionalities. Some functions were integrated into the S4RIS platform whereas others were demonstrated stand-alone. Table 2 presents the tools involved in SE and in which phase each tool was involved.

TABLE 2 TOOLS INVOLVED IN SIMULATION EXERCISE 1

PREVENTION	DETECTION	RESPONSE	RECOVERY

CaESAR CAMS iCrowd PRIGM RAM2 SecuRail TISAIL/OSINT DATAFAN BB3d	CuriX RAM2 TISAIL/OSINT WINGSPARK DATAFAN	iCrowd RAM2 DATAFAN WINGSPARK CaESAR	CAMS BB3d

The evaluation was conducted through observations and online questionnaires, followed by a debrief in which the users stated their feedback on the SAFETY4RAILS tools.

Altogether four debrief sessions were conducted, one after each workshop/resilience phase. The online debrief was organised using the Microsoft Forms questionnaires. The number of the questionnaires was dependent on the structure of the exercise and each questionnaire assess the same elements of the tools in different resilience phases. The final debrief also included a discussion session where participants were asked to provide oral feedback on pre-prepared questions.

The exercise started with the prevention phase. Two simultaneous sessions were held in which the BB3D (Bomb Blast Simulation with outdoor and indoor effects (Civil Construction Department)) and CAMS (Proactive asset management and preparedness (Maintenance Department)) were presented in one session and iCrowd (Outdoor stampede due to bomb blast. Assessment CCTV configurations for detecting blind spots (Security Department)) and SecuRail (Offline risk assessment (Security Department)) in another session. This means that not all participants were able to provide their feedback from each tool used in the exercise. After these sessions TISAIL/OSINT (Identification of existing vulnerabilities in the cyber domain) and PRIGM (PRIGM - Detailed report regarding hardware-based vulnerabilities, supporting countermeasures) were presented to all participants. The first debrief took place after the prevention phase activities.

Further during the prevention phase DATAFAN (Prediction of passenger flow in stations and related what-if-scenarios), CaESAR (Cascading effects and resilience analysis) RAM2 (Vulnerability and security gaps assessment) were demonstrated and the second debrief concluded the phase.

In the response and detection phase test, first the WINGSPARK, CuriX and SAFETY4RAILS information system GUI were presented and after the presentation, the functional simulation “live” exercise took place. The capabilities of relevant individual tools and their overall correlation, enabled through the S4RIS architecture with its Distributed Messaging system (DMS), for managing on-going attacks were demonstrated. The Postman tool (Inc., 2022) was used to publish messages, prepared in advance of the simulation, primarily for subscription by the RAM2 tool which to date provides the main decision support in S4RIS. The JSON messages matched those that the individual tools generate in terms of structure and content (Crabbe, 2022).

The last phase of the exercise was the recovery phase where BB3D and CAMS session were organised in parallel. The final debrief with the discussion session concluded the exercise and evaluation session.

The objectives for the tools in MdM exercise was:

- **CaESAR (Fraunhofer):** One of the Simulation Exercise objectives is to test CaESAR’s correct identification of weak components in the MdM infrastructure and the proposed improvement measures to prevent an attack or mitigate the damages. The second objective is the evaluation of the adequacy of the proposed mitigation measures influencing resilience specific to the scenario. The simulation will give Fraunhofer a good representation of events to know if the CaESAR development is carried out in the right way thanks to the feedback of MdM as a metro infrastructure.
- **CAMS (RMIT):** Main objective of the simulation is testing-friendly-user interface; completion of information developed; new features introduced (Prediction of normal deterioration due to aging and degradation of railway assets, Maintenance, and repair budget calculation for railway components,

Deterioration, and budget calculation in case of extreme event). The exercise will give the chance to spot strong and weak points and gather suggestion from end-user point of view.

- **DATAFAN (Fraunhofer):** One objective is to test whether the number of predicted passengers for future time steps is an asset for redistributing passengers from the affected station Santiago Bernabeu to another. The second objective is to get feedback if the speed of computation is sufficient and if the presentation of the results is clear. The third objective is to evaluate whether the proposed reliability analysis for the results adds value to the end-user. If possible, the GUI of the DATAFAN tool should also be evaluated if it is clearly structured or too complex
- **RAM2 (ELBIT):** Monitoring tool vendors workshop (together with CuriX) to ensure data structure and data insights, integration of testing scenarios with each monitoring data sources and recorded scenarios data for scenario simulation from monitoring tools, with all relevant event types, from each data sources.
- **CURIX (IC):** The first objective is to test CuriX to show identified anomalies in the behaviour of "MdM technical systems" from their monitoring data, which could indicate a potential threat or disruption. A second objective is to test the identification of metrics and devices responsible for causing the major change in the system behaviour. Another objective is the evaluation the appropriateness of alerts and information related to content and timing as well as the health scores of the monitored technical system. A further objective is general feedback regarding the user-friendliness of the CuriX dashboard.
- **SECURAIL (STAM):** ThisSimulation Exercise will allow first to test SecuRail functionalities implemented in this initial release. For this purpose, SecuRailwill be used to carry out an off-line risk analysis of the MdM network infrastructure under examination within the Simulation Exercise. The risk analysis will be based on a set of inputs, such as the areas and asset included within the sections and stations belonging to the infrastructure, the countermeasures with which they are equipped, the crowding levels etc. that will be entered by the user through the SecuRail UI. The simulation, indeed, will provide an overview of the core functionalities of SecuRail and it will allow end-user to identify risk level of different components of the network, as well as the most dangerous threat scenarios that can occur in its infrastructure and the consequent impact on people, assets, and services.
- **TISAIL/OSINT (TREE/INNO):** The main objective for TISAIL/OSINT in this simulation exercise is to provide cybersecurity threats that are relevant for MdM security team as well as to provide a better understanding of real threats in the railway/metro sector.
- **WINGSPARK (WINGS):** WINGSPARK tool objectives will constitute the three different phases. First to detect potentially overcrowded areas during the day of the event in the metro station, to better manage the crowd in case of emergency. Then, to detect if there are any anomalies in the metro speed, analyse them and send an alert to the system's team. Finally, to inform, send details, during the response phase, of the detected issue in the metro speed. Alerts will be also raised in the case of overcrowded areas and guidelines in case of evacuation will be provided. Overall, WINGSPARK tool will try and identify anomalies, monitor areas in the facility and to detect if there is something that is not usual, possibly restrictions related to mobility (like forbidden areas etc.), overcrowded areas and propose measures to prevent chaos.
- **iCrowd (NCSRD):** iCrowd will be extended to provide not only the prediction of passenger flow rates and evacuation times assuming different congestion levels, but also the determination of the possible fallout from misleading information delivered by compromised digital assets. Crowd behaviours will also be refined to follow an objective-oriented approach, where instead of programming specific actions, the user will specify the objectives of a simulated agent and its actions will be determined automatically.
- **PRIGM (ERARGE):** Exchange the knowhow from previous and ongoing project for the sake of security assessment and vulnerability by (re)elicitation for the MdM data network and cyber infrastructure, identification of vulnerabilities within the network by analysing the communication and data transfer between nodes, analysis of the relations interlinking the nodes and extract the threat/attack surfaces. These objectives will be handled at low-level attack types (e.g., attack against hardware components) and will be aligned with the ENISA threat taxonomy.

- **BB3d (RINA):** Based on surface burst experimental data (i.e., validated by definition), potential verification of some BB3d functionalities (e.g., casualties) by comparing numerical results with data collected considering the effects of past bomb attacks.

3.2 Results of the exercise 1

All in all around 60 persons participated the exercise both online and present. Not all the respondents have participated in all the phases of the exercise neither have they had opinion or expertise of all the tools and therefore the number of responses related to different tools varied. The answering percent to evaluation questionnaires of the number of all the participants varied approximately between 10-26%. Low answering percent can be explained by the fact that feedback was collected only from end-users.

According to the D8.1 Evaluation methodology the questionnaires related to the usability of S4RIS GUI, the S4RIS platform specific and the scenario-based requirements were addressed only to the end-users. Of all the 59 participants 22 persons were representing end-user organisations. However, not all the 22 end-user representatives might have felt that they belonged to the end-users based on their duties in employer organisations. Totally 16 respondents have forwarded their feedback from the MdM scenario exercise in questionnaires. Of these 16 persons four (4) have represented the end-users organising the exercise and 12 persons have represented end-users from the Consortium (and therefore observing the pilot case). The answering percentage to evaluation questionnaires of the number of all the participating end-users has thus varied approximately between 23-64%. The answering percentage might have been even higher as obviously not all the end-user organisations representatives have reported themselves as end-users and neither have all the participating end-users participated in all the exercise phases.

The low number of the participants of the end-users organising the exercise has been explained by the difficulties of detaching people from their daily duties.

At this very first Simulation Exercise the decision was also taken in the preparation phase not to invite external end-users as participants. (In later exercises with increasing confidence in the S4RIS platform, external end-users supporting SAFETY4RAILS through the external board were invited.)

There were no significant differences when statistically comparing the results between these two end-user groups and therefore the results are not presented separately. The reader needs to take into consideration that the evaluation presented in this chapter is based on these first 16 responses.

The results presented in this chapter are the averages of the respondents' agreeing level to the questionnaire statements that each tool has received during the resilience phases they have participated during the exercise. Likert-scale answers in questionnaires have been changed to numbers as follows: strongly agree=5, agree=4, neither agree nor disagree=3, disagree=2, strongly disagree=1. Detailed questions and answers to each questionnaire are presented in Annex III. Answers to open-ended questions are presented original as they were provided.

The results presented in the following figures are largely following the schedule of the simulation exercise as presented in Annex II:

- S4RIS contributory tools prevention phase
- S4RIS contributory detection & response phase
- S4RIS contributory recovery phase
- S4RIS GUI and platform specific feedback
- Overall objectives of MdM evaluation and organization of the simulation exercise

Annex IV provides an assessment of how far the MdM scenario objectives were met based on end-users' evaluation for all resilience phases simulated at MdM.

3.2.1 Prevention phase

In MdM exercise, feedback for tools performance in prevention phase has been asked in questionnaires 1 and 2. In Figure 3 are presented the average rates that different tools have received with their capabilities relating to the prevention phase. 13 end-users have answered in questionnaire 1 and five end-users in questionnaire 2 to prevention phase related questions.

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the prevention phase/the decision-making process
- The GUI of the individual tool is user-friendly

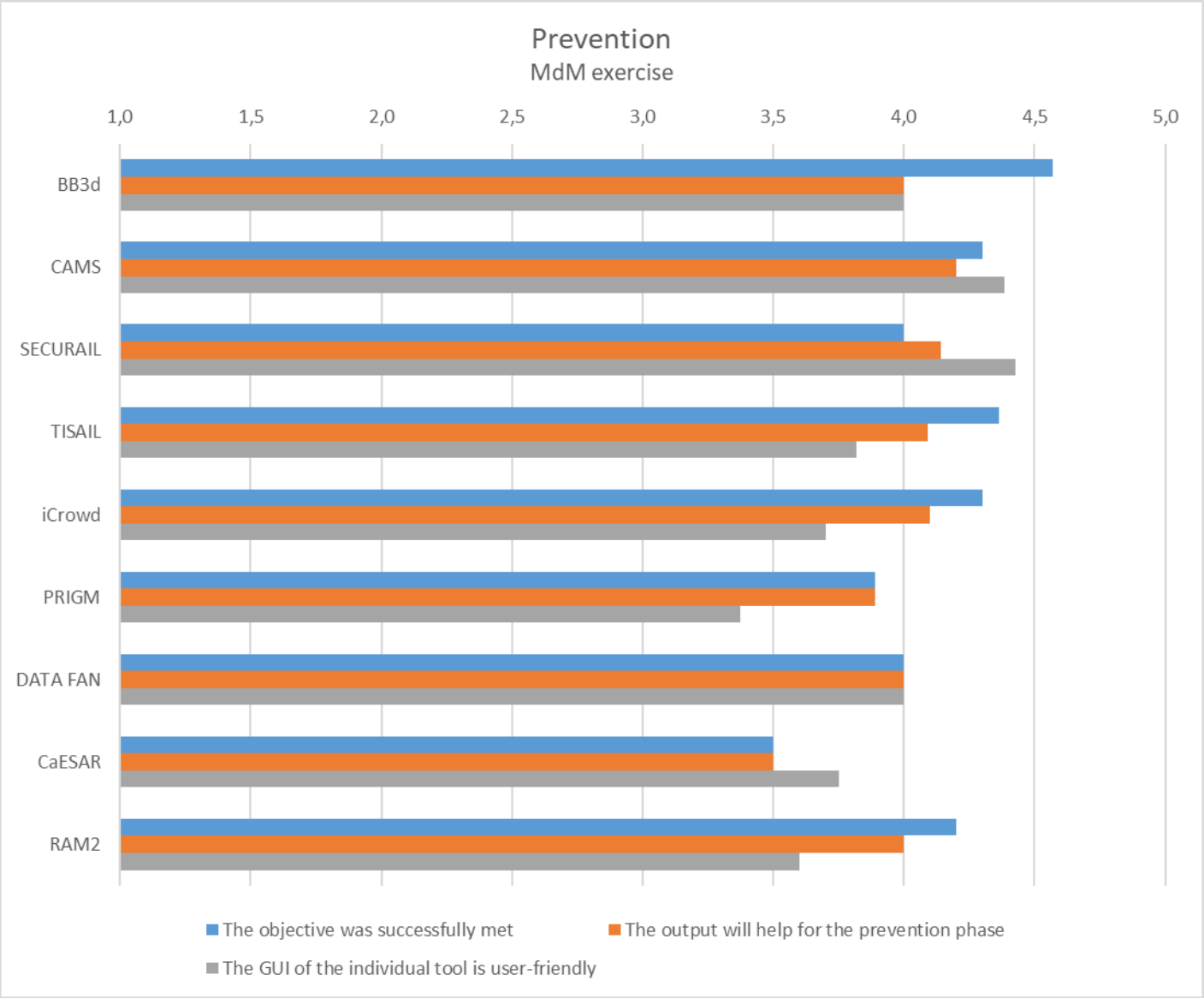


FIGURE 3 MDM EXERCISE PREVENTION PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

3.2.2 Detection phase

In MdM exercise feedback for tools performance in detection phase has been asked in questionnaire 3. In Figure 4 are presented the average rates that different tools have received with their capabilities relating to the detection phase. Seven end-users have answered to questionnaire.

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the detection phase/the decision-making process
- The GUI of the individual tool is user-friendly
- The time for processing was acceptable

During the individual tool demo sessions, the second statement has been "*The output will help for the detection phase*" and during the functional simulation exercise "*The output will help for the decision-making process*". In Figure 4 these results have been combined.

Statement "*The time for processing*" has been used only during the functional simulation exercise (detection and response phases).

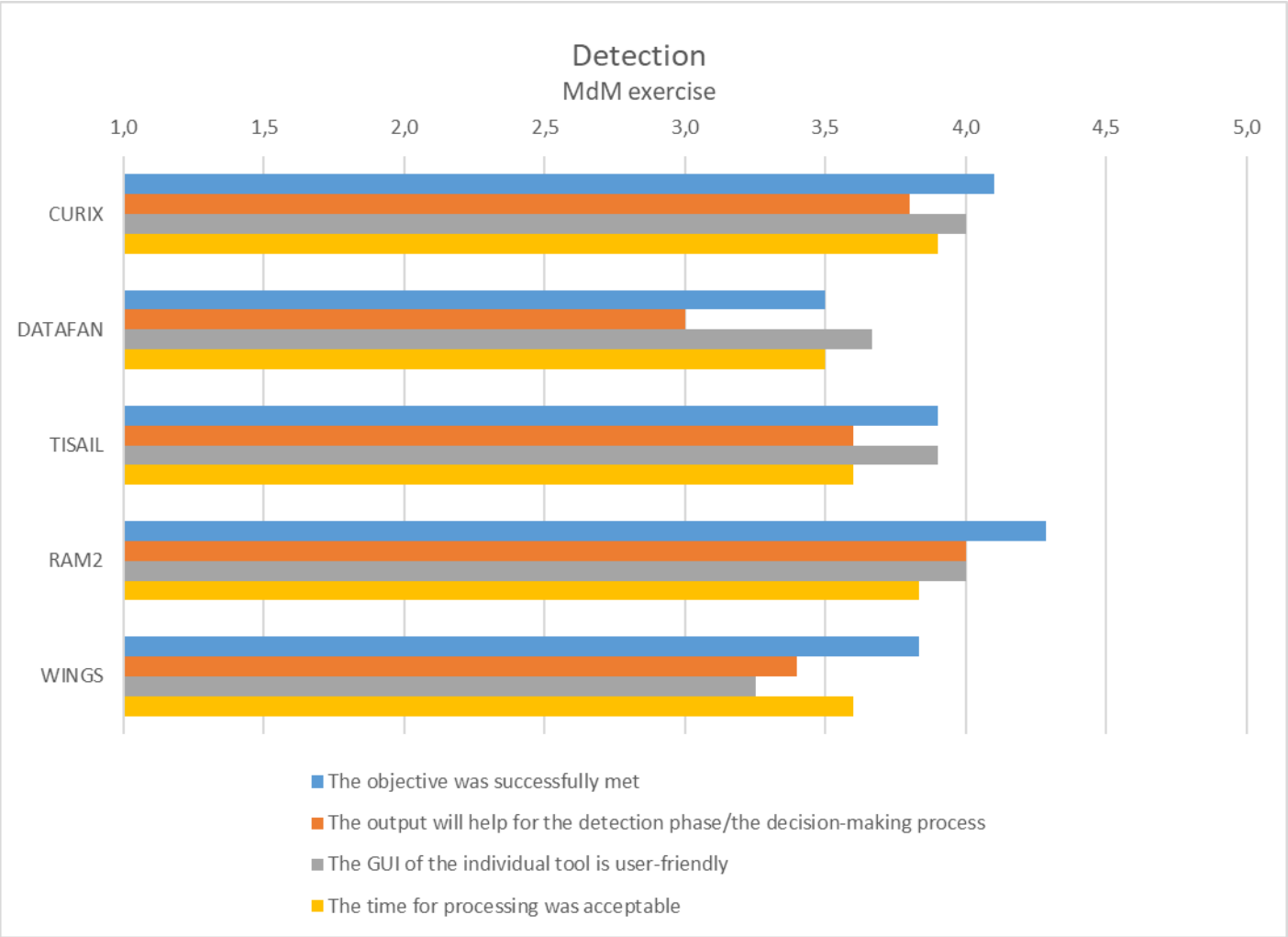


FIGURE 4 MDM EXERCISE DETECTION PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

3.2.3 Response phase

In MdM exercise feedback for tools performance in response phase has been asked in questionnaire 3. In Figure 5 are presented the average rates that different tools have received with their capabilities relating to the response phase. Seven end-users have answered to questionnaire.

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the response phase/the decision-making process
- The GUI of the individual tool is user-friendly
- The time for processing was acceptable

During the individual tool demo sessions, the second statement has been "*The output will help for the response phase*" and during the functional simulation exercise "*The output will help for the decision-making process*". In Figure 5, these results have been combined.

Statement "*The time for processing*" has been used only during the functional simulation exercise (detection and response phases).

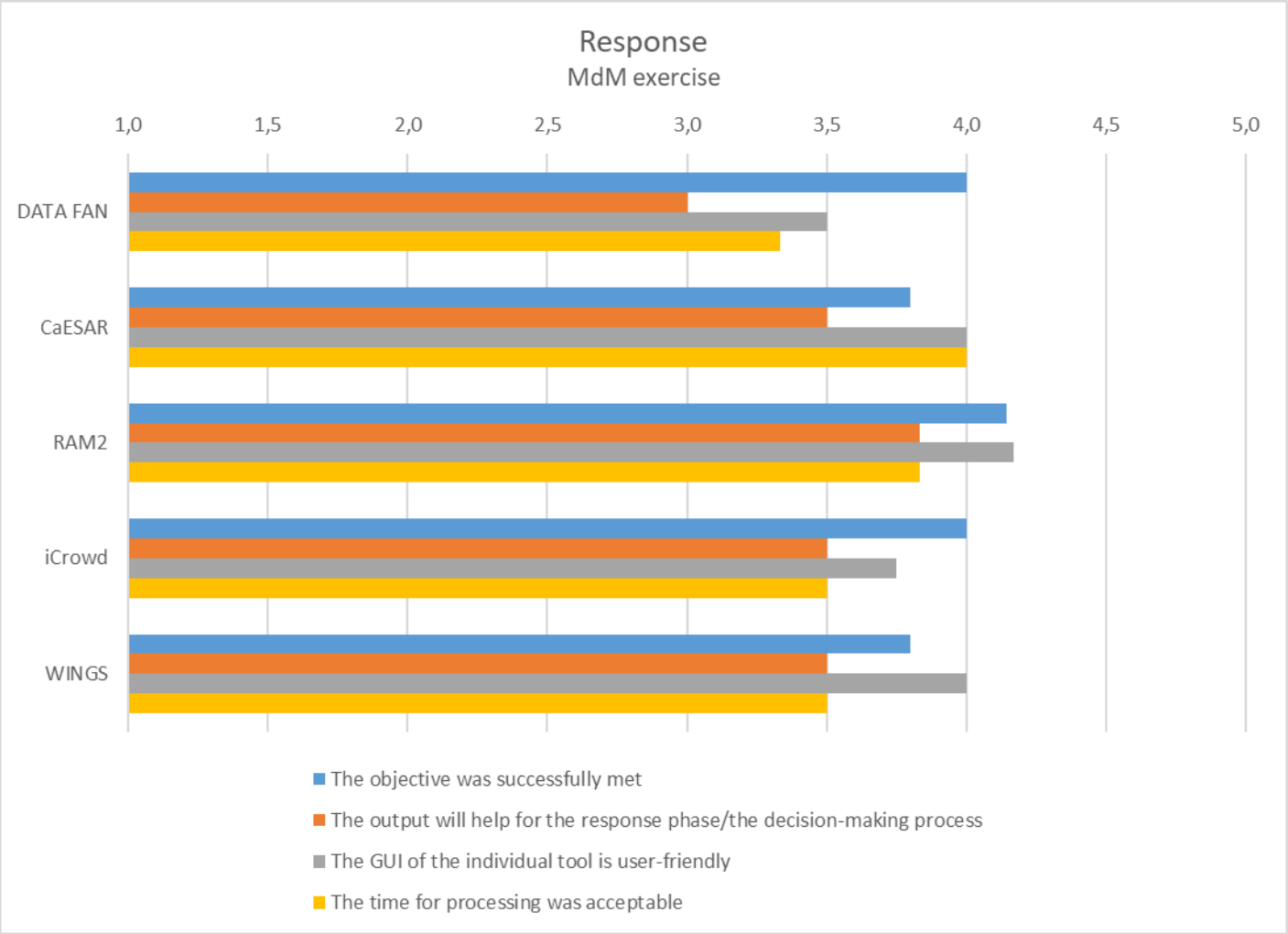


FIGURE 5 MDM EXERCISE RESPONSE PHASE – AVERAGE RATES FOR DIFFETENT TOOLS

3.2.4 Recovery phase

In MdM exercise feedback for tools performance in recovery phase has been asked in questionnaire 3. In Figure 6 are presented the average rates that different tools have received with their capabilities relating to the recovery phase. Seven end-users have answered to questionnaire.

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the recovery phase/the decision-making process
- The GUI of the individual tool is user-friendly

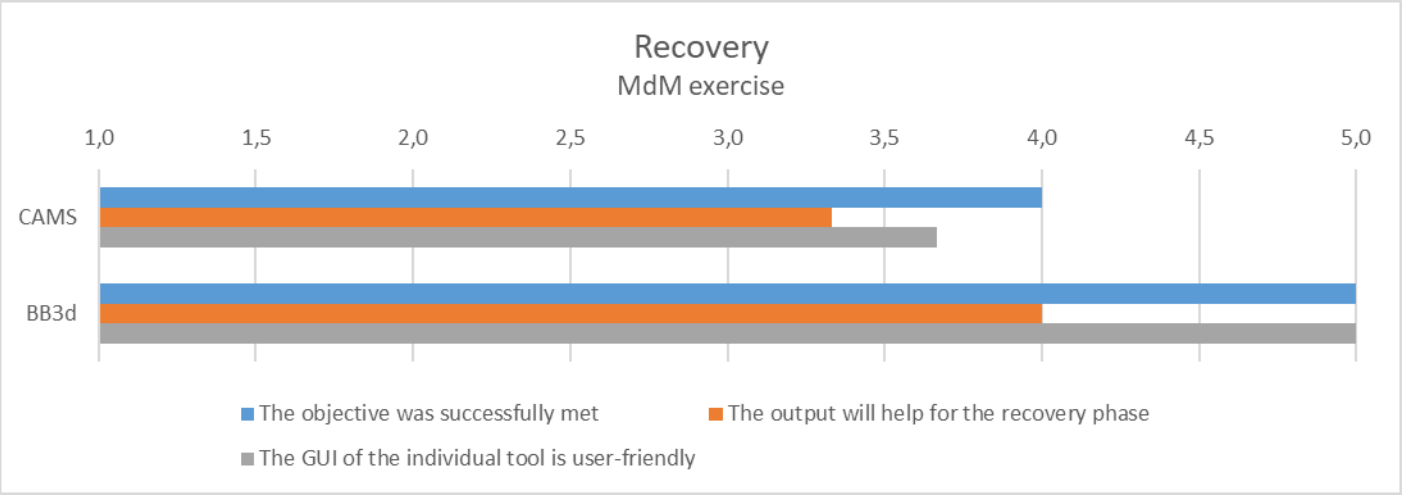


FIGURE 6 MDM EXERCISE RECOVERY PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

3.2.5 S4RIS Graphical User Interface

The feedback exercise's end-user participants have given for S4RIS GUI in Likert-scale statements is presented in Figure 7. Seven end-users have given their feedback in questionnaire 4.

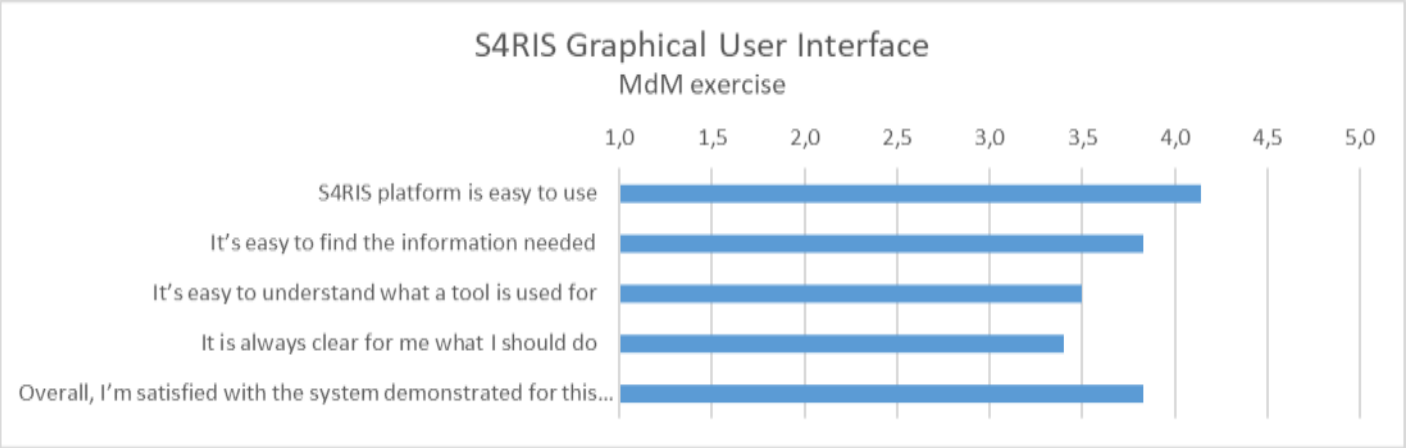


FIGURE 7 MDM EXERCISE S4RIS GUI – AVERAGE RATES FOR STATEMENTS

3.2.6 S4RIS platform

The feedback exercise's end-user participants have given for S4RIS platform in Likert-scale statements is presented in Figure 8. Seven end-users have given their feedback in questionnaire 4.

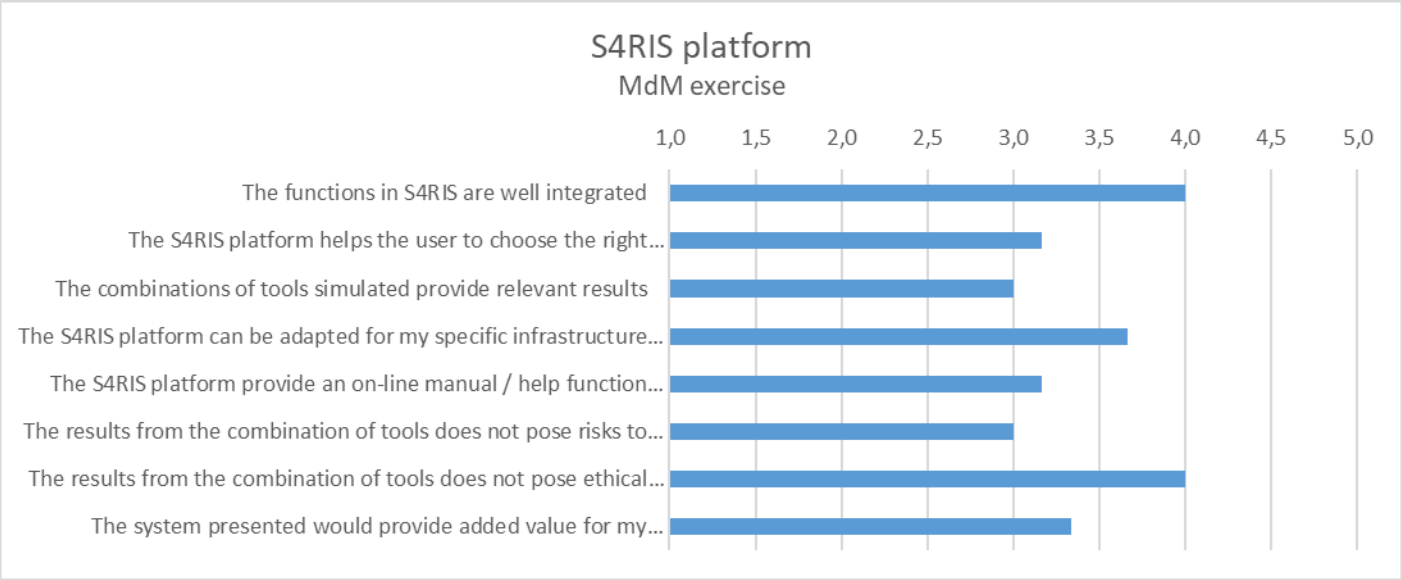


FIGURE 8 MDM EXERCISE S4RIS – AVERAGE RATES FOR STATEMENTS

The response to the statement "*The S4RIS platform provide an on-line manual / help function which is easy to understand*" is misleading. No on-line manuals or help functions were presented. In questionnaire an option "Not applicable" was offered for such a case when respondent is not able to answer, but no respondent has chosen that.

3.2.7 MdM exercise evaluation

Seven end-users have given their feedback to MdM exercise in questionnaire 4.

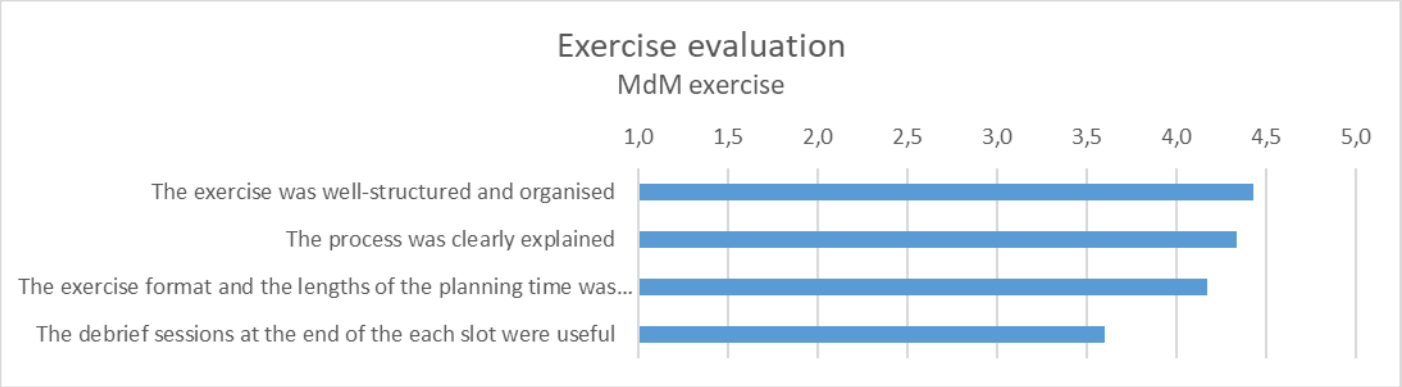


FIGURE 9 MDM EXERCISE EVALUATION – AVERAGE RATES FOR STATEMENTS

3.2.8 Overall questions

Seven end-users have given their feedback for the combination of tools in questionnaire 4.

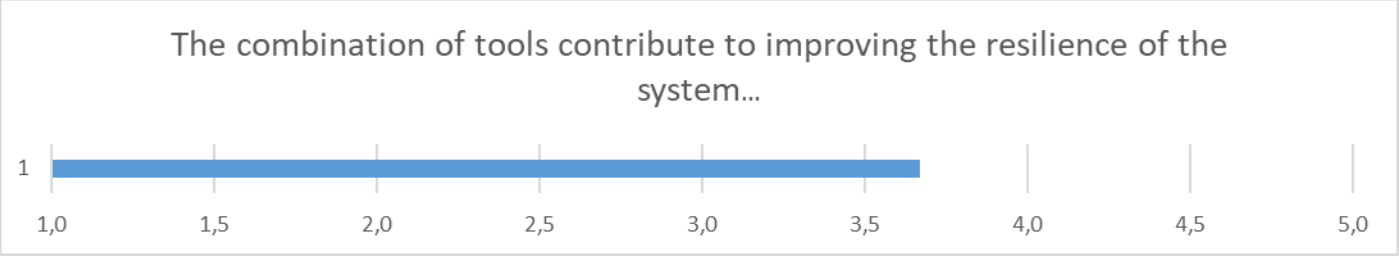


FIGURE 10 MDM EXERCISE OVERALL FEEDBACK OF S4RIS – AVERAGE RATE FOR STATEMENT

3.3 Analysis of the results of the exercise 1

Background

The MdM simulation exercise was the first simulation exercise and focused on a combined cyber and physical attack in the metro environment. It addressed four resilience phases: prevention, detection, response and recovery. Eleven tools and some of their capabilities have been demonstrated successfully, with 24 requirements tested (Annex IV) and evaluated by 16 end-users.

Functional evaluation analysis

In general, the capacities of the tools were appreciated by the responders with the majority of them evaluating that the objectives were successfully met, the output useful for the related resilience phases and the GUI of the tools user friendly (see Annex III).

From a functional point of view, no request for revising the requirements was raised by the end-users.

The Main benefits of the tools highlighted by the responders when answering the open questions of the questionnaires (available in Annex III) are the following:

- The demonstrated simulation capacities (BB3D, CAMS, SecuRAIL, iCrowd, DATAFAN, CAESAR) bring a lot of added value for managing cyber and physical risks and helping decision makers on the measures to be put in place to make metro systems more resilient:
    - The knowledge on how bomb blast may affect the metro infrastructures may help to make them more resilient in case of an attack: this may have a **clear impact on reducing deaths and injuries.**
    - Enabling off-line analysis to understand the level of risk for each critical assets during a given hazardous event may **contribute to the risk management process** and **help the user to compare the different measures and select them**.
    - Provision of information on the asset condition and degradation due to normal ageing or after a set of possible events may help to plan budget and improve asset obsolescence management, especially those in OT environments
    - In the prevention phase, the simulation of crowd in case of different events can be used to **improve the design of the infrastructure** as well as the implementation of CCTV taking into account blind spots. In the response phase, it can be used **to take decision on the closure or not of the station and on the best way to evacuate the station.**
- The detection tools (CaESAR, TISAIL, PRIGM, CURIX, WINGS) which demonstrated early detection of anomalies or vulnerabilities were appreciated by some of the responders for **anticipating situation and preventing or mitigating the consequences of cyber and physical attacks**.
- The integration of alerts from multiple sources in RAM2 help the users **ease the correlation of the events for proactive responses**.

The possible improvements that were mentioned are the following:

- Simulation capacities would benefit from more accurate data as well as more variables.
- The integration of the S4RS tools with the company information systems would need to be assessed.
- The integration of tools in the SAFETY4RAILS platform should be further developed.

Analysis of the organisation of the exercise and recommendations for the remaining exercises

The following recommendations were given for the organisation of the remaining three exercises:

- More end-users should be continued to be encouraged to attend and respond to the questionnaires.
- Invitations to end-users should identify for tools and resilience phases who are the targeted audiences based on roles in end-user organisations.
- Within the end-user group, different actors (operation planners, crisis managers, cybersecurity experts, etc.) should be included
    - Specifically, control centre managers from other railway operators were mentioned

- Show what would have been done in the specific scenario without S4RIS and compare them. This would show how S4RIS can add value to the management of these kind of events.
- Spend more time in the management process
- The exercise should be more adapted to railway scenarios, when compared to cases in Madrid
- Consider how better to track and document the responses provided informally during the breaks and in follow-up conversations.

Analysis of the Evaluation methodology and recommendations for the remaining exercises

The organisation of the exercise was well rated by the responders (Figure 9).

The main challenges of the evaluation by the end-users were first that the end-users representatives participating in the events had different profiles (e.g. Physical security experts, cybersecurity experts, safety experts) and were not able to comment on the added value or the possible improvement of the tools given the complexity of railways and metro environment.Second challenge for this first exercise was also to “digest” all the information provided during the simulation exercise with the presentation of 11 very innovative tools addressing a broad range of functionalities.

Based on data as provided in chapter 3, as well as internal debriefs and discussions of Madrid evaluations, the following recommendations can be given for the evaluation of the remaining three exercises:

- Check all end-user evaluators have access to the D1.4 sections 2.2 and 2.3 (requirement and specifications) and are requested to familiarise themselves with them before the simulation exercise.
- The online questionnaire should be presented in advance to the simulation exercise. This could be done by providing the link and access to it sometime before the exercises, though the ability to respond would of course be limited to after the exercise. The planned time period for their distribution is early week 16 2022 for the Ankara exercise.
- Answers to specific tool related questions are taken immediately after the tool presentation, with an opportunity to add to it in a debrief session later.
- It should be considered to collect developer feedback in a similar was to that as from the end-users. However, the responses should remain separate and the focus of activities and effort in WP8 should remain on obtaining end-user feedback.
- Feedback should be given to the tool developers as soon as possible after the exercise
- Open-ended question should be changed to Likert format questions as much as possible. Some open-ended questions should still remain in order to provide direct quotes and new points of view or approaches not covered in Likert scale questions.
- The Nominal Group Technique evaluation should be arranged as soon as possible after the second exercise (Ankara) and as soon as possible after the two exercises in Rome and Milano.
- Add open-ended questions related specifically to potentials to improve the business continuity management and especially the crisis management for the railway companies.

4. Exercise 2 (Ankara Turkey;TCDD&EGO)

This section describes the Ankara (TCC&EGO) exercise results and how the methodology was applied to it. In short, the S4RIS and the contributory tools included in the Ankara exercise based on their development status at that time were successfully demonstrated.

4.1 Use scenario summary and S4RIS capabilities tested

In the Ankara Metro (TCDD&EGO) Simulation Exercise, a second integrated version of the S4RIS platform was evaluated along with several innovative tools brought to the project. The use scenario was based on UC-004 *Physical attack – Potential terrorist attack via IED carried via baggage*, UC-006 *Physical attack – Intrusion*

and bomb planted and UC-007 *Physical Attack – Intrusion in Sensitive Place*, which are described in S4RIS deliverable D8.3 section 2.2. The Use cases included Cyber – Physical attack against the railway system. This specific scenario also covered multimodality by including Turkish State Railways (TCDD) in key parts of the exercise e.g. the prevention phase of the demonstration was conducted in a Workshop, involving the EGO personnel operating in the Operational Centre and analysing main weaknesses in the infrastructure and prepare proactive mitigations through S4RIS.

In the first simulation exercise, only the end-users were asked to answer the evaluation questions. Evaluation of the MdM exercise identified that also other participants could provide valuable feedback. In the Ankara exercise, the approach was adopted so that the end-users and tool providers answered tools and S4RIS related questions and all answered common exercise related questions. Answers from different types of participants can be distinguished.

Altogether six debrief sessions were conducted, one after each workshop/resilience phase. The online debrief were organised using the Microsoft Forms questionnaires. The exercise schedule is presented in AnnexV.

On day one, the first session had two individual tool presentations in the prevention and recovery phases. The tools presented in this part were iCrowd and CAMS, after which the first online questionnaire was distributed. The second session had four tool presentations: SECURAIL, CaESAR, DATAFAN and TISAIL/OSINT. After these individual presentations, a presentation of the S4RIS Platform User interface and progress so far with contributory tool integration was held. These were followed by the second online questionnaire.

Day two opened with a full joint scenario exercise, which included all four phases (prevention, detection, response, and recovery). RAM2 was the main decision support tool. Following this, the third questionnaire was presented, focusing more on the S4RIS solution as a whole. Later on in day two, there were more individual tool presentations but this time on the detection and response phases. The tools presented here were CURIX, PRIGM, SENSTATION and GANIMEDE. These were followed by the fourth online questionnaire, focusing once more on individual tool questions similar to day one. Day two afternoon continued with more individual tool presentations for the same phases (as relevant): DATAFAN, , TISAIL/OSINT and CaESAR followed by the fifth questionnaire. Closing the day was the sixth and final online questionnaire for the Ankara exercise, which included some final questions on user interface and tool integration so far. Table 3 presents the tools involved to SE and to which phase each tool were involved.

For a full schedule of the simulation exercise, please refer to ANNEX V Ankara (TCDD&EGO) exercise schedule.

TABLE 3 TOOLS INVOLVED IN SIMULATION EXERCISE 2

PREVENTION	DETECTION	RESPONSE	RECOVERY
CaESAR	GANIMEDE	DATAFAN	CAMS
DATAFAN	PRIGM	SecuRail	
PRIGM	SENSTATION	iCROWD	
SecuRail	TILSAIL/OSINT	CaESAR	
TILSAIL/OSINT	DATAFAN	RAM2	
CAMS	RAM2		
iCROWD	Curix		
RAM2			

The objectives for the tools in Ankara exercise was:

- **CaESAR (Fraunhofer):** One of the Simulation Exercise objectives was to test CaESAR correct identification of weak components in the EGO infrastructure and the proposed improvement measures to prevent an attack or mitigate the damages. The second objective was the evaluation of the adequacy of the proposed mitigation measures influencing resilience specific to the scenario and understanding propagation of the impact in the network.

- **DATAFAN (Fraunhofer):** One objective was to test whether the number of predicted passengers for future time steps is an asset for redistributing passengers from the affected station to another. The second objective was to get feedback if the speed of computation is sufficient and if the presentation of the results is clear. The third objective was to evaluate whether the proposed reliability analysis for the results adds value to the end-user.
- **Ganimede (LDO):** The main objective was the detection of objects and people in each frame with Convolutional Neural Networks (CNN) and their movement to determine if the object is candidate for abandon.
- **CURIX (CuriX):** The first objective was to test CuriX to show identified anomalies in the behaviour of "EGO's technical systems" from their monitoring data, which could indicate a potential threat or disruption. A second objective was to test the identification of metrics and devices responsible for causing the major change in the system behaviour. A third objective was to evaluate the appropriateness of alerts and information related to content and timing as well as the health scores of the monitored technical system. A further objective was general feedback regarding the user-friendliness of the CuriX dashboard.
- **PRIGM (ERARGE):** The main objective was to prevent cyber and cyber-physical attacks by establishing a secure data channel between end nodes (i.e.,Senstation which is a secure gateway encrypting the sensor data collected from the field).
- **SECURAIL (STAM):** SecuRailwas used to carry out an off-line risk analysis of the EGO network infrastructure under examination within the Simulation Exercise.
- **Senstation (ERARGE):** The main objective was to validate the functionality of the server-client/node communication by presenting a laboratory-scale implementation of sensors and Senstation.
- **TISAIL/OSINT (TREE/INNO):** The main objective for TISAIL in this simulation exercise was to test functionally with a real/realistic device and component data used in the system and to simulate the detection of vulnerable devices.
- **CAMS (RMIT):** Tabletop exercise to evaluate the predictions produced by the tool.
- **iCrowd (NCSRD):** iCrowdwasapplied to provide passenger flow rates and evacuation times assuming different congestion levels, considering the possible fallout from misleading information delivered by compromised digital assets.
- **RAM2 (ELBIT):** Monitoring tool vendors workshop (together with Curix IC) to ensure data structure and data insights, integration of testing scenarios with each monitoring data source and recorded scenarios data for scenario simulation from monitoring tools, with all relevant event types, from each data sources.

4.2 Results of the exercise 2

The evaluation of the TCDD&EGO exercise in Ankara was conducted with six questionnaires, which were modified from the MdM exercise to fit the Ankara exercise scenario and the exercise programme. In Ankara exercise, the feedback was requested not only from the end-users but also from tool providers related to tools, S4RIS GUI and platform. All the participants were requested to give overall feedback and feedback of the exercise itself. The evaluation target group was enlarged from the first exercise to enable sufficient number of replies for evaluation.

All the participants did not participate in all the exercise phases neither did all the participants give their feedback. Therefore, the number of responses varies between the questionnaires replies in different groups: end-users 7-14 replies, tool providers' 4-12 replies and others 2-4 replies. The answering percentage to evaluation questionnaires has been varying approximately between 25-60%. During the exercise and also after it all participants were requested to complete the questionnaires, even if some aspects would be answered with "no opinion". Where this was done, it was evaluated that the individuals felt they were unable / not suitable to provide an opinion on the content of the particular questionnaire.

The evaluation was conducted according to the D8.1 Evaluation methodology (except adding the tool providers to the questionnaire target groups) and the exercise schedule. The number of questionnaires might have been one factor influencing to the low interest to give feedback as the number of replies decreased from Q1 (30 replies) to Q5 (13 replies). However, there is no confirmation of this view as the number of the participants

varied between the exercise phases and even inside the different phases. There exist no precise numbers for the participants for each phase separately. Another factor could be the way how the exercise was conducted. When people are participating on-line, they might not have the same kind of obligation to reply to surveys as if they were physically present.

The results presented in the following figures are the averages of all the respondents' agreeing level to the questionnaire statements that each tool has received during the resilience phases they have participated during the exercise. Likert-scale answers in questionnaires have been changed to numbers as follows: strongly agree=5, agree=4, neither agree nor disagree=3, disagree=2, strongly disagree=1.

All the tools that participated the Full Joint Scenario Exercise have also been presented during the individual tool demos. Therefore, open-ended questions have not been presented during the Joint Exercise.

Detailed answers to evaluation questionnaires separated to different groups (end-users/tool providers/others) are presented in Annex VI and Annex VII provides an assessment of how far the TCDD&EGO scenario objectives were met based on end-users' evaluation for all resilience phases simulated at TCDD&EGO SE. In ANNEX VI, the answers to open-ended questions are presented original as they were provided.

4.2.1 Prevention phase

In TCDD&EGO exercise feedback for tools performance in prevention phase has been asked in questionnaires1, 2 and 3. Respondents agreeing/satisfaction level to the tools' performance is presented in Figure 11. Answers were given as follows:

- Q1: end-user 14, tool provider 12, other 4
- Q2: end-user 9, tool provider 9, other 2
- Q3: end-user 9, tool provider 7, other 3

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the prevention phase/the decision-making process
- The GUI of the individual tool is user-friendly
- The time for processing was acceptable

During the individual tool demo sessions, the second statement has been "*The output will help for the prevention phase*" and during the functional simulation exercise "*The output will help for the decision-making process*". In Figure 11, these results have been combined.

The statement "*The time for processing was acceptable*" has been presented only during the Full Joint Scenario exercise and therefore that statement is missing from some of the tools that have performed only in the individual tool demos.

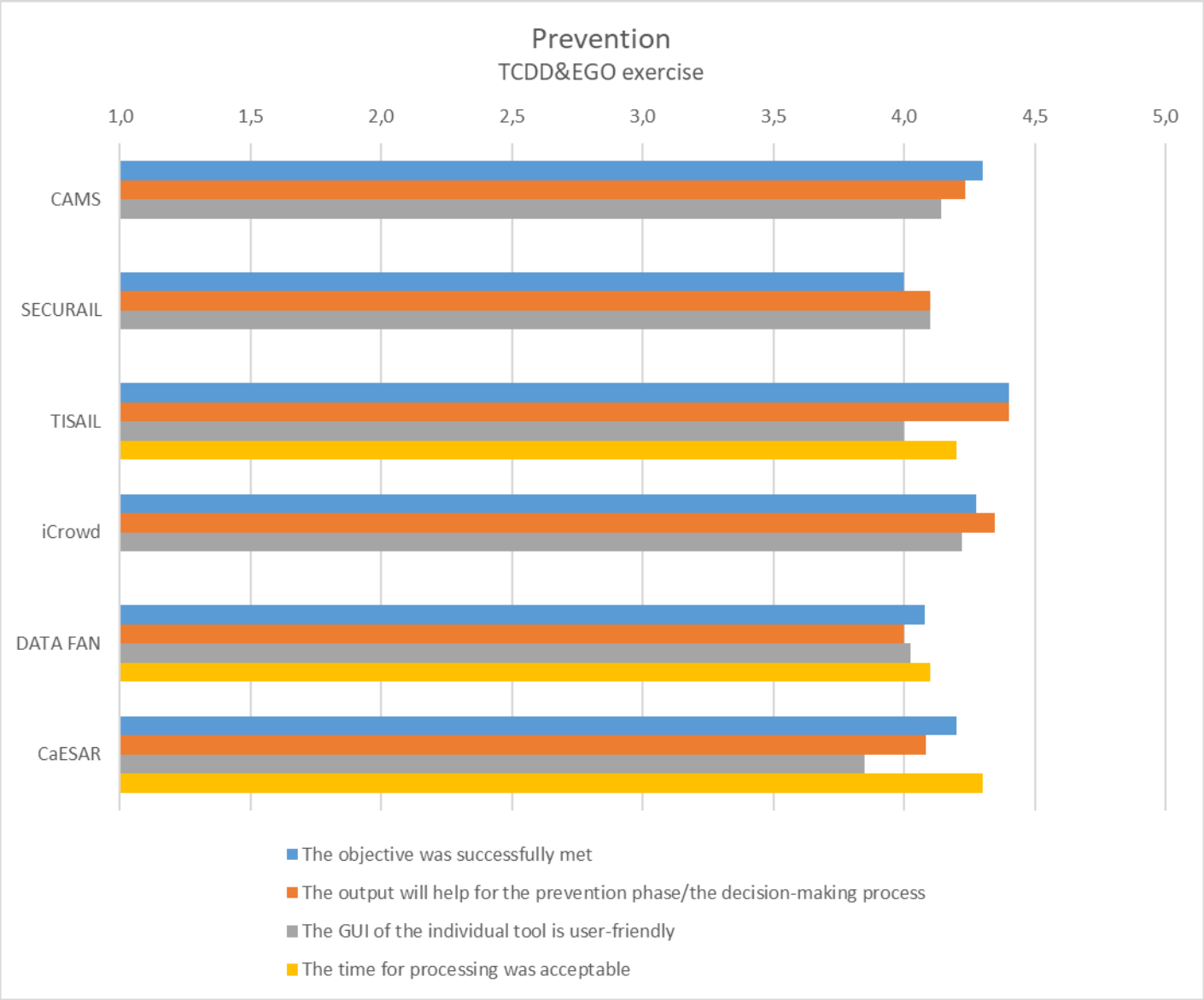


FIGURE 11 TCDD&EGO EXERCISE PREVENTION PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

4.2.2 Detection phase

In TCDD&EGO exercise feedback for tools performance in detection phase has been asked in questionnaires3, 4 and 5. Respondents agreeing/satisfaction level to the tools' performance is presented in Figure 12. Answers were given as follows:

- Q3: end-user 9, tool provider 7, other 3
- Q4: end-user 8, tool provider 6, other 2
- Q5: end-user 7, tool provider 4, other 2

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the detection phase/the decision-making process
- The GUI of the individual tool is user-friendly
- The time for processing was acceptable

During the individual tool demo sessions, the second statement has been "*The output will help for the detection phase*" and during the functional simulation exercise "*The output will help for the decision-making process*". In Figure 12, these results have been combined.

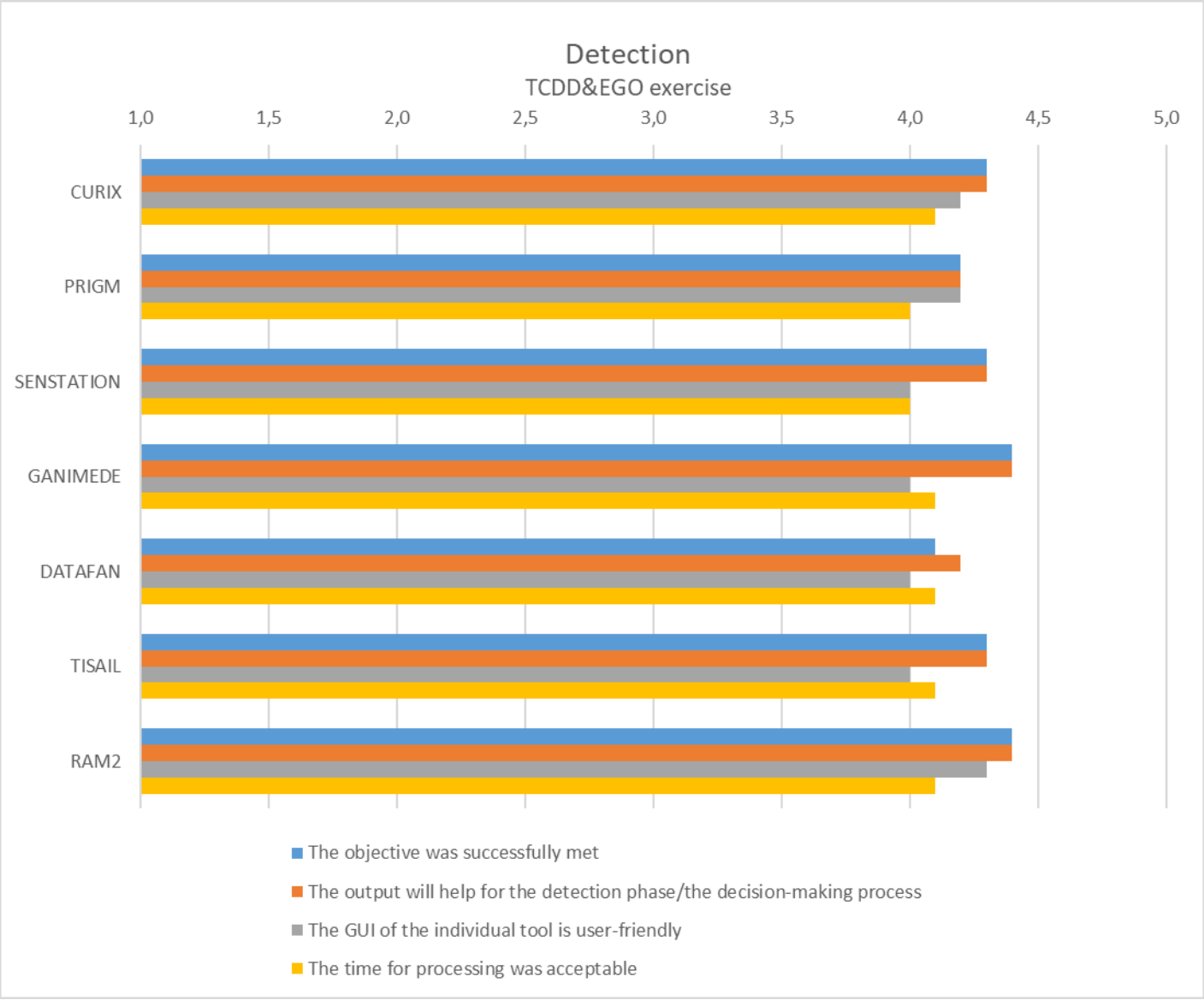


FIGURE 12 TCDD&EGO EXERCISE DETECTION PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

4.2.3 Response phase

In TCDD&EGO exercise feedback for tools performance in response phase has been asked in questionnaires3, 4 and 5. Respondents agreeing/satisfaction level to the tools' performance is presented in Figure 13. Answers were given as follows:

- Q3: end-user 9, tool provider 7, other 3
- Q4: end-user 8, tool provider 6, other 2
- Q5: end-user 7, tool provider 4, other 2

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the response phase/the decision-making process
- The GUI of the individual tool is user-friendly
- The time for processing was acceptable

During the individual tool demo sessions, the second statement has been "*The output will help for the response phase*" and during the functional simulation exercise "*The output will help for the decision-making process*". In Figure 13, these results have been combined.

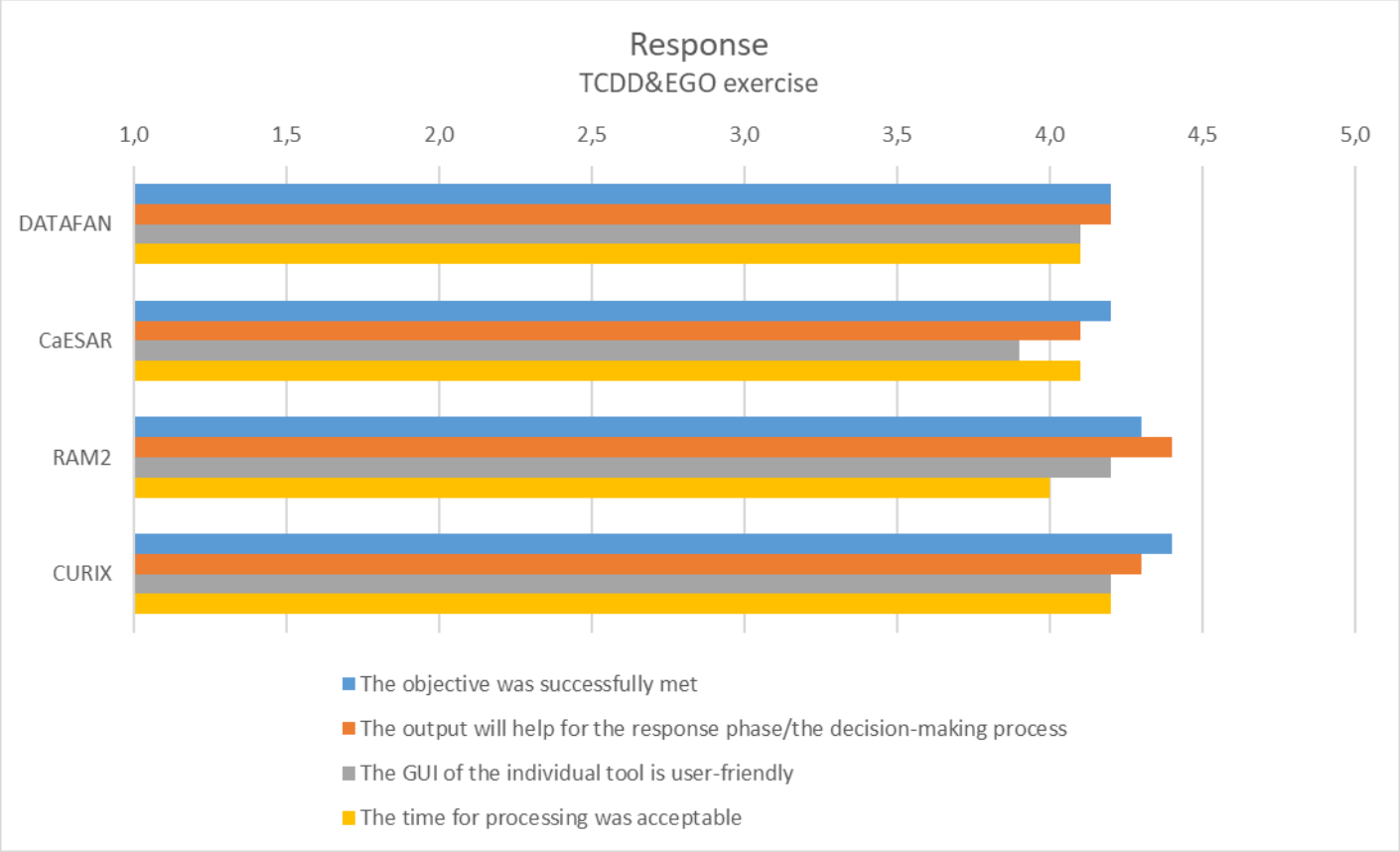


FIGURE 13 TCDD&EGO EXERCISE RESPONSE PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

4.2.4 Recovery phase

In TCDD&EGO exercise feedback for tool's performance in recovery phase has been asked in questionnaire 1. Respondents agreeing/satisfaction level to the tool's performance is presented in Figure 14. Answers were given as follows:

- Q1: end-user 14, tool provider 12, other 4

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the recovery phase
- The GUI of the individual tool is user-friendly

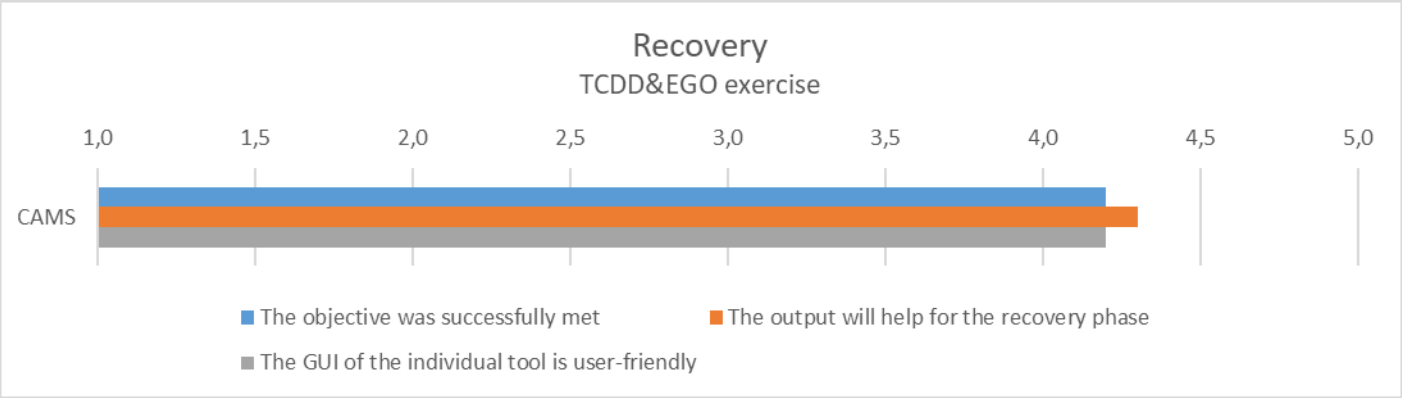


FIGURE 14 TCDD&EGO EXERCISE RECOVERY PHASE – AVERAGE RATE FOR TOOL

4.2.5 S4RIS Graphical User Interface

The feedback exercise's participants have given for S4RIS GUI in Likert-scale statements is presented in Figure 15. Answers were given as follows:

- Q6: end-user 8, tool provider 6, other 4

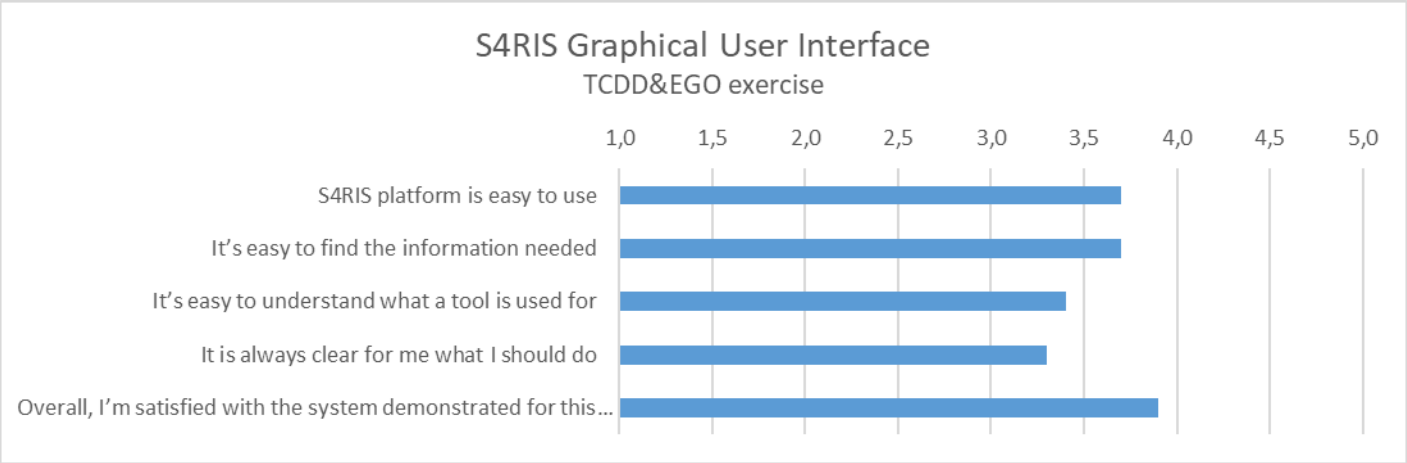


FIGURE 15 TCDD&EGO EXERCISE S4RIS GUI – AVERAGE RATES FOR STATEMENTS

4.2.6 S4RIS platform

The feedback exercise's participants have given for S4RIS platform in Likert-scale statements is presented in Figure 16. Answers were given as follows:

- Q6: end-user 8, tool provider 6, other 4

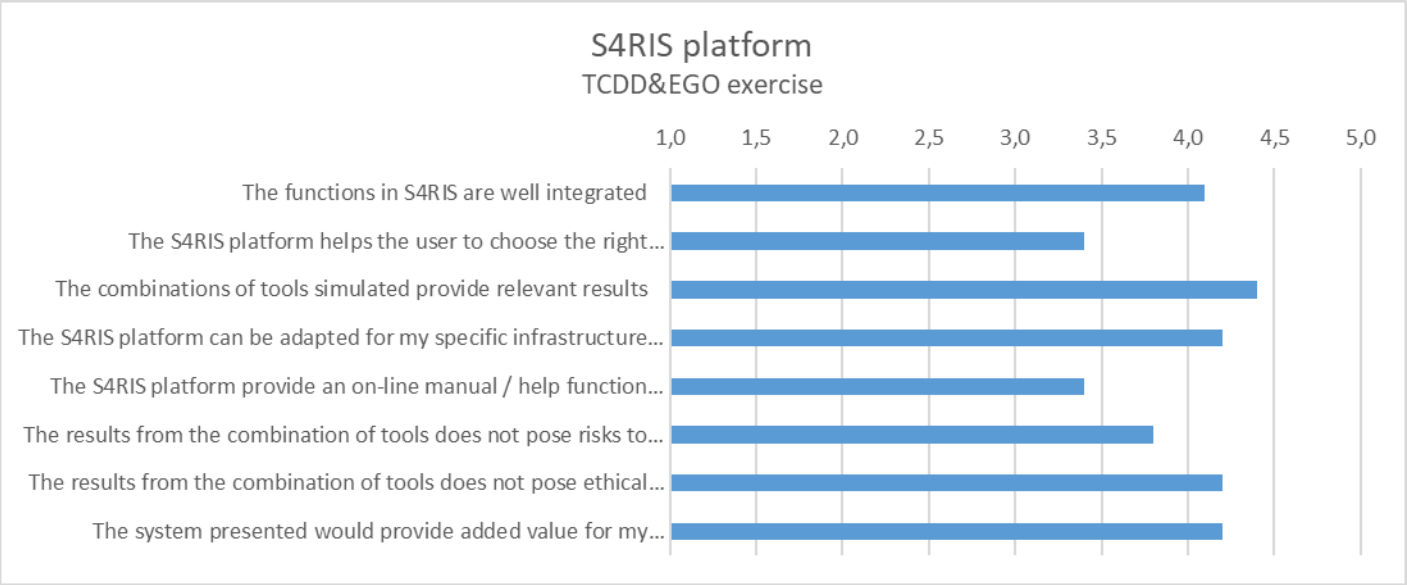


FIGURE 16 TCDD&EGO EXERCISE S4RIS PLATFORM – AVERAGE RATES FOR STATEMENTS

The response to the statement "*The S4RIS platform provides an on-line manual / help function that is easy to understand*" is misleading. No on-line manuals or help functions were presented. In questionnaire an option "No opinion" was offered for such a case when respondent is not able to answer, but only 4/16 respondent has chosen that.

4.2.7 TCDD&EGO exercise evaluation

The feedback exercise's participants have given for the exercise in Likert-scale statements is presented in Figure 17. Answers were given as follows:

- Q6: end-user 8, tool provider 6, other 4

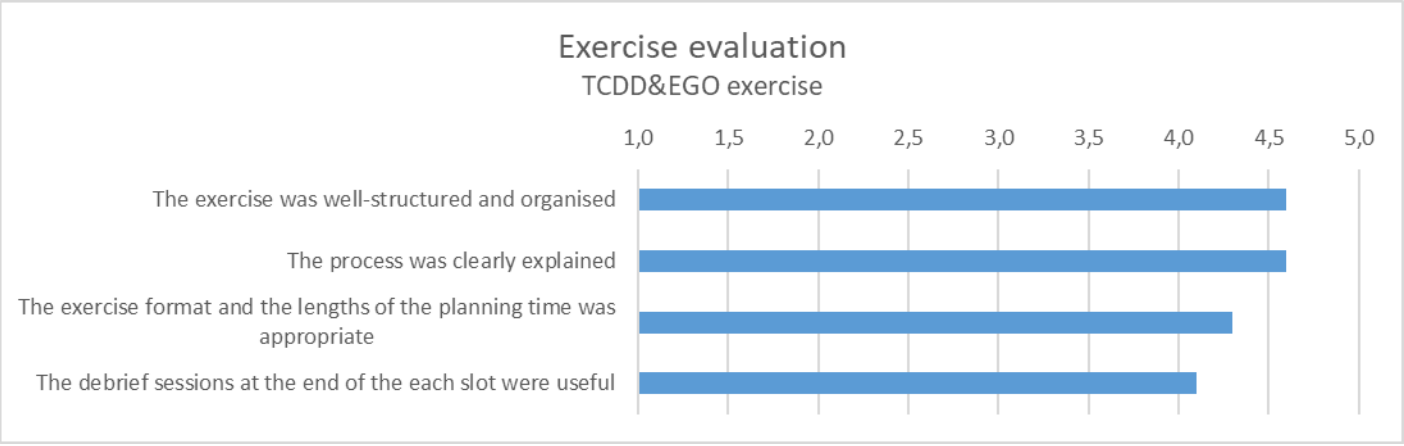


FIGURE 17 TCDD&EGO EXERCISE EVALUATION – AVERAGE RATES FOR STATEMENTS

4.2.8 Overall questions

The feedback exercise's participants have given overall for S4RIS in Likert-scale statements is presented in Figure 18. Answers were given as follows:

- Q6: end-user 8, tool provider 6, other 4

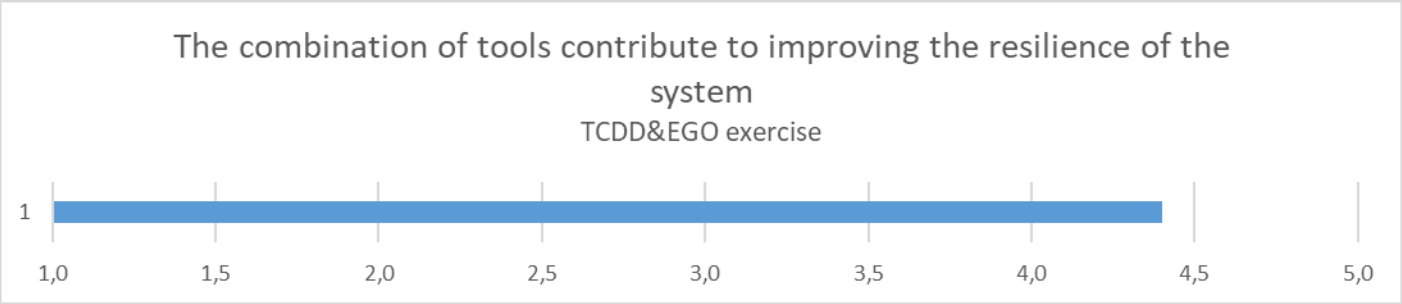


FIGURE 18 TCDD&EGO EXERCISE OVERALL FEEDBACK OF S4RIS – AVERAGE RATE FOR STATEMENT

4.3 Analysis of the results of the exercise 2

Background

The TCDD&EGO simulation exercise was the second simulation exercise and focused on Physical attack – Potential terrorist attack via IED carried via baggage, Physical attack – Intrusion and bomb planted and Physical Attack – Intrusion in Sensitive Place. The use cases included Cyber – Physical attack against the railway system. It addressed four resilience phases: prevention, detection, response and recovery. Eleven tools and some of their capacities have been demonstrated successfully, with 18 objectives tested (Annex VII) and evaluated by 7-14 end-users, 4-12 tool providers and 2-4 other participants.

Functional evaluation analysis

The overall impression by the respondents to the tools tested during the exercise has been mainly positive and the objectives set for the tools in different resilience phases were met.The respondents'average satisfaction rate (answers to Likert scale questions changed to numbers strongly agree=5…strongly disagree=1) in different resilience phases to how the tools have met the tools' objectives, their outputs, time for processing and GUIs has varied between 4.1-4.3 (rating from 1 to 5). The capabilities of the tools, which have been mostly appreciated during the exercise based on the answers to open-ended questionsare risk management, situational awareness, decision-making support, in financial planning and automatic information collection from several sources. Detailed answers to the open-ended questions and Likert-scale questions are available in Annex VI. Answers to open-ended questions are presented original as they were provided.

From a functional point of view, no request for revising the requirements were raised by the end-users.

Main benefits of the tools highlighted by the responders when answering the open questions of the questionnaires (available in Annex VI) are the following:

- The demonstrated simulation capacities (CAMS, iCrowd, SECURAIL, CAESAR, DATAFAN) bring a lot of added value for managing cyber and physical risks and helping decision makers on the measures to be put in place to make metro systems more resilient. Beyond the benefits already highlighted in the MDM simulation exercises, the following additional ones can be cited:
    - The organised structure of the information regarding the assets of a company combined with the simulation capabilities can **help asset owners to make best monitoring and maintenance decisions.**
    - Simulation capabilities can support the operators for a **better estimation of needed times or expected delays when managing the crowd.**
    - Off-line risk analysis to understand the level of risk for each critical asset during a given hazardous event can **help to perform a cost benefit analysis** of the infrastructure for different events.
    - The strong simulation-based computation model may help decision makers to **understand the transportation dynamics and potential cascading effects at city scale**.

- The detection tools (TISAIL, PRIGM, SENSTATION, CURIX, GANIMEDE, DATAFAN) which demonstrated early detection of anomalies or vulnerabilities were appreciated by some of the responders for **anticipating situation and preventing or mitigating the consequences of cyber and physical attacks.**

- The integration and the processing of the alerts (RAM2) which provided the end-user with **a comprehensive overview of the situation**.

The main possible improvements that were mentioned by some of the participants are as follows:

- For some of the tools, the GUI could be improved to make it simpler for the end-users, several languages should be available.
- More tests in different conditions and different sets of data would be needed to better evaluate the tools and their capabilities. Real data would also be very useful, but they are difficult to obtain due to their sensitivity and data regulation.
- There are still some tools which are not integrated in the S4RIS platform.

Regarding the S4RIS GUI, main improvements highlighted are as follows:

- Purpose of each tool and their connections should be clearly informed.
- The GUI could be adapted for different user profiles.
- One login should be enough to get to the different tools.
- User guide would be needed.

Overall, the respondents valued most the developing integration between the different information sources and systems as well as detection capabilities.

As obstacles were mentioned current habits and working methods (resistance to change), financial issues, data availability and privacy, lack of standards for data and communication and integration into existing IT-systems.

Analysis of the organisation of the exercise and recommendations for the remaining exercises

The organisation of the exercise was well rated by the responders (Figure 17).

The following recommendations were given for the organisation of the remaining two exercises:

- The remaining exercises should be face to face with more interactions between the participants and the tool providers.
- The technical explanations of the tools could be shorter and focus more on the scenario and the information that would be useful for the end-user.
- Most useful parts of the exercises that were cited are the full joint scenario exercise and the demonstration of the S4RIS platform which give an overview of how the system will look at the end of the project and how all the demonstrated tools will work together in a threat scenario.
- More end-users representatives and stakeholders involved in a crisis such as police authorities should be participating in the simulation exercise.

Analysis of the Evaluation methodology and recommendations for the remaining exercises

The evaluation methodology was adapted after MDM simulation exercise feedback. No major recommendations were received during this second simulation exercise.

Main challenges encountered when filling the questionnaire is

- The scope of the simulation exercise is very large and each responder can only address part of questions.
- It is very hard to follow so many tools in a short period of time. It was suggested by one of the responders to do questionnaires right after each tool to get more clear answers.
- Experiencing the tool(s) for a while would be needed to make a better evaluation.

5. Exercise 3 (Rome Italy; RFI)

This section describes the Rome (RFI) exercise results and how the methodology was applied to it. In short, the S4RIS and the contributory tools included in the Rome exercise based on their development status at that time were successfully demonstrated

5.1 Use scenario summary and S4RIS capabilities tested

The RFI Simulation Exercise scenario was based on UC-003, *Physical Attack – Terrorist Attack using Firearms inside a Railway Station* and UC-004, *Physical attack – Potential terrorist attack via IED carried via baggage*, which are in detail described in S4RIS deliverable D8.3. The Use scenario included also a cyber-attack.

Based on the experience from the previous two exercises the evaluation system was changed so that the evaluation questions were sent to Rome exercise participants beforehand. Moreover, for having more relevant feedback all participants were asked to answer to all questions and the results were categorised by the evaluators afterwards.

Altogether four debrief sessions were conducted, one after each three individual tool demonstration sessions and one after the full joint scenario exercise. After the fourth and final survey followed an open discussion session where participants were asked to provide oral feedback on S4RIS and exercise arrangements. The exercise schedule is presented in Annex VIII.

The exercise was organised so that in the first three sessions the participating tools and their contribution and input for the exercise were presented tool by tool. SAFETY4RAILS Information System (S4RIS) graphical user interface (GUI) was presented in session three and therefore evaluated in questionnaire #3.

During the fourth session the tools functionalities were combined in the same scenario framework. The questionnaire of the fourth session included questions about the tools participating in the exercise scenario but also platform specific questions, exercise evaluation questions and overall questions.

For a full schedule of the simulation exercise, please refer to ANNEX VIII Rome (RFI) exercise schedule.

This arrangement provided for the RFI exercise participants the possibility to evaluate all the tools used in the exercise. Table 4 presents the tools involved to SE and to which phase each tool were involved.

TABLE 4 TOOLS INVOLVED IN SIMULATION EXERCISE 3

PREVENTION	DETECTION	RESPONSE	RECOVERY
CaESAR	GANIMEDE	DATAFAN	CAMS
DATAFAN	RAM2	CaESAR	
TILSAIL/OSINT	Curix	RAM2	
RAM2	WINGSPARK	WINGSPARK	

The participating tools and their objectives in RFI exercise according to D8.3 were:

- **GANIMEDE (LDO)**: The objectives were: 1) the analysis of an audio stream searching for relevant patterns in the context of safety and security (a shot in this case); 2) the detection of objects and people in each frame and their movement to determine if the object is candidate for abandon; 3) the ability of recognizing people based on the clothes they are wearing.
- **CaESAR (Fraunhofer)** demonstrated the GUI and functionality of the tool. The tool demonstrated features including 1) Criticality analysis of the network 2) Offline analysis using What-If scenarios. 3) Resilience assessment and impact propagation in the network. 4) Quantification of performance of different mitigation measures. Further, it aimed to receive feedback from end-users about the functionality and potential improvements/enhancements of the tool and GUI.

- **DATAFAN (Fraunhofer):** The main objective was to verify whether the predicted number of passengers for the Termini Railway Station in Rome could be used for an effective and well-informed passenger redistribution during the incident. To this end, a GUI for analysing and visualizing the passenger data was provided and its functionality was evaluated. In addition, the tool provided a reliability analysis to help the end-user in the decision-making process and to support itstechnology acceptance, which was tested in the new scenario.
- **TSAIL (TREE):** The objective of TISAIL was to provide useful insights for the security team. The information provided by TISAIL was tohelp the security team to raise the security awareness of the whole organisation and to update their defence mechanisms.
- **RAM2 (ELBIT):** As Decision Support tool monitored events during the Simulation Exercise raising alarms received from tools (together with CuriX) and displaying related Mitigation Actions.
- **CAMS (RMIT):** The main objective was to test features of CAMS to provide accurate recovery cost for assets involved in a sudden event through the assessment of final assets damage. The final damage was assessed using the initial condition (before incident) and the impact measure of the specific incident on the asset**.**
- **WINGSPARK (WINGS):** The objective of WINGSPARK wasto forward the relative alerts to RA^{M2} in case the specified thresholds have been exceeded and provide evacuation guidelines to ease the situation.
- **CURIX (CuriX):** The objective was to show the identified anomalies in the monitoring data that indicate a DoS for the CCTV system in the CuriX dashboard and to forward it

5.2 Results of the exercise 3

The evaluation of the RFI exercise in Rome was conducted with four questionnaires modified further from the exercises in Madrid and Ankara to fit the Rome exercise scenario and the exercise programme. In Rome exercise, the feedback was requested from all the participants to all the questionnaires including tools, S4RIS GUI and platform, exercise itself and overall questions about the S4RIS.

Not all the participants participated in all the exercise phases nor did all the participants gave her/his feedback. Therefore, the number of responses varies between the questionnaires replies in different groups: end-users 2-4 replies, tool providers' 4-9 replies and others 7-11 replies. Around 50 participants participated in the exercise (around 50% physically and 50% remote) so the answering percent to evaluation questionnaires has varied approximately between 28-48%.

The evaluation was conducted according to the D8.1 Evaluation methodology (except adding all the participants to the questionnaire target groups) and the exercise schedule. One factor for low interest to give feedback has obviously been the way how people have participated to the exercise. Of all the participants who have been physically present in the exercise 63% have answered at least one questionnaire while of those who participated remotely only 26% has given feedback at least in one survey. When people are participating on-line, they seem not have the same kind of obligation to reply to surveys as if they were physically present.

The results presented in the following figures are the averages of all the respondents' agreeing level to the questionnaire statements that each tool has received during the resilience phases they have participated during the exercise. Likert-scale answers in questionnaires have been changed to numbers as follows: strongly agree=5, agree=4, neither agree nor disagree=3, disagree=2, strongly disagree=1.

All the tools that participated in the Joint Tools Simulation Exercise have also been presented during the individual tool demos, except RAM2. Therefore, open-ended questions have not been presented during the Joint Exercise.

Detailed answers to evaluation questionnaires separated into different groups (end-users/tool providers/others) are presented in Annex IX and Annex X provides an assessment of how far the RFI scenario objectives were met based on end-users' evaluation for all resilience phases simulated at RFI SE. In ANNEX IX, the answers to open-ended questions are unfiltered.

5.2.1 Prevention phase

In RFI exercise feedback for tools performance in prevention phase has been asked in questionnaire 1. Respondents agreeing/satisfaction level to the tools' performance is presented in Figure 19. Answers were given as follows:

- Q1: end-user 2, tool provider 6, other 9

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the prevention phase
- The GUI of the individual tool is user-friendly

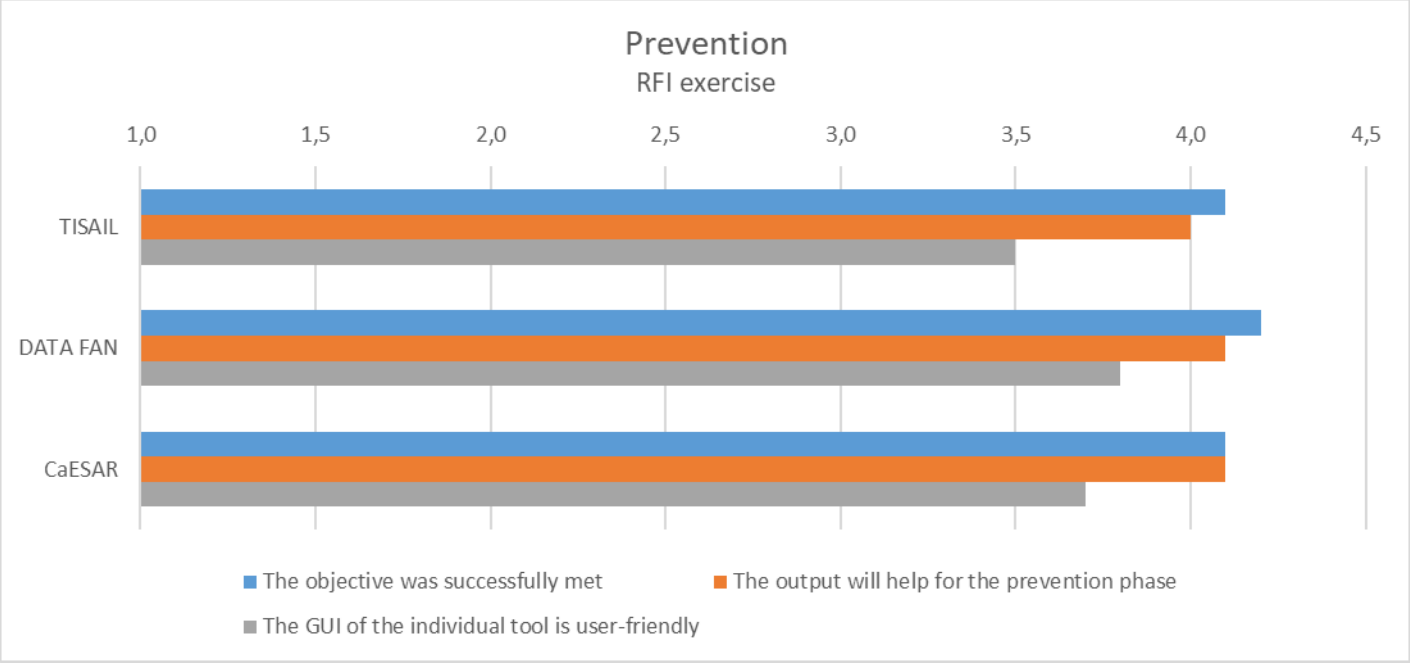


FIGURE 19 RFI EXERCISE PREVENTION PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

5.2.2 Detection phase

In RFI exercise feedback for tools performance in detection phase has been asked in questionnaires2, 3 and 4. Respondents agreeing/satisfaction level to the tools' performance is presented in Figure 20. Answers were given as follows:

- Q2: end-user 3, tool provider 4, other 7
- Q3: end-user 4, tool provider 9, other 11
- Q4: end-user 4, tool provider 5, other 7

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the detection phase/the decision-making process
- The GUI of the individual tool is user-friendly
- The time for processing was acceptable

During the individual tool demo sessions, the second statement has been "*The output will help for the detection phase*" and during the functional simulation exercise "*The output will help for the decision-making process*". In Figure 20, these results have been combined.

The statement "*The time for processing was acceptable*" has been presented only during the Full Joint Scenario exercise and therefore that statement is missing from some of the tools that have performed only in the individual tool demosin this resilience phase.

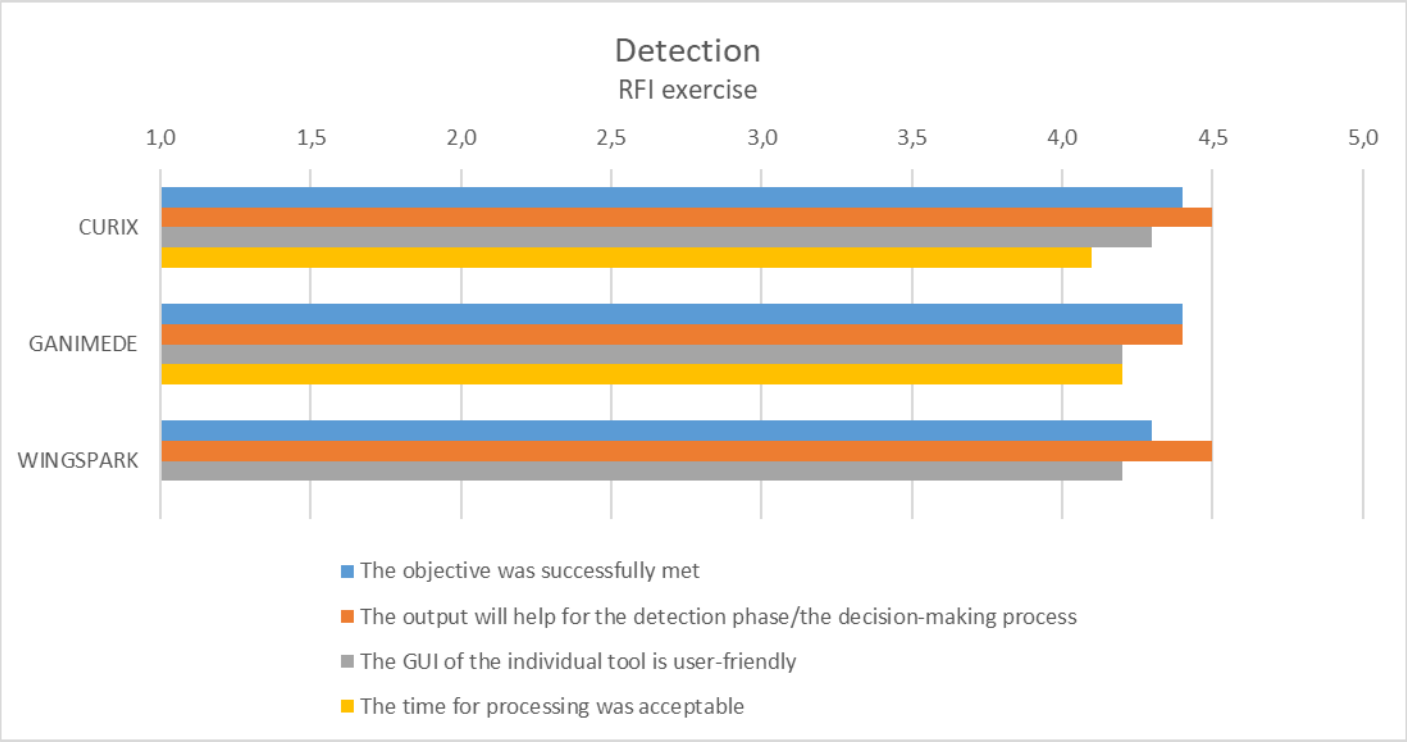


FIGURE 20 RFI EXERCISE DETECTION PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

WINGSPARK tool does not have valuation of *Time for processing was acceptable* in the figure above. Wingspark had only one objective for the combined detection & response phase. Based on the exercise scenario Wingspark function has been more in response and therefore this evaluation is presented in response phase figure.

5.2.3 Response phase

In RFI exercise feedback on tools performance in the response phase has been asked in questionnaires1, 3 and 4. Respondents agreeing/satisfaction level to the tools' performance is presented in Figure 21. Answers were given as follows:

- Q1: end-user 2, tool provider 6, other 9
- Q3: end-user 2, tool provider 9, other 11
- Q4: end-user 4, tool provider 5, other 7

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the response phase/the decision-making process
- The GUI of the individual tool is user-friendly
- The time for processing was acceptable

During the individual tool demo sessions, the second statement has been "*The output will help for the response phase*" and during the functional simulation exercise "*The output will help for the decision-making process*". In Figure 21, these results have been combined.

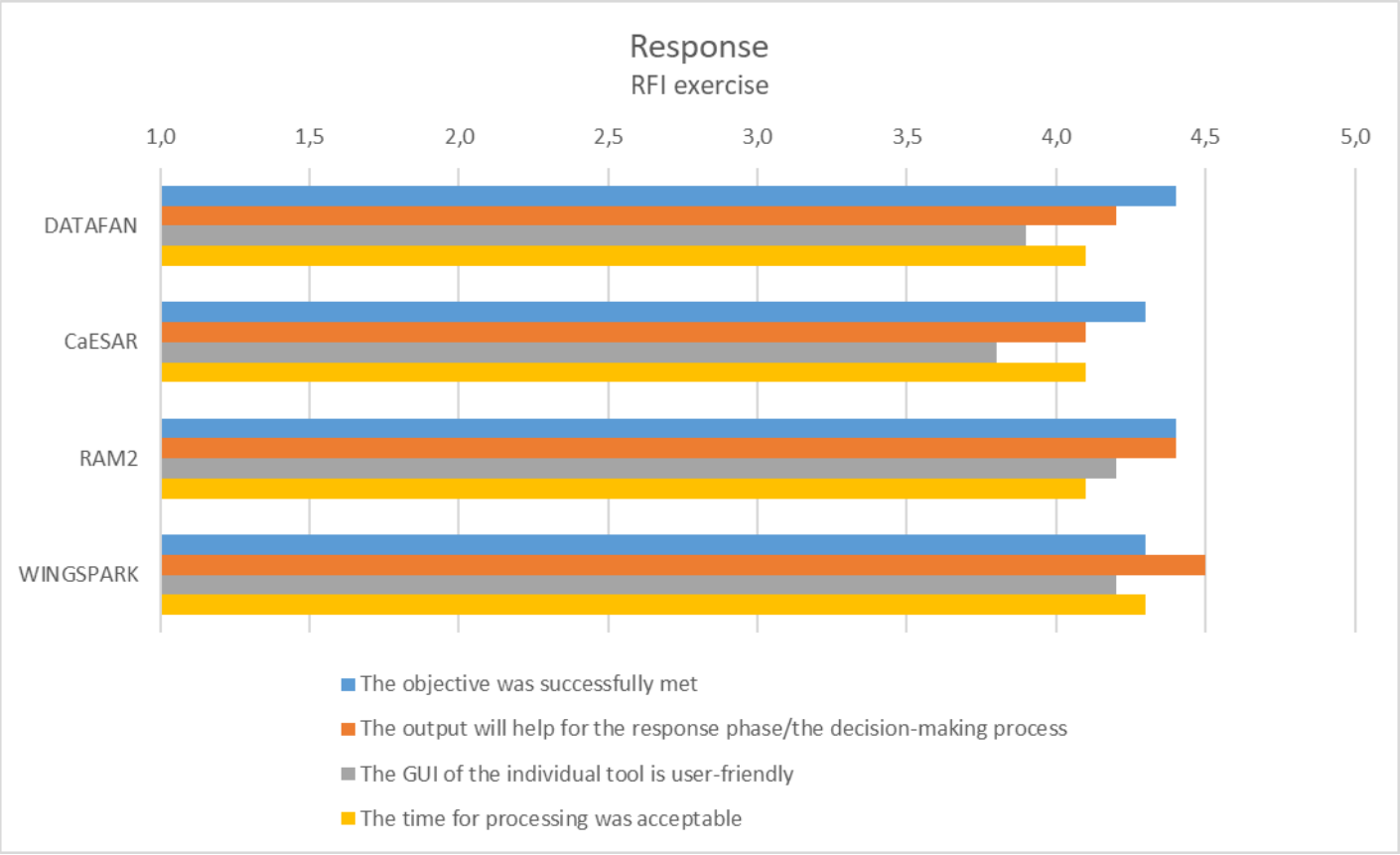


FIGURE 21 RFI EXERCISE RESPONSE PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

5.2.4 Recovery phase

In RFI exercise feedback for tool's performance in recovery phase has been asked in questionnaire3. Respondents agreeing/satisfaction level to the tool's performance is presented in Figure 22. Answers were given as follows:

- Q3: end-user 4, tool provider 9, other 11

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the recovery phase
- The GUI of the individual tool is user-friendly

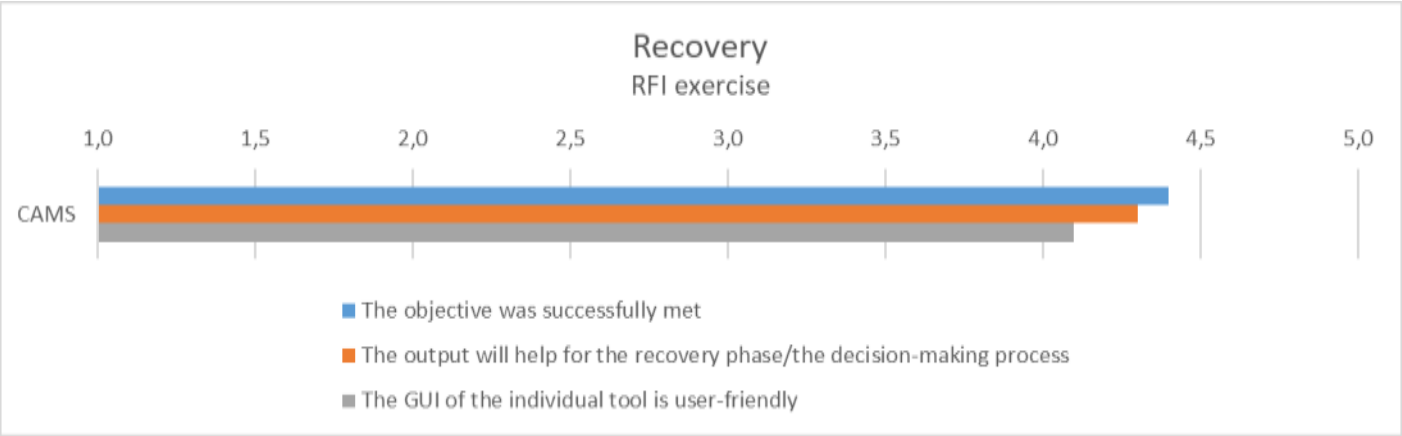


FIGURE 22 RFI EXERCISE RECOVERY PHASE – AVERAGE RATE FOR TOOL

5.2.5 S4RIS Graphical User Interface

The feedback exercise's participants have given for S4RIS GUI in Likert-scale statements is presented in Figure 23. Answers were given as follows:

- Q3: end-user 4, tool provider 9, other 11

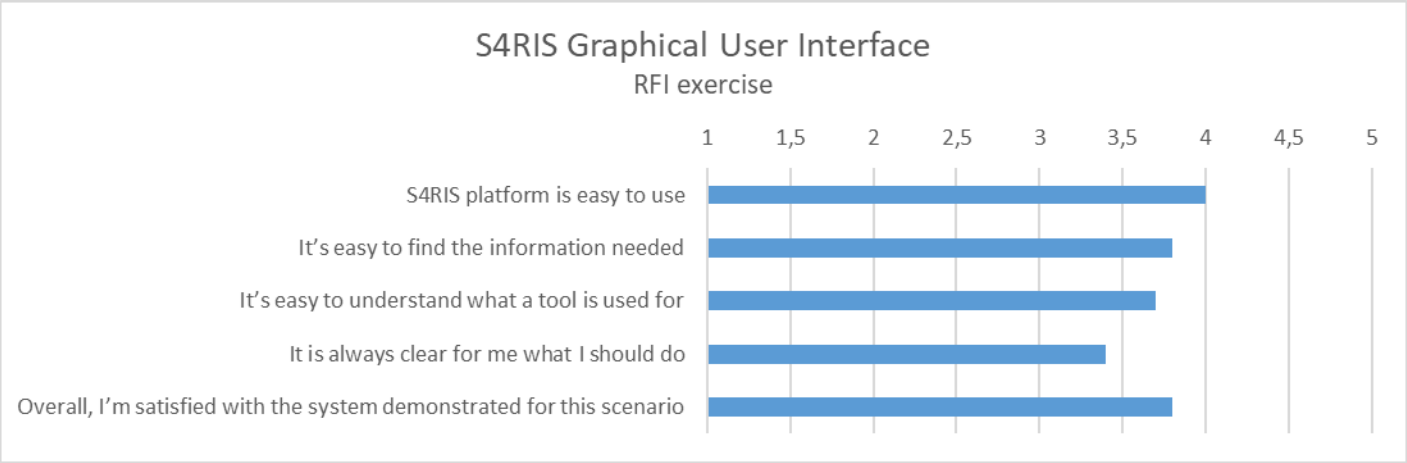


FIGURE 23 RFI EXERCISE S4RIS GUI – AVERAGE RATES FOR STATEMENTS

5.2.6 S4RIS platform

The feedback exercise's participants have given for S4RIS platform in Likert-scale statements is presented in Figure 24. Answers were given as follows:

- Q4: end-user 4, tool provider 5, other 7

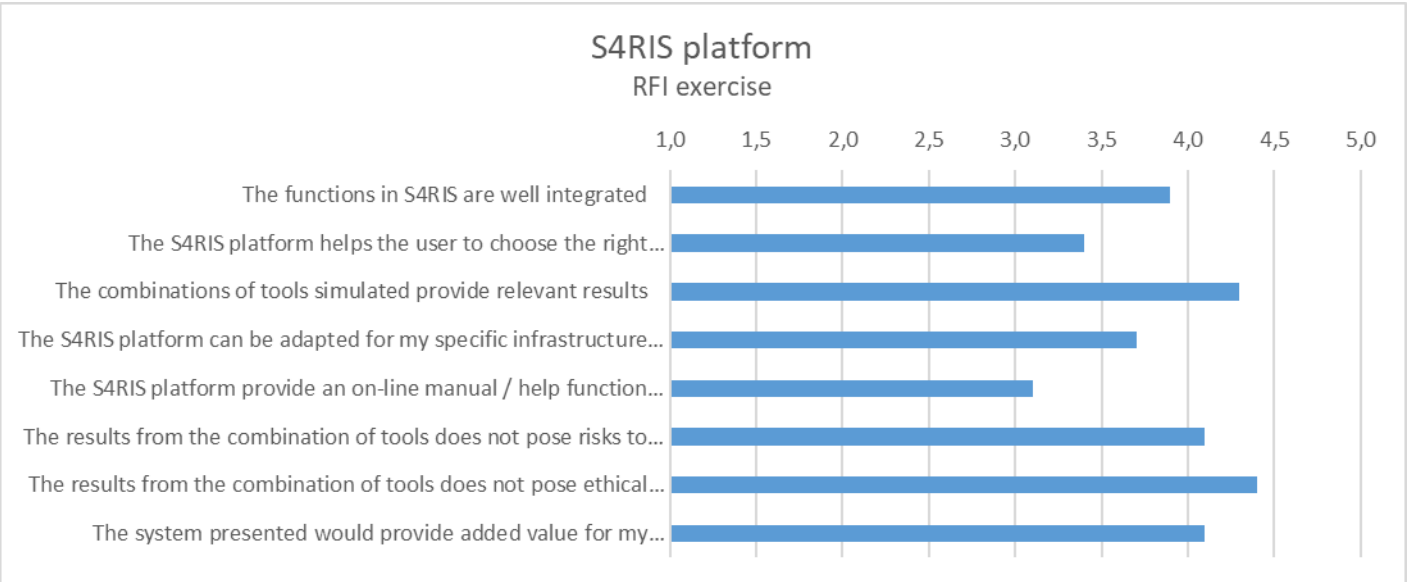


FIGURE 24 RFI EXERCISE S4RIS PLATFORM – AVERAGE RATES FOR STATEMENTS

The response to the statement "*The S4RIS platform provides an on-line manual / help function which is easy to understand*" is misleading. No on-line manuals or help functions were presented. In questionnaire an option "No opinion" was offered for such a case when respondent is not able to answer, but only 5/16 respondent has chosen that.

5.2.7 RFI exercise evaluation

The feedback exercise's participants have given for the exercise in Likert-scale statements is presented in Figure 25. Answers were given as follows:

- Q4: end-user 4, tool provider 5, other 7

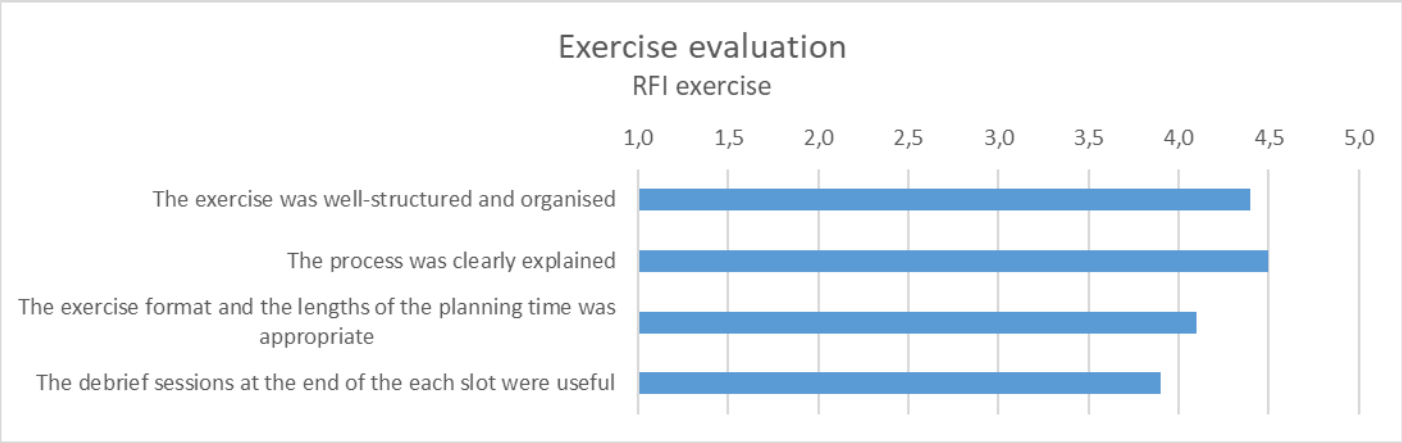


FIGURE 25 RFI EXERCISE EVALUATION – AVERAGE RATES FOR STATEMENTS

5.2.8 Overall questions

The feedback exercise's participants have given overall for S4RIS in Likert-scale statements is presented in Figure 26. Answers were given as follows:

- Q4: end-user 4, tool provider 5, other 7

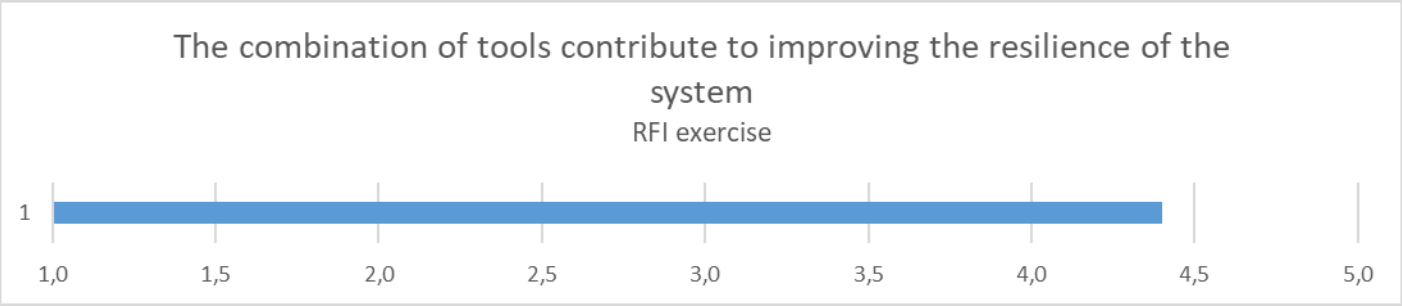


FIGURE 26 RFI EXERCISE OVERALL FEEDBACK OF S4RIS – AVERAGE RATE FOR STATEMENT

5.3 Analysis of the results of the exercise 3

Background

The RFI simulation exercise was the third simulation exercise and focused on Physical Attack – Terrorist Attack using Firearms inside a Railway Station and UC-004, Physical attack – Potential terrorist attack via IED carried via baggage, in the railway environment. The use-case scenario also included a cyber-attack. It addressed four resilience phases: prevention, detection, response and recovery. Eight tools and some of their capacities have been demonstrated successfully, with 17 objectives tested (Annex IX) and evaluated by 2-4 end-users, 4-9 tool providers and 7-11 other participants.

Functional evaluation analysis

The respondents have mainly been satisfied withthe tools' functionalities presented during the RFI exercise. The respondents' average satisfaction rate (answers to Likert scale questions changed to numbers strongly agree=5…strongly disagree=1) in different resilience phases to how the tools have met the tools' objectives, their outputs, time for processing and GUIs has varied between 3.7-4.4 (rating from 1 to 5).

From a functional point of view, no request for revising the requirements were raised by the end-users.

Main benefits of the tools highlighted by some of the responders when answering the open-ended questions of the questionnaires (available in Annex IX) are the following:

- For simulation and prediction tools (CaESAR, DATAFAN, CAMS)
  - Improving situational awareness and get information such as on critical nodes but also passengers' numbers and free capacities of interconnected infrastructures.
  - Be better prepared in case of an attack by studying different simulations.
  - Data based decision making which will make acceptability much higher.
  - Automated and real time check of the health of the system and its components
  - Recovery Cost estimation
- For detection tools (TISAIL, CURIX, GANIMEDE, WINGS)
  - Detection of vulnerabilities in CCTV and DVR systems.
  - Overview and control of IT systems and/or sensors.
  - Early detection of anomalies, suspicious situation and behaviour (e.g. audio detection, abandoned luggage, crowd concentration) and making guards or similar aware of it.

Again, the joint simulation exercise was seen beneficial because numerous tools were seen interacting.

The main possible improvements are very similar to those highlighted in the Ankara simulation exercises regarding GUIs of some of the tools, provision of additional data and integration of more tools.

Many improvements were implemented on the GUI since the last exercise, there were still suggestions from some responders to further improve it, e.g.

- Explanation of different tools and when to use those.
- User guidance / online manual.
- The link to the GUI should be provided to the partners to be able to test it and give more feedback.

Analysis of the organisation of the exercise and recommendations for the remaining exercises

The organisation of the exercise was well rated by the responders (Figure 25).

The following recommendations were given for the organisation of the remaining Milan exercise:

- More focus on the joint exercise and the mitigation measures with the possibility to look at the details in the individual tool that has provided the alert.
- More end-users' representatives should be participating in the simulation exercise and more discussions should be held.
- It was again highlighted that more complete set of real data should be provided: as stated in the Ankara exercise, these data are very sensitive for railways, therefore open data or artificial data may be used.
- More explanation needed on the messaging system.
- It would have been nice to have further tools involved in the joint exercise.

Analysis of the Evaluation methodology and recommendations for the remaining exercises

The feedback was minimal, and participants were happy with the evaluation methodology.

6. Exercise 4 (Milan Italy; CdM)

This section describes the Milan (CdM) exercise and how the methodology was applied to it. In short, the S4RIS and the contributory tools included in the CdM exercise based on their development status at that time were successfully demonstrated.

6.1 Use scenario summary and S4RIS capabilities tested

In the CdM Simulation Exercise, the S4RIS and a selection of contributory tools were tested in a scenario based on UC-001 *Natural Disaster – Flooding*, which is described in deliverable D8.3. The UC-001 was co-designed with Comune di Milano and was different in respect to the use cases that were the basis of the previous exercises as it was based on a natural incident.

In this scenario, a sudden storm hit the city of Milan at the time of the opening ceremony of the 2026 Winter Olympic Games.The torrential rain caused several floods in the city and the overflow of the Seveso River that floods several stations of the metro line M5 in the northern area of the city. This scenario consequentially created great inconvenience especially in the area of the station of Milan Porta Garibaldi. The two subway lines were shut down, as were most of the rail connections, and this had severe repercussions for vehicular traffic and surface transportation. In addition, one of the two interrupted lines (the M5 metro) was the one that should take spectators and non-spectators to the San Siro Stadium for the opening event. The unpredictable situation caused the almost total blockage of traffic in the northern part of the city, bringing to its knees not only the area but also the smooth running of the event. Table 5 presents the tools involved in the SE and to which phase each tool were involved.

TABLE 5 TOOLS INVOLVED IN SIMULATION EXERCISE 4

PREVENTION	DETECTION	RESPONSE	RECOVERY
CaESAR SECURAIL DATAFAN SARA	CuriX WINGSPARK	RAM2 CaESAR WINGSPARK	CAMS

The objectives for each tools according to D8.3 were as follows:

- **S4RIS GUI**: In respect to the previous Simulation Exercise, the tools involved in this SE were activated through the S4RIS GUI (where implemented). Another improvement was that the tools sent the relevant JSON messages directly to the DMS, while in previous SE this was simulated using a script.
- **CaESAR (Fraunhofer)**: aimed to demonstrate the GUI and functionality of the tool using this exercise (as also mentioned in the section 5.1). The tool also demonstrated the integration with the S4RIS GUI and overall Distributed Messaging System (DMS) platform in a live environment. Further, it aimed to receive feedback from end-users about the functionality and potential improvements/enhancements of the tool and GUI. Especially, feedback wasrequestedabout the mitigation options under consideration.
- **DATAFAN (Fraunhofer):** The main objective was to verify whether the predicted number of passengers for the Milan Porta Garibaldiand its surrounding stations could be used for an effective and well-informed passenger redistribution during the flooding incident.
- **SARA (RINA_C)**: aimed to analyse the station from a security point of view, with reference to the individual equipment (e.g., ventilation, communication, power supply, etc.).
- **RAM2 (ELBIT):** as Decision Support tool monitoredthe events during the Simulation Exercise raising alarms received from tools (together with Curix) and displaying related Mitigation Actions
- **CAMS (RMIT):** A major objective of CAMS in the context of the simulation exercise was to test the friendliness of the user interface and introduce new features following below:
    - Predicting normal deterioration of railway/subway assets due to age or damage.
    - Budget calculations for railway/subway maintenance and repair.
    - Asset analysis and deterioration during extreme hazard conditions.

The simulation exercises enabled End-users to identify strong and weak points and gain suggestions based on their viewpoint.

- **WINGSPARK (WINGS):** The objective of WINGSPARK was to take as input train speed data simulated as coming from IoT devices (sensors) and to trigger specified alerts when an abnormal behaviour was detected. In addition, it was for WINGSPARK to detect overcrowded situations in the monitored railway infrastructure, based on video acquired through CCTV cameras. Then, during the response phase, the objective was to forward the relative alerts RAM^2 in case the specified thresholds have been exceeded and to propose dynamic evacuation plans to ease the situation.

- **SECURAIL (STAM):** This Simulation Exercise enable first testing ofSecuRail improved functionalities that wereimplemented in itsfinal release. For this purpose, SecuRailwas used to carry out a risk analysis of the network infrastructure under examination within this Simulation Exercise. Moreover, in this simulation, the dashboard, which displays all the relevant information concerning the results of the risk computation in an aggregated way, was presented.

- **CuriX (CuriX):** The objective was to show the identified anomaly in the monitoring data that indicates a blackout for the electrical power supply of the Porta Garibaldi station in the CuriX dashboard. The GUI and functionalities of CuriXwere explained, and general feedback regarding the user-friendliness of the CuriX dashboard was appreciated.

Three questionnaires were organised during the Milan Simulation Exercise. Questionnaires one and three were related to individual tool demos and the questionnaire two was based on the Full Joint Scenario exercise. In this evaluation, the Full Joint Scenario questionnaire included also open-ended questions because it included tools that was not introduced in individual tool demos.

For a full schedule of the simulation exercise, please refer to ANNEX XI Milan (CdM) exercise schedule.

6.2 Results of the exercise 4

The evaluation of the CdM exercise in Milan was conducted with three questionnaires modified from the former exercise evaluation questionnaires in Madrid, Ankara and Rome to fit the Milan exercise scenario and the exercise programme. In Milan exercise, the feedback was requested from all the participants to all the questionnaires including tools, S4RIS GUI and platform, exercise itself and overall questions about the S4RIS.

As the actual exercise took place in one day the number of responses did not vary significantly between the questionnaires replies in different groups: end-users 3-6 replies, tool providers' 14 replies and others 6-7 replies. Around 56 participants participated in the exercise so the answering percent to evaluation questionnaires has been approximately 45%.

The evaluation was conducted according to the D8.1 Evaluation methodology (except adding all the participants to the questionnaire target groups) and the exercise schedule. As well as in RFI exercise in Rome one factor for low interest to give feedback has been the way how people have participated to the exercise. Based on the attandees' list, which is though indicative at most, of all the participants who have been physically present in the exercise 89% have answered at least to one questionnaire while of those who participated remotely only 13% has given feedback at least in one survey. When people are participating on-line, they seem not have the same kind of obligation to reply to surveys as if they were physically present.

The results presented in the following figures are the averages of all the respondents' agreeing level to the questionnaire statements that each tool has received during the resilience phases they have participated during the exercise. Likert-scale answers in questionnaires have been changed to numbers as follows: strongly agree=5, agree=4, neither agree nor disagree=3, disagree=2, strongly disagree=1.

Tools that participated in the Full Joint Scenario Exercise (detection and response phases) were not presented in individual tool demos (except CaESAR which presented its functionality in the prevention phase in tool demo). Therefore, open-ended questions have been included to the Full Joint Scenario Exercise questionnaire (Q2).

Detailed answers to evaluation questionnaires separated to different groups (end-users/tool providers/others) are presented in Annex XII and Annex XIII provides an assessment of how far the CdM scenario objectives were met based on end-users' evaluation for all resilience phases simulated at CdM SE. In ANNEX XII, the answers to open-ended questions are unfiltered.

6.2.1 Prevention phase

In CdM exercise feedback for tools performance in prevention phase has been asked in questionnaire 1. Respondents agreeing/satisfaction level to the tools' performance is presented in Figure 27. Answers were given as follows:

- Q1: end-user 4, tool provider 14, other 7

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the prevention phase
- The GUI of the individual tool is user-friendly

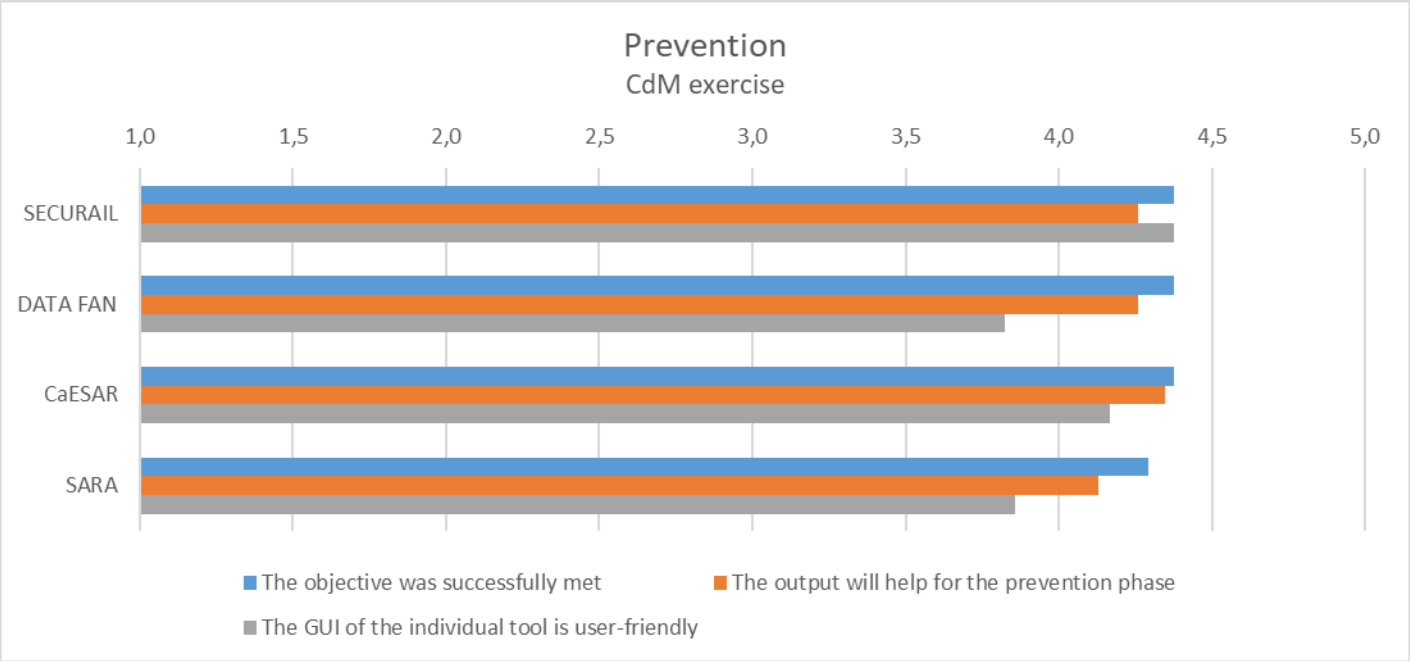


FIGURE 27 CDM EXERCISE PREVENTION PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

6.2.2 Detection phase

In CdM exercise feedback for tools performance in detection phase has been asked in questionnaire 2. Respondents agreeing/satisfaction level to the tools' performance is presented in Figure 28. Answers were given as follows:

- Q2: end-user 3, tool provider 14, other 7

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the detection phase/the decision-making process
- The GUI of the individual tool is user-friendly
- The time for processing was acceptable

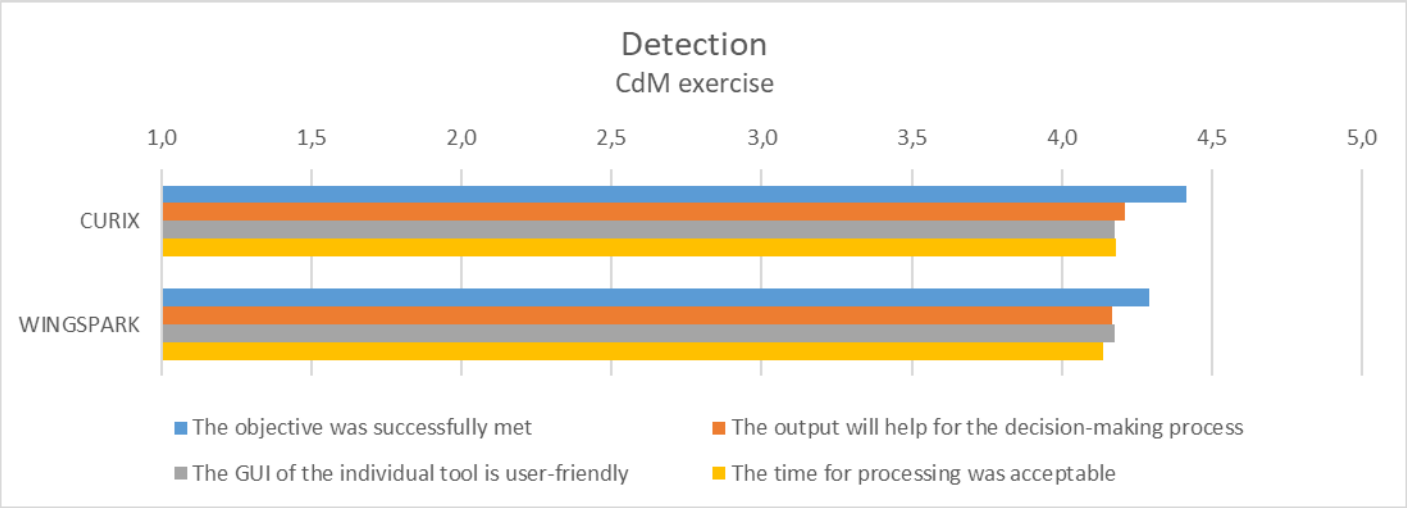


FIGURE 28 CDM EXERCISE DETECTION PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

6.2.3 Response phase

In RFI exercise feedback for tools performance in response phase has been asked in questionnaire 2. Respondents agreeing/satisfaction level to the tools' performance is presented in Figure 29. Answers were given as follows:

- Q2: end-user 3, tool provider 14, other 7

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the response phase/the decision-making process
- The GUI of the individual tool is user-friendly
- The time for processing was acceptable

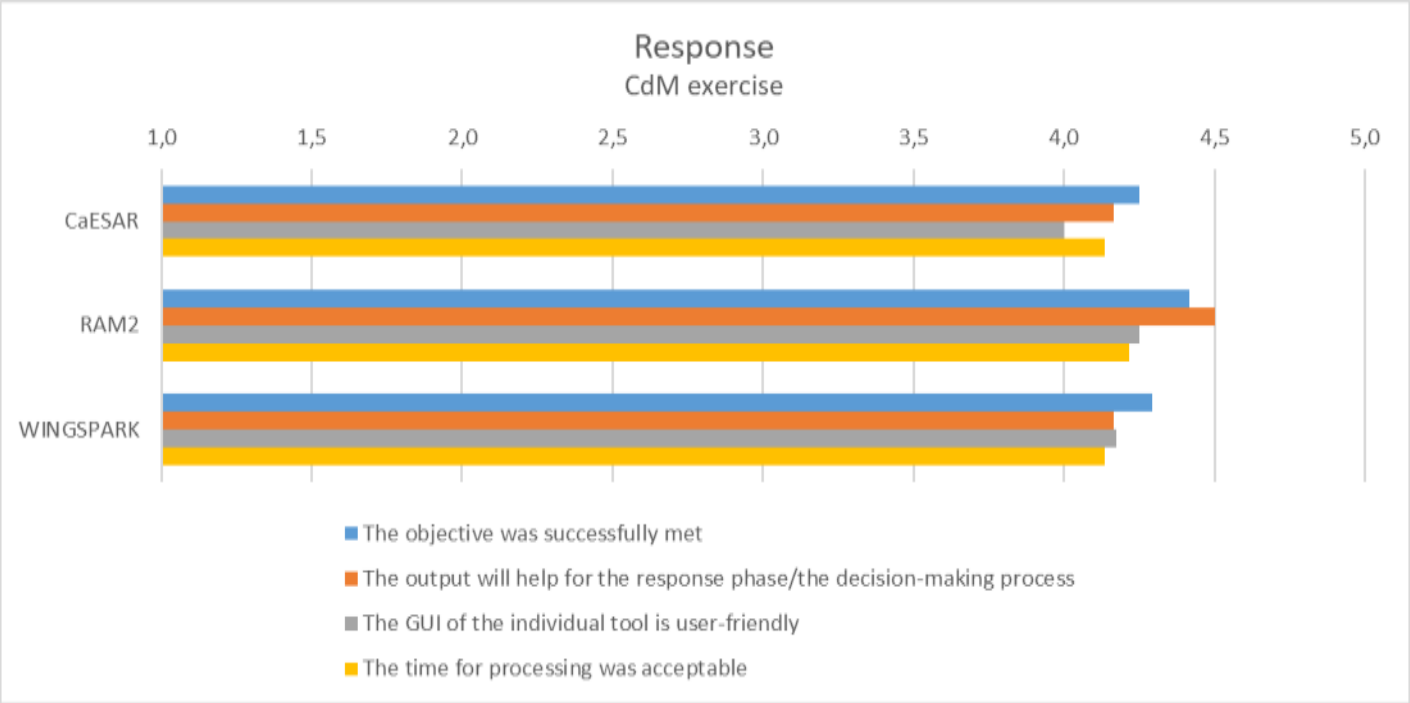


FIGURE 29 CDM EXERCISE RESPONSE PHASE – AVERAGE RATES FOR DIFFERENT TOOLS

6.2.4 Recovery phase

In CdM exercise feedback for tool's performance in recovery phase has been asked in questionnaire 3. Respondents agreeing/satisfaction level to the tool's performance is presented in Figure 30. Answers were given as follows:

- Q3: end-user 6, tool provider 14, other 6

Respondents' satisfaction level has been explored with the statements:

- The objective was successfully met
- The output will help for the recovery phase
- The GUI of the individual tool is user-friendly

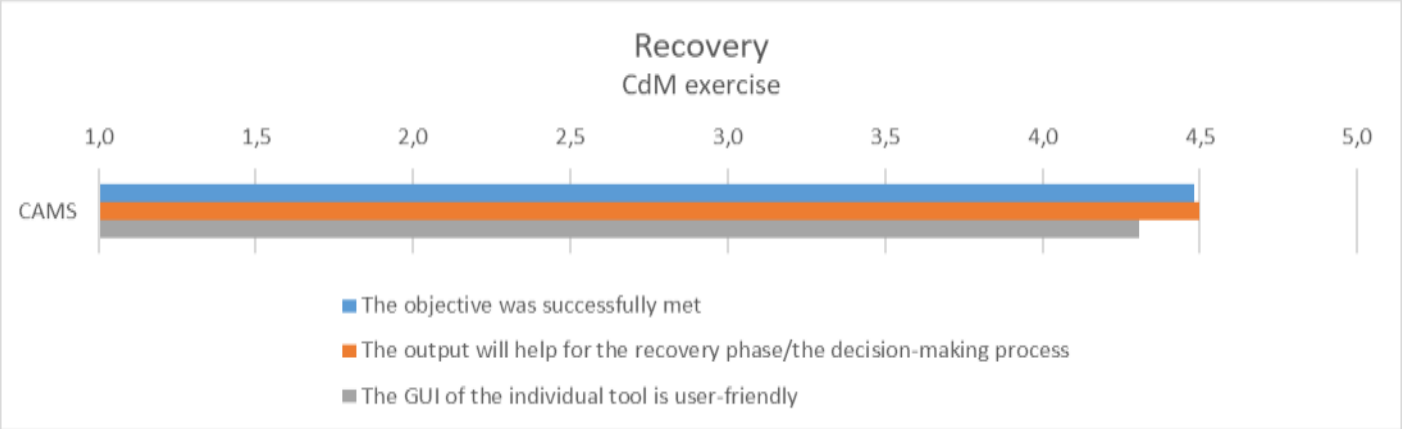


FIGURE 30 CDM EXERCISE RECOVERY PHASE – AVERAGE RATE FOR TOOL

6.2.5 S4RIS Graphical User Interface

The feedback exercise's participants have given for S4RIS GUI in Likert-scale statements is presented in Figure 31. Answers were given as follows:

- Q3: end-user 6, tool provider 14, other 6

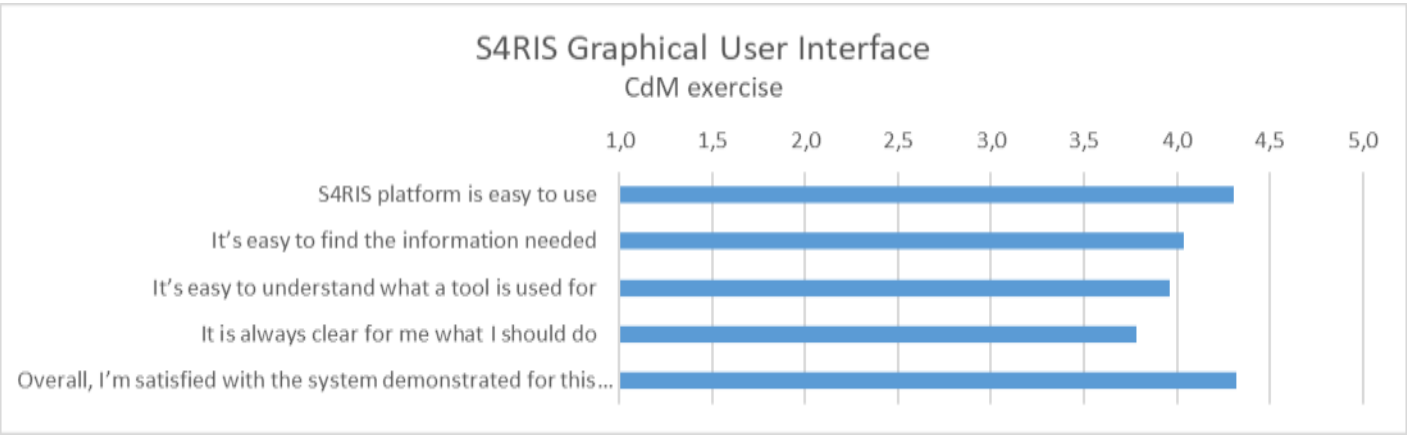


FIGURE 31 CDM EXERCISE S4RIS GUI – AVERAGE RATES FOR STATEMENTS

6.2.6 S4RIS platform

The feedback exercise's participants have given for S4RIS platform in Likert-scale statements is presented in Figure 32. Answers were given as follows:

- Q4: end-user 6, tool provider 14, other 6

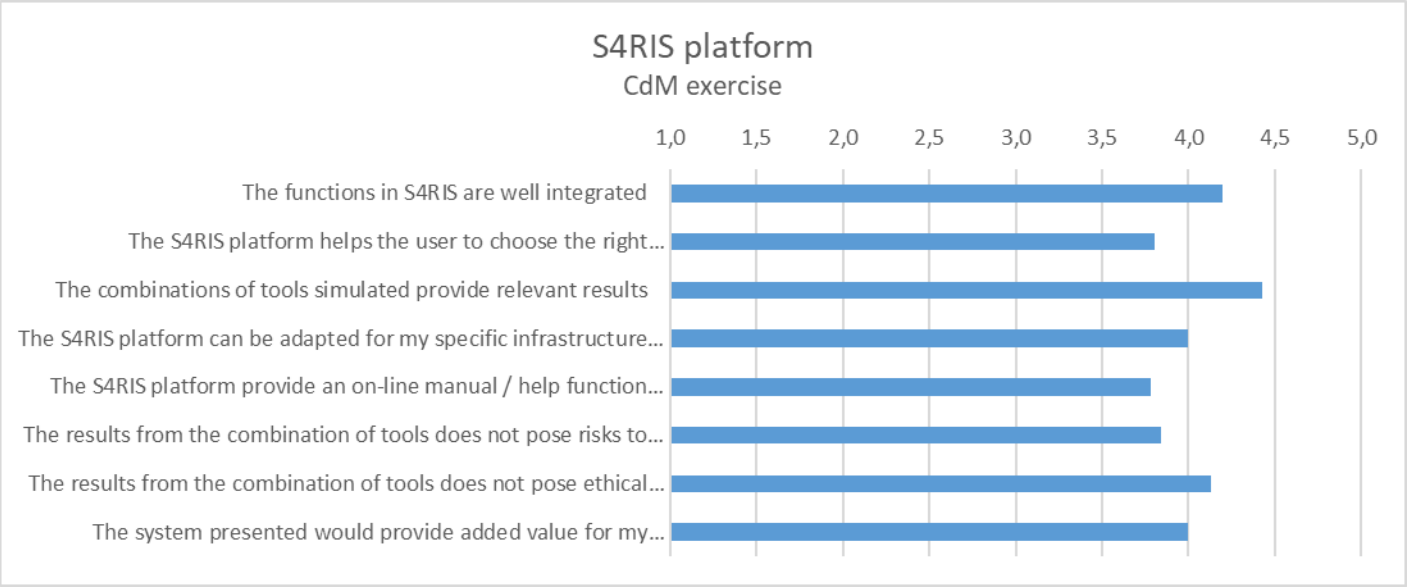


FIGURE 32 CDM EXERCISE S4RIS PLATFORM – AVERAGE RATES FOR STATEMENTS

The response to the statement "*The S4RIS platform provide an on-line manual / help function which is easy to understand*" is partly misleading. Only one individual tool participated to exercise presented an on-line manual. No other help functions were presented.

6.2.7 CdM exercise evaluation

The feedback exercise's participants have given for the exercise in Likert-scale statements is presented in Figure 33. Answers were given as follows:

- Q4: end-user 6, tool provider 14, other 6

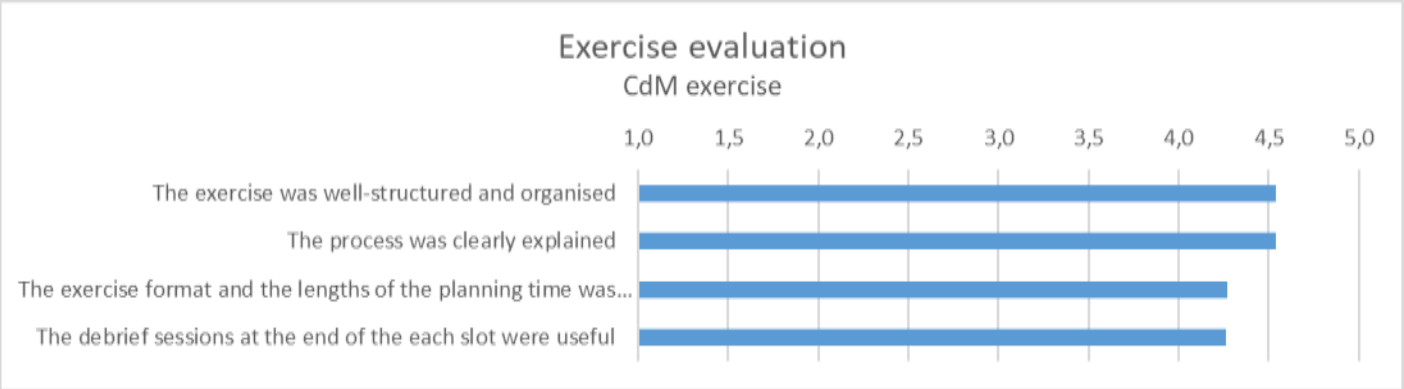


FIGURE 33 CDM EXERCISE EVALUATION – AVERAGE RATES FOR STATEMENTS

6.2.8 Overall questions

The feedback exercise's participants have given overall for S4RIS in Likert-scale statements is presented in Figure 34. Answers were given as follows:

- Q3: end-user 6, tool provider 14, other 6

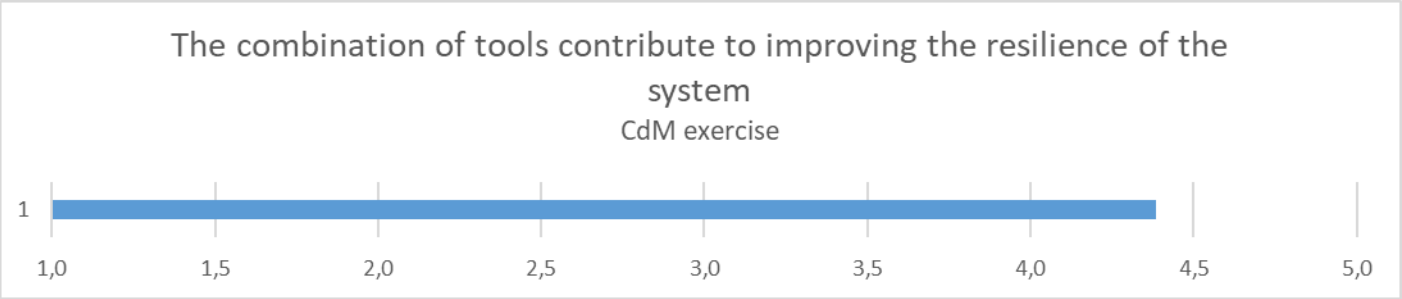


FIGURE 34 CDM EXERCISE OVERALL FEEDBACK OF S4RIS – AVERAGE RATE FOR STATEMENT

6.3 Analysis of the results of the exercise 4

Background

The CdM simulation exercise was the last simulation exercise and focused on *Natural Disaster – Flooding* attack in the metro environment. It addressed four resilience phases: prevention, detection, response and recovery. Eight tools and some of their capacities have been demonstrated successfully, with 23 objectives tested (Annex XIII) and evaluated by 4-6 the end-users, 14 tool providers, and 7-8 other partners.

Functional evaluation analysis

The respondents' evaluation of the tools' functionalities presented during the CdM exercise have been for the most part positive. The respondents' average satisfaction rate (answers to Likert scale questions changed to numbers strongly agree=5…strongly disagree=1) in different resilience phases to how the tools have met the tools' objectives, their outputs, time for processing and GUIs has varied between 3.9-4.5 (rating from 1 to 5).

From a functional point of view, no request for revising the requirements were raised by the end-users.

Main benefits of the tools highlighted by some of the responders when answering the open-ended questions of the questionnaires (available in Annex XII) are the following:

- For simulation and prediction tools (SECURAIL, CaESAR, DATAFAN, SARA, CAMS)
  - Enhance risk assessment and management with a complete overview on the assets to protected and capabilities for risk analysis.
  - Be better prepared to manage crowd in case of a disruptive event such as flooding.
  - Support decision making on the best of mitigation measurescombination.
  - Estimation of the propagation of failures in case of a flooding
  - Automated and real time check of the health of the system and its components
  - Recovery Cost estimation
- For detection tools (CURIX, GANIMEDE, WINGS)
  - Early detection of anomalies (e.g. power supply, crowd concentration, train speed) to be able to react as soon as possible.

Similarity to the previous exercises, the joint simulation exercise was seen beneficial because manytools were seen interacting. The integration of all alerts from different tools gathered in the same interface (RAM2) as well as the mitigation measures displayed for each alert were appreciated by many responders.

The acceptable time to process the information for each tool was also evaluated during the exercise. In general, it was rated as acceptable.

Among the main possible improvements, again the improvement of GUIs, provision of additional data and integration of more tools were mentioned by some of the responders. Other improvements were suggested regarding

- The complexity of some of the tools and therefore the need for user guideline, manuals and other support such as training for the end-users.
- More detailed support to plan mitigation measures.
- Prioritization of alerts.

- Regarding decision making for replacing/repairing asset, it was highlighted by one of the end-users that criticality of assets is focussing on safety and if any damage on a component can lead to safety issues, it is replaced.

There were also suggestions from some responders to further improve the S4RIS GUI, e.g.:

- More attractive design.
- Provision of a dashboard with main information on the current situation.
- Dividing tools according to the resilience phase and provide explanation on when each tool is most useful.
- User manuals.
- Single sign-on for all integrated tools.
- Explanation of tools connections to information sources.

Analysis of the organisation of the exercise and recommendations for the future similar exercises

The organisation of the exercise was well rated by the responders (Figure 33).

Although the CDM exercise was the last one in the series of SEs, the recommendations for future similar exercises were asked and the main ones are as follows:

- More end-users should be continued to be encouraged to attend and respond to the questionnaires as well as stakeholders linked to Commune di Milano. The timing might be one reason regarding the Milan exercise which was organised in mid-July close by the summer holiday period.
- The simulation exercise could be designed in a more interactive way with the possibility for the participant to “play“ with the tools and have more time to discuss with the tool providers.
- Future simulation exercises could be organized at an actual premises of the railway stations or metro station: a test site would allow to have real sensors and to demonstrate the tools in more realistic conditions. *(In response, in producing this report: a precondition is of course that an end-user organisation(s) management agrees to such a test site and that it is available or can be built-up.)*
- More stakeholders such as authorities, other transport operators and infrastructure managers, should be participating in the exercise. This was difficult to organise in SAFETY4RAILS in the context of the COVID-19 crisis first and then the Ukrainian-Russian war.
- In some of the answers, the schedule was seen clear and supporting the exercise. First explaining the scenario - also by the host CDM - then explaining the tools and their specifications to the scenario and then the debriefing session. However, some of the participants stated that different phases with respect to the scenario could be made clearer.
- Such simulation exercises should be held in person only to strengthen live discussions andhelp partners to better know each other.

Analysis of the Evaluation methodology and recommendations for the future similar exercises

The evaluation methodology applied in the simulation exercises was mainly based on questionnaires with both Likert scale questions and the open-ended questions.

The scope of the project is very broad: for each simulation exercise, between 8 and 13 tools were demonstrated and had to be evaluated.

It has been very challenging for the end-users’ representatives to evaluate the solutions for several reasons:

- The duration of the project is very short with a very broad scope, many tools, many partners.
- Online meetings since the beginning of the project due to the pandemiccrisis make more difficult theunderstanding of such a large project.
- The tools are very innovative, most of them are based on artificial intelligence which is at a very early stage within rail companies.
- Many different expertise is needed to answer the questions.

- During the simulation exercise, the tools are presented in a relatively short timeslot. To be able to really evaluate the system, you have to use it yourself.

Some of the suggestions from the partners to improve the evaluation methodology are as follows:

- There should be more debrief questionnaires and the questionnaires should be shorter.
- The debriefing session should be longer - there should be more time to get answers that are more specific.
- An open discussion after each phase or after the questionnaire would increase the involvement persons in giving different feedback.

7. Nominal Group Technique evaluation

The Nominal Group Technique (NGT) is a highly structured group-based technique using face-to-face meetings. It combines individual and group phases. The purpose of the structure and individual phases is to limit group dynamics and social power dynamics. The technique prevents dominant individuals from controlling the group and limits the researcher's interaction in the generation of ideas.

The original plan for the use of the NGT was laid out in D8.1 of SAFETY4RAILS project, Evaluation Methodology. Two online NGT focus group discussions were organised via Microsoft Teams, the first 09.06.2022 and the second one 12. /13.7.2022. For the first NGT, every end-user attendee who agreed to be contacted in the online questionnaires of the first two, i.e., Madrid and/or Ankara exercises were invited. This was because event was organised before the third and fourth exercises.

In both sessions, the same methodology was used. The first NGT focused on S4RIS influence to Business Continuity Management (BCM) and Crisis Management (CM) whereas in the second NGT the focus was on end-users and on the S4RIS platform e.g. applicability, feasibility and on the potential the developed solution provides for end-users. The attendees were not required to prepare in any specific way. However, the topics / questions were sent to participants in advance for the second NGT. The sessions were recorded to aid analysis. The moderator asked all questions and directed the proceedings, while the evaluator concentrated on collecting manual notes. As the NGT session started, the attendees were given basic information and were asked baseline questions. Answers to these questions were not done using the NGT methodology, as they merely provided background, not directly related to the exercises. The baseline questions asked were as follows:

- Do you consent to recording this session? This is only for internal review. The recording will not be made public. Final report will not include your name or your employer.
- Where do you work and in what capacity?
- Which exercises did you participate in?
- What do you consider the number one goal of Business Continuity Management (BCM) in your industry?
- What do you consider the number one goal of Crisis Management (CM) in your industry?

After the baseline questions, the actual NGT questions were posed, revealed on screen one at a time. The attendees were instructed to consider their answer, request any necessary elaboration, if necessary, then type the answer into the Microsoft Teams chat window, but only send the answer once prompted by the chairperson to do so. In this way, answers to the question were visible only after everyone had their own. This simulated the traditional NGT technique of writing the answer on paper and then revealing it when prompted.

7.1 Focus group discussions 1

The NGT questions posed were as follows:

1. After witnessing the S4RIS solution and tools, do you think it could provide added value to BCM in your industry?
2. Which aspect or tool specifically is useful for BCM?
3. What could it need more in order to provide added value to BCM?
4. After witnessing the S4RIS solution and tools, do you think it could provide added value to CM in your industry?
5. Which aspect or tool specifically is useful for CM?
6. What could it need more in order to provide added value to CM?

The motivation to ask these specific questions was based on the DoA of the SAFETY4RAILS project. In the DoA, it is stated that the evaluation should “generate for each scenario an evaluation/validation report incl. lessons learnt, which concentrateon optimization potentials and technical aspects of the S4RIS but also on identified potentials to improve theBusiness Continuity Managementand especially the Crisis Management for the railway companies”. While the optimization potentials and technical aspects were possible to respond to with questionnaires, the BCM and CM potentials are more holistic and harder to respond to on a questionnaire.

The first NGT had the following makeup:

- Moderator from organiser
- Support person to take notes from organiser
- An end-user, business manager from Ankara Metro, with co-worker interpreting (participant #1)
- An end-user, project manager from Catalonian Railway transport company TC (participant #2)

Relevant answers to baseline questions were as follows:

- Both agreed to recording and use of their names, if necessary
- Participant #1 was present in the Ankara exercise.
- Participant #2 was present in Madrid, Ankara, and Rome exercises. It should be noted that the Rome exercise was organized a few days before this NGT was held, but after the invitations were sent.
- The number one goal of Business Continuity Management (BCM) [in the rail industry] was reliability, availability, and safety of passengers.
- The number one goal of Crisis Management (CM) [in the railway industry] was seen as reducing any possible fatalities to zero.

7.1.1 Results of the focus group discussions 1

After the baseline questions the actual NGT session wasproceeded. The questions and collected and compiled responses are provided below.

Question 1: After witnessing the S4RIS solution and tools, do you think it could provide added value to BCM in your industry?

As a product that merges different tools for crisis management, it can add value in the future. S4RIS is still under development, but it has potential to provide added value with more refinement. These tools and this project have the potential to help increase the level of safety.

Question 2: Which aspect or tool specifically is useful for BCM?

The merging of different tools. The iCrowd tool, as demonstrated in the Ankara simulation exercise, was specifically mentioned.

Question 3: What could it need more in order to provide added value to BCM?

It should have a graphical user interface (GUI) that adapts to the different end-users' physical facilities. To provide a more in-depth answer, we should try it in our own facilities, and of course, a real scenario will tell even more. Obviously, that is impossible to organize. In any case, the more adaptable the S4RIS solution is the better.

Question 4: After witnessing the S4RIS solution and tools, do you think it could provide added value to CM in your industry?

Yes, there is an added value for CM. However, in order to implement the tool successfully, a process of adaptation and training should be carried out internally for each Railway Operator. Unsure how this in the scope of the project, but it would be hard to start from scratch. Although they are useful applications, their integrated development with similar projects will yield even more beneficial results in crisis management.

Question 5: Which aspect or tool specifically is useful for CM?

The way it is merging different tools and different alerts that help detect, prevent, and mitigate the effects of a crisis. Ganimede specifically seemed helpful in this regard, at least based on the Ankara case. In addition, iCrowd and Ganimede tools were specifically mentioned to have beneficial results in crisis management.

Question 6: What could [the S4RIS solution] need more in order to provide added value to CM?

More adaptability to the end-users' contexts and cultures, and the development of manuals and training plans. As a thought: resolving problems that may arise from human errors and weaknesses, with the use of such applications, yields effective results in crisis management.

7.2 Focus group discussions 2

The objective of the second FGD was to consolidate the results received from simulation exercises questionnaires and on the other hand specify open issues found during the results analysis.
In the second Focus Group Discussions (FGD) the focus was on end-users and on the S4RIS platform e.g. applicability, feasibility and on the potential the developed solution provides for end-users. The invitation was sent to seven end-users. They were the end-users, who had agreed to be contacted later for this purpose when they filled the exercise questionnaire in one or several simulation exercises. The FGD was organised in two sessions so that all invited end-users could participate to the discussions.

The baseline questions were the same as in NGT 1.

The following NGT questions were discussed:

Question 1: What you consider the most important feature S4RIS offers for your business.
Question 2: Based on the presentations and full joint scenarios during the simulation exercises, what is your experience, is the S4RIS GUI user friendly and how it would be future develop for matching better to your gabs or needs.
Question 3: After witnessing the S4RIS solution and tools during the exercises, how would you describe the S4RIS GUI development?
Question 4: Marketing potential of S4RIS, top reasons to buy this product or service? (Adoption – adaption model)
Question 5: Based on the Simulation Exercises and your expertise how you would describe the S4RIS platform applicability for your daily routines including its strengths and weaknesses
Question 6: How the S4RIS platform should be further develop in order to improve even better the railway safety

The first session of the second NGT had the following makeup:

- Moderator from organiser
- Two evaluators from organiser
- Three end-users, representing International Union of Railways (France) and two from Commune de Milan (Italy)

Relevant answers to baseline questions

- All agreed to recording
- All participated in all four Simulation Exercise

The second session of the second NGT had the following makeup:

- Moderator from organiser
- Three evaluators from organiser
- Four end-users, representing RFI (Italy), ProRail (Netherlands), Metro de Madrid (Spain) and Catalonian Railway transport company TC (Spain)

Relevant answers to baseline questions

- All agreed to recording
- Three participants had participated in three and one in all simulation exercises.

7.2.1 Results of the focus group discussions 2

After the baseline questions the actual NGT session was proceeded. The questions and a summary of responses can be found below.

Question 1: What you consider the most important feature S4RIS offers for your business?
The integration of tools and information was mentioned as most important feature as seen from the answers. The integration of the tools with the provision of alerts in a single tool: usually cyber and physical threats are managed by different services and the comprehensive overview of all alerts can be very useful.

Question 2: Based on the presentations and full joint scenarios during the simulation exercises, what is your experience, is the S4RIS GUI user friendly and how it would be future develop for matching better to your gaps or needs.

The participants of the first NGT session found the GUI quite user friendly and easy to use. It was also mentioned that the GUI was developed in a short project and a GUI that includes 18 different tools needs longer time to develop operational. The participants of the second session stated that it is difficult to say whether the GUI is user friendly or not because it was just presented during the exercise. A clear opinion could be provided after using the system for a while.

Question 3: After witnessing the S4RIS solution and tools during the exercises, how would you describe the S4RIS GUI development?
The GUI development got positive feedback. It was mentioned that GUI has a clear and simple style. It was also stated in several answers that this kind of project is too short a time period for developinga fully operational GUI and therefore it needs to be further developed to meet different end-users needs.

Question 4: Marketing potential of S4RIS, top reasons to buy this product or service? (Adoption – adaption model)
The marketing questions was a bit difficult to answer for the first session participants while they were more in stakeholder role than in operative end-user role. The second session included operative end-users and the Crisis Management and Business Continuity with tools covering the prevention, detection, and response phase was highlighted in each comments as a potential aspect that S4RIS provides. The capability for integrating several tools in one platform was mentioned also as an advantage for marketing the solution

Question 5: Based on the Simulation Exercises and your expertise how you would describe the S4RIS platform applicability for your daily routines including its strengths and weaknesses?

The applicability of S4RIS daily routines would be in the management of crisis. The Integrated Control Centre would have an extra input of information when solving a crisis as well as single point of interface, strong aspects in the data collection for meta-data analysis and the alert systems.

While the Question 6 was not relevant for the S4RIS evaluation, the answers are not presented in this document.

8. Strengthening of end users' feedback from the S4RIS during post-project phase

During SAFEYT4RAILS' project lifetime the main end-user feedback came from:

- 8 end-user beneficiaries integrated within the consortium: the six railway/metro and/or rail/metro infrastructure operators, UIC the International Union of Railways "the worldwide professional association representing the railway sector and promoting rail transport"[10] with more than 200 members and a city municipality.
- 10 external members of the End-User Board who were experts employed at railway/metro and/or rail/metor infrastructure operators, the International Association of Public Transport (UITP) (with more than 1,900 members) and a relevant ministry.
- Feedback from other end-users during communication and dissemination events such as the Final Conference.

Sections 3.2, 4.2, 5.2 and 6.2 have reported the number of specific questionnaire answers from "end-users" during the simulation exercises. In some simulation exercises and their individual phases, the number of end-user responses were lower than SAFETY4RAILS targeted and expected. The same sections describe some discussion on why the responses may have been lower. To this can be added that some end-users' answers to the questionnaires were sent in groups, gathering the information from several attendees. Even if quantatively the number of responses can seem low, from a qualitative point of view the evaluation of the exercises gave good results. These evaluations together with overall feedback to the project enabled the good faith assessment by the consortium in the Annex XIV with regards to which of the D1.4 requirements/specifications were tested directly and/or indirectly in the SEs and how far they were met. The deliverable review process ensured this good faith assessment with the beneficiary end-users' input and agreement.

Beyond the evaluation itself, presented in this report, a lot of exchanges between the end-users and the providers were held during the project final conference in Paris where a demonstration of the final version of S4RIS was performed as well as a poster session. The conference was attended by representatives from:

- Nine major railways in Europe (CD, DBAG, FGC, INFRABEL, NS, PKP, PRORAIL, RFI, SNCF)
- Three public transport companies (MDM, RATP, UITP)
- Two transport Ministries (France, Germany) and
- One city (CDM)

Even if there was no formal evaluation for the event, the feedback from the end-users was very positive.

Nevertheless, in the post-project phases, SAFETY4RAILS plans to build on the feedback received within the duration of the project and to mitigate against limitations in the targeted audiences and collected feedback (and specifically the number of replies from the simulation exercises). This is to be achieved as an integral part of the exploitation plans which includes further dissemination and communication.

The S4RIS exploitation plan in post-project phase is presented in SAFETY4RAILS deliverable D10.9 (last version: "D10.9_V1_1_20230113"). The deliverable highlights that the results can be exploited through a number of routes e.g. individual results by individual partners, a number of results by a number of partners together in a sub-group and the "full" S4RIS platform with chosen and tailored components depending on the specific end-user. All of these routes include further activities with end-users, such as demonstration and piloting, with the goal of end-users taking up operational productive versions of the project results. These activities will increase the audience targeted to date and provide further evaluation, again targeted to the successful exploitation of the results.

[10] https://uic.org/about/about-uic/

D10.9 identifies that the S4RIS as a combined result will not be taken to the market immediately and it requires at least 2 to 3 years of preparation and future tailoring to the railway segment. The main reasons for this are to increase the Technology Readiness Levels (TRLs) (most results are at TRL7, some lower), the "highly regulated environment with specific provisions on safety" and the "complex safety and security schemes currently implemented by end-users"[11]

In the D10.9, the main exploitation plan for the S4RIS as a combined result includes three phases:

Phase 1 Preparation, at least one year after the end of the project

Phase 2 Industrialisation; years 2 and 3 after 1st phase

Phase 3 Commercialisation: years 4 and 5 after 1st phase

D10.9 identifies that an EU-funded Pre-Commercial Procurement (PCP)[12] could support (and informs) these phases and that the SAFETY4RAILS end-users have been advised to prepare and launch a PCP.[13] Members of the consortium are also continually reviewing further mechanisms which could help to financially support the exploitation plan.

In all phases further feedback from end-users will be gained. In what follows we present only those foreseen activities with a main focus on communication with end-users and their input, feedback and evaluation:

"YEAR 1: PREPARATION PHASE

…

- Evaluation of the needs and challenges
- Launching an open-market consultation
- Drafting specifications and requirements

…

- Assess the market and customer needs
- Map potential interested end-users

…

YEAR 2: INDUSTRIALISATION PHASE

…

- Customisation and adaptation of the User Interface and User Experience to the specific end-user usability needs.
- Scale the SAFETY4RAILS solution to the management of the large volume of data linked to the assets in a railway network, including full interoperability with end-users legacy systems and facilities.
- Develop additional modules/features required by the end-users (if any).
- Perform technical verification and validation of the system.

….

YEAR 3: INDUSTRIALISATION PHASE

…

- Develop and test pre-production/ installation hardware and software system at pilot demos.
- Full integration and deployment with legacy systems at the end-user premises to allow full interoperability and information exchange.

---

[11] SAFETY4RAILS Deliverbale D10.9 Exploitation Strategy (Jaunary 2023), page 64.
[12] European Commission (2007). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe. COM(2007) 799 final. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0799:FIN:EN:PDF
[13] Supra:- SAFETY4RAILS D10.9, page 65.

…

YEAR 4: COMMERCIALISATION PHASE

…

- …. early adopters – those participating in the PCP. Specific procurement mechanisms would be launched from the end-user side to adopt the solution.

…

- Further training activities would be performed with the end-user to facilitate adoption.
- Demonstrations at relevant security-related events would be organised and attended by Railway Infrastructure Managers

YEAR 5: COMMERCIALISATION PHASE

…

- Launch commercial activities with Railway Infrastructure customers in other countries with high market value in Europe…

…

- Perform commercial demos in the targeted countries and stimulate customer interest using a test version." [14]

One important issue the end-users mentioned in the NGT discussions was that two-to-three-day exercise is a short time to assess a solution such as S4RIS if you do not know the system and the tools beforehand and that it requires using the system by oneself to provide increased understanding of the usefulness. In other words, further hands-on doing was requested and regarding this particularly the phases 2 and 3 foresee (and require) further hands-on experience for end-users.

The business strategy of the industrial partners (reflected in the deliverable D10.8 Market analysis and business plan) also involves additional communication and dissemination of project results, demonstrations, usability tests and pre-sales sessions to facilitate uptake and ensure the endorsement from end-users. These activities will also be used as opportunities to gather further end-user feedback.

The vast majority of technical partners have confirmed their interest in taking part in the joint exploitation of the S4RIS. Interested partners have also formed an Exploitation Coordination Committee which will oversee the joint exploitation approach for the SAFETY4RAILS results, what is reflected in the deliverable D10.9.

Seven end-users, as identified above, support the exploitation, including metro and railway infrastructure, as well as UIC. These partners, along with all other partners, are committed to raise awareness among their networks about the SAFETY4RAILS results, as described in the deliverable D10.3 Second update of the dissemination and communication plan. This will also provide further end-user feedback on the project results (and support the uptake of the results as well as cooperation with providers to allow them to reach their markets).

By way of example, after the end of the project, UIC has disseminated the results of the project in six international events gathering rail security experts:

- 5-6 October 2022: CIPC Conference (180 security experts from authorities, rail companies, public transport operators, research centres, transport associations and international organisations).
- 14 October 2022: UIC Cyber security platform (about 15 cyber security experts in Europe)
- 19 October 2022: LANDSEC (EU expert group in land transport security)
- 6-7 December 2022: UITP Security Committee (around 40 security experts from metro operators worldwide)

[14] Op.cit.

- 17-18 November 2022: COLPOFER General Assembly (around 30 security experts) from railways in Europe
- 21-23 February 2023: UIC world Security Congress (around 100 security experts)

As stated in the exploitation plan D10.9, UIC will continue to disseminate the results in international events, but also bilaterally with members of UIC that are interested. Integration of security technologies and artificial intelligence are topics regularly addressed in the UIC working group on New Technology. SAFETY4RAILS has been regularly presented during the meeting of this group.

From the industrial and commercial side, we have IT companies used to bringing innovation into the market with their understanding and experience of engaging with end-users to ensure successful commercialisation of the project results. The large portfolio of clients and already implemented technologies are the perfect presentation card to promote and commercially exploit the outputs of SAFETY4RAILS with end-users.

9. S4RIS influence for railway companies Business Continuity Management and Crisis Management.

The Figure 35 visualises how SAFETY4RAILS expects to support rail and metro operators to increase the resilience of their services through the provision of capabilities to do it. According to SAFETY4RAILS Deliverable 1.4, S4RIS platform aims to offer software that offers and combines risk assessment, monitoring, simulation and decision support capabilities as well as “visualisation means to prevent, forecast, detect, defuse, respond and mitigate the impact of cyber and physical threats in a holistic methodological and operational approach resulting from a collaboration between cyber-physical security technologies and actors” ((European Comission, June 2021) Part B p.26).

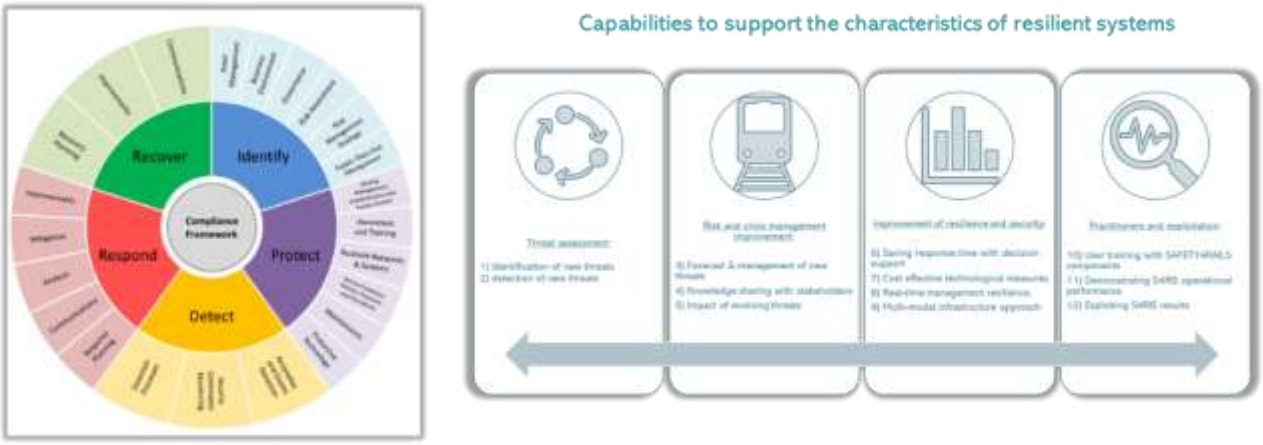


FIGURE 35 SAFETY4RAILS OBJECTIVES DESIGNED TO DELIVER CAPABILITIES TO SUPPORT THE CHARACTERISTICS OF RESILIENT SYSTEMS. LEFT IMAGE (DEPARTMENT OF COMMUNICATIONS, AUGUST 2019) P.8 AND P. 22, RIGHT IMAGE (EUROPEAN COMISSION, JUNE 2021) P. 32

Business continuity management (BCM), crisis management (CM), disaster recovery (DR), and resilience are related concepts, the purpose of which is to secure the critical functionality of the system in all situations. Risks and crises are often a derivative of external stressors, while the organization's resilience is more intrinsic, and from this sense, the priority of preventive behaviour at the organizational level is the preparation of various procedures for response to certain crises or risk events. Traditionally, BCM combines risk management and quality management. DR details of procedures and steps to recover from a disaster. CM Plan details are steps to be taken to handle the crisis. The BC Plan lists the steps to be taken to ensure continuity of mission-critical business operations. Crisis Management Plan and DR Plan are components of the overall BC Plan. The Figure 36, based on the summary of the literature review in WP7, presents the management cycles BCM and resilience management. The holistic BCM process identifies potential threatening impacts on the organization and provides a framework for developing resilience and the ability to respond effectively to protect the system and the interests of key actors. The goal of resilience engineering is to improve resilience by reducing the drop in capability and speeding up recovery. The goal of resilience management is also to learn from unwanted events and thus improve the system's capability.

a) Business continuity cycle

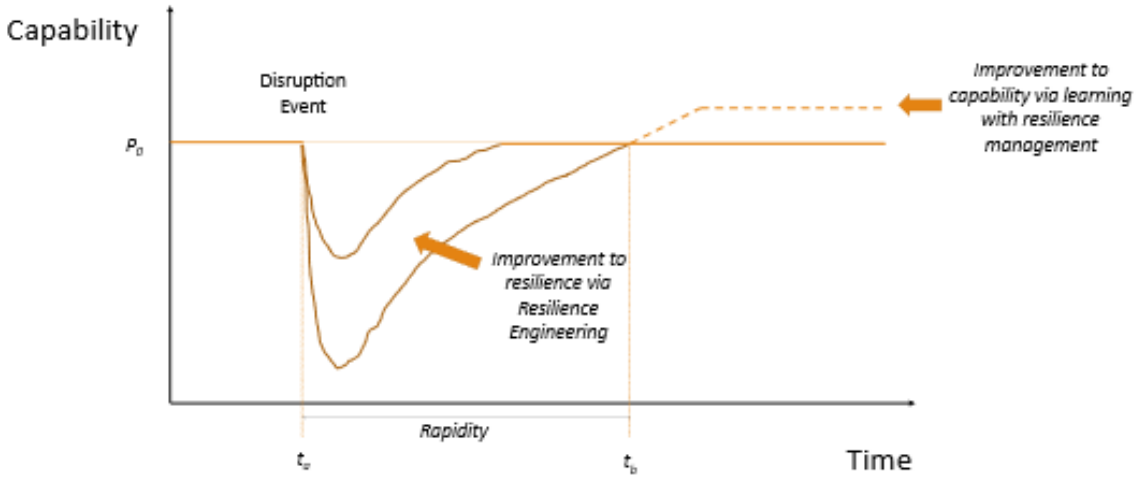


FIGURE 36 BCM AND RESILIENCE CYCLES

b) Resilience cycle and aspects of resilience engineering

SAFETY4RAILS Deliverable 1.4 gives 29 crisis management requirements for S4RIS. Specific Business Continuity Management requirements for S4RIS have not been given, but general instructions can be found in standard ISO 22301 – Security and resilience – Business continuity management which is the international standard helping organizations put business continuity plans in place to protect themselves and recover from disruptive incidents when they occur. Many on the CM requirements in Deliverable 1.4 concentrate on organisational aspect, while this report is based on four exercises that concentrate on optimization potentials for technical aspects of the S4RIS.

There were no specific BCM and CM questions in the surveys related to the exercises, but the first focus group discussion (NGT1) concentrated on S4RIS influence to BCM and CM. Based on NGT1, the number one goal of BCM in the rail industry is to secure the safe transport of passengers. Accordingly, the main goal of CM is zero fatalities in rail traffic, and distribution of information about the situation to the public. The results of NGT1 can be found in Section 7.1.1.

S4RIS is still under development, but it has potential to provide added value with more refinement for railway and metro companies. When ready, S4RIS will be a product that merges different tools for BCM and CM. The exercises gave good examples of how the S4RIS can help in BCM and CM. However, it will only be a tool and the railway and metro operators will have the main responsibility for BCM and CM.

10. Conclusion

The S4RIS was evaluated in four Simulation Exercises and feedback was collected with altogether 17 online questionnaires. In addition to those, feedback was collected in two Nominal Group Technique focus groups and less formally in bilateral and/or smaller group discussions. This later, less formal feedback, has not been the subject of their report. The main target group for evaluation was the end-users and in the first SE, only end-users were asked to answer the S4RIS tools related questions. During the first SE it was discussed that tool providers and other participants could provide also valuable feedback for the evaluation and the evaluations were changed so that all participants were requested to answer the surveys in the rest of the exercises. It was however always possible to distinguish end-users' feedback from the feedback from other participants. With this arrangement altogether 292 responses were received from the 17 questionnaires. The end-users share of provided answers was 37%. In our opinion, the participation of and evaluation from end-users in SAFETY4RAILS was high on average for a Horizon 2020 project, but, as it was mentioned in almost all SEs open-end answers, evaluation by further end-users and their connected operational stakeholders would be additional valuable input. This is input into designing the implementation steps following the completion of the project.

Overall, the respondents valued most the developing integration between the different information sources and systems as well as detection capabilities. The platform gives the opportunity of collecting information and updating it, obtaining a simulation of different choices and giving back a decision support system for security purposes. The benefit of support in decision-making and combined alert from different tools were also highlighted. The detection tools, which demonstrated early detection of anomalies or vulnerabilities, were appreciated for anticipating situations and preventing or mitigating the consequences of cyber and physical attacks.

With regard to the simulation exercises, some comments have been made that the exercises could have given the end users even more time to get to know the system(s) e.g. the tools were presented in a relatively short timeslot and more time would be appreciated to use the system / its tools and to understand the numerous capabilities. It is accepted that this was an intrinsic challenge for SAFETY4RAILS given its starting point and duration. When planning future exercises and evaluations it will be useful to think about how this could be achieved.

Another challenge that was highlighted by many participants was the importance of getting more sets of real data to make the scenarios more realistic and better assess the solutions. Given the sensitivity of data, data regulations and also the short timeframe to provide the data, the provision of real data was a challenge. Anyway, open data, artificial data as well as historical data provided by the end-users in each simulation exercise were used and allowed to demonstrate the tools capabilities and assess them in an operational context.

It was also expressed the challenges to adopt S4RIS to current systems due to different stakeholders, integration of systems, lack of standards for data and communication, availability of data, internal manners and culture as well as legislation aspects.

All tools were offered the opportunity to take part in all SEs. The decision whether to take part or not was primarily down to tool provider's readiness and willingness to take part in the SE. Four contributory tools participated in all four exercises and four tools were not participating in any SE. Table 6 presents the combination of tools in each simulation exercise.

TABLE 6 TOOLS PARTICIPATION IN SIMULATION EXERCISES

Tool	MdM				TCDD&EGO				RFI				CDM			
	Prevetion	Detection	Response	Recovery	Prevetion	Detection	Response	Recovery	Prevetion	Detection	Response	Recovery	Prevetion	Detection	Response	Recovery
BomBlast3d	X			X												
iCrowd	X		X		X		X									
CAMS	X			X				X				X				X
SecuRail	X				X		X						X			
TILSAIL	X	X			X	X			X							
PRIGM	X				X	X										
SENSTATION					X											
DATA FAN	X	X	X		X	X	X		X		X		X			
CaESAR	X				X				X		X		X			
WINGSPARK		X	X							X	X			X	X	
CuriX		X				X				X				X		
RAM2	X	X	X		X	X	X		X	X	X				X	
SARA													X			
Ganimede						X				X						
SecaaS																
WIBAS																
uniMS																
SISC2																

The contributory tools which were evaluated in each SE depended on the original scenarios proposed by the end-user hosts together with their extension, where necessary, to cover those tools committed to be tested by their providers. As described earlier in this report, for each SE, scenario-based requirements/objectives identified in SAFETY4RAILS Deliverable D8.2 and in SAFETY4RAILS Deliverable D8.3 referenced back to tool specific requirements/specifications identified in D1.4 were tested.

As a further step in evaluation, Annex XIV provides a good faith assessment by the consortium of which of the D1.4 requirements/specifications were tested directly and/or indirectly in the SEs and how far they were met. The assessment is based on the rather limited number of test demonstrations at the SEs together with what the individual S4RIS component and/or tool providers presented their component(s)/tool(s) could do at the SEs. The assessment indicates that there was a prioritisation towards testing core requirements/specifications most relevant for the SEs as designed and arguably core to the S4RIS platform and its contributory tools at this stage of development. *(The deliverable D6.4 Final developmental validation and evaluation of the S4RIS system reports also on the testing and evaluation of the full set of requirements/specifications during technical testing in the work package 6 as anticipated in the section 1.1 above.)*

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. 79 essential, one essential/conditional, 13 conditional, seven optional and 20 not specified requirements were tested in the Simulation Exercises scenarios. The standards (55), Blockchain technology (4) and Railways in smart city (10) related requirements were not part of the SE evaluation as assessed.

Twenty-six S4RIS platform specific requirements were defined in D1.4 of which one was conditional and one optional. The rest 24 were essential. In four SEs, five essential requirements were involved in the SE scenarios and evaluated.

The S4RIS GUI was involved operationally in the CDM exercise. During the other SEs, it was presented using power point presentations. 28 S4RIS GUI related requirements were defined, 16 essential, 10 conditional and 2 optional requirements. Nine essential, four conditional and one optional requirement were included in the simulation scenarios. S4RIS GUI related questions have been in all SE questionnaires thus, it is obvious that at least the Likert scale answers provided in the three first SEswere related to RAM^2 GUI or another individual tool GUI.

Table 7 provides information on the number of tools requirements/specifications as well as the number of the tested requirements/specifications as assessed.

TABLE 7 SAFETY4RAILS GOOD FAITH ASSESSMENT OF D1.4 REQUIREMENTS/SPECIFICATIONS TEST COVERAGE IN SES

Requirement	Priorities and tests							
Specificationtype	Essential	Tested	Conditional	Tested	Optional	Tested	No specific	Tested
S4RIS platformspecific	24	7	1		1			
Knowledge / Usability	1	1						
Graphical User Interface - GUI	16	9	10	4	2	1		
Standards	34[1)]		21					
Data Protection	1							
Open-source intelligence technologies for the S4RIS	4	2	1					
Blockchaintechnology	3				1			
Railways in the Smart City	2		2				6	1
Crisis Management	1						29	19
Communicationwiththepublic	5		2		1			
Cost	1	1						
BB3d (RINA-C)	6	2						
CaESAR (Fraunhofer)	7	4	1	1				
CAMS (RMIT)	9	7	2	2				
CuriX (CuriX)	6	6	3		2	1		
DATAFAN (Fraunhofer)	9	7						
Ganimede (LDO)	5	4	1	1				
iCrowd (NCSRD)	3	3	1		3	2		
PRIGM (ERARGE)	6	6	1	1				
RAM[2] (ELBIT)	7	5						
SARA (RINA-C)	2[2)]	1						

Requirement	Priorities and tests							
Specificationtype	Essential	Tested	Conditional	Tested	Optional	Tested	No specific	Tested
SecaaS (ICOM)	2		1					
SecuRail (STAM)	3	3	3	3	1	1		
Senstation (ERARGE)	4	4	1	1				
SISC2 (ICOM)	1		1					
TISAIL (TREE)	5	4			3	2		
uni|MS™ (ICOM)	1		1					
WIBAS (ICOM)	1		1					
WINGSPARK (WINGS)	5	4						

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

As Annex XIV indicates overall of the requirements/specifications which WP8 assessed it was able to provide an evaluation on the results were the following:

- Achieved: 71
- Partially achieved: 58
- Not achieved: 16
- Not known to date (of extent of achievement): 132 (incl. requirements not tested in WP8)

The NGT sessions brought benefit for evaluation and broadly confirmed the results received from the questionnaires and observation during the SEs.Although the participants represented both stakeholders and operative end-users, the outcome of the events was equal. Each questionnaire and NGT provided indirectly feedback for BCM and CM but the first NGT was the only evaluation event that was focused directly on BCM and CM. The Simulation Exercises timing changed during the project, which was a bit challenging for the NGT arrangements, especially after the CdM SE, evaluators had only few days to analyse the answers for finding the gaps to be covered during the second NGT sessions.

Crisis Management is a component of the overall business continuity management. WP2 has defined 29 specific CM requirements for S4RIS. Although the scenarios of the Simulation Exercises did not cover all these requirements, the S4RIS was mentioned as a beneficial solution for both BCM and CM in NGT feedback. Especially when discussing about the marketing potential S4RIS have, the Crisis Management and Business Continuity with tools covering the prevention, detection, and response phase was highlighted.

The development of the S4RIS GUI started from scratch and the version used in SEs was the initial version of the GUI. Although the timeframe of the project was short for development, the GUI was improved for each SE and more tools were integrated into the GUI. At the end of the development phase in this project, the GUI was seen user friendly and one of the advantages it has (together with the Distributed Messaging System (DMS) component of the S4RIS platfrom is the integration of several tools in one platform.

This deliverable concludes the workpackage dedicated to SEs and evaluations with end-users. In it the SAFETY4RAILS end-user, stakeholder and developers cooperated to design, implement and evaluate the results of SEs with the S4RIS platform and its contributory tools, based on S4RIS platform component and tool

provider's readiness and willingness to take part in the SEs, against the core requirements/specifications identified earlier in the project. The SEs were based on what the end-users considered real operational environment challenges in the domain of rails on an everyday and authentic real work basis. In our evaluation, the SEs demonstrated that SAFETY4RAILS delivered the expected results very well, advancing the implementation of and providing a solid basis for the future tools and services and related continuums. In addition, SAFETY4RAILS project offered its participants and stakeholders valuable insights into the development of the capabilities in the rail domain.

In the post-project phases, SAFETY4RAILS plans to build on the feedback received within the duration of the project and to mitigate against limitations in the targeted audiences and collected feedback (and specifically the number of replies from the simulation exercises). This is to be achieved as an integral part of the exploitation plans which includes further dissemination and communication (as described in section 8).

Bibliography

Crabbe et al., SAFETY4RAILS Information System platform demonstration at Madrid Metro simulation exercise, 32nd European Safety and Reliability Conference 2022, *preprint*.

Department of Communications, Climate Action & Environment, NIS Compliance Guidelines for Operators of Essential Service (OES), available at: https://assets.gov.ie/76729/ea0bcd3b-0161-41d2-8c51-df00e558689c.pdf (last accessed 20/07/2022).

European Commission (2007). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe. COM(2007) 799 final, availabe at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0799:FIN:EN:PDF (last accessed 21/03/2023).

International Organization for Standardization Ergonomics of human-system interaction: part 11: usability: definitions and concepts (ISO/DIS 9241-11.2:2016). German and English version prEN ISO 9241-11:2016.

International Organization for Standardization.ISO 22301:2019 – Security and resilience – Business continuity management.

SAFETY4RAILS Deliverable D1.4 Specification of the overall technical architecture (October 2021).

SAFETY4RAILS Deliverable D2.5 Specific requirements for multimodal transport systems (June 2021).

SAFETY4RAILS Deliverable D6.4 Final developmental validation and evaluation of the S4RIS systemy (Draft version September 2022).

SAFETY4RAILS Deliverable D8.1 Evaluation methodology (December 2021).

SAFETY4RAILS Deliverable D8.2 First version – development of a blueprint exercise handbook (February 2022).

SAFETY4RAILS deliverbale D10.3 Second update of the dissemination and communication plan (October 2022).

SAFETY4RAILS Deliverable D10.8 Market analysis and business plan (October 2022).

SAFETY4RAILS Deliverable D10.9 Exploitation Strategy (January 2023).

SAFETY4RAILS Grant Agreement, version 2.0 with amendment (June 2021).

Postman Inc., What is Postman? 2022, available at: https://www.postman.com/product/what-is-postman/ (last accessed 13/04/2022).

ANNEXES

ANNEXI Glossary and Acronyms

TABLE 8 GLOSSARY AND ACRONYMS

Term	Definition/description
BCM	Business Continuity Management
CdM	Comune di Milano
CCTV	Closed-circuit television (video surveillance)
CD	České dráhy
DBAG	Deutsche Beteiligungs AG
DMS	Distributed Messaging System
DoA	Description of the Action (Annex 1 to the Grant Agreement)
DR	Disaster Recovery
DVR	Digital Video Recorder
EGO	Ankara Metro
FGC	Ferrocarrils de la Generalitat de Catalunya
CM	Crises Management
GUI	Graphical User Interface
IED	Improvised Explosive Device
INFRABEL	Belgian government-owned public limited company
IT	Information Technology
JSON	JavaScript Object Notation
MdM	Metro de Madrid
NGT	Nominal Group Technique
NS	Nederlandse Spoorwegen
OT	Operational Technology
PKP	PKP Intercity, Train transport company, Poland
PRORAIL	Rail Infrastructure Manager in the Netherlands
PtMP	Point-to-MultiPoint
RATP	Public transport operator and maintainer, France
RFI	Rail Infrastructure Manager in Italy
SE	Simulation Exercise
SNCF	Railway company, France
S4RIS	SAFETY4RAILS Information System
TCDD	State Railway in Turkey
TOC	Train Operating Company

UC	UseCase
UIC	International union of railways
UITP	The International Association of Public Transport
UR	User Requirement
WP	WorkPackage
WS	Workshop
CAMS	Central Asset Management System

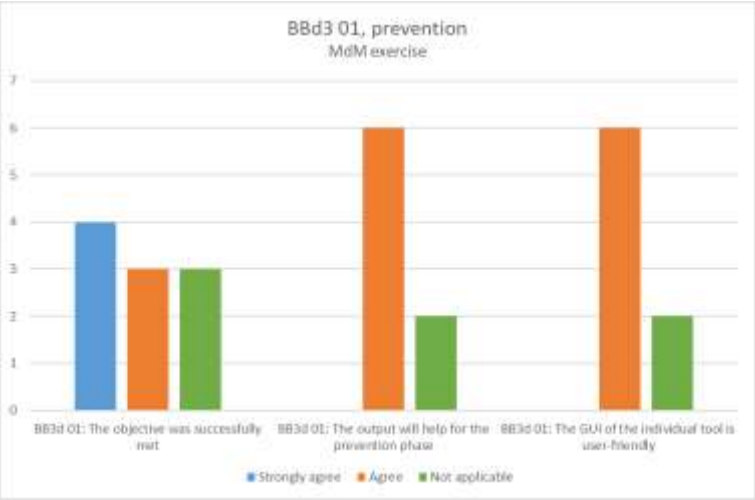
ANNEX II Madrid (MdM) exercise schedule

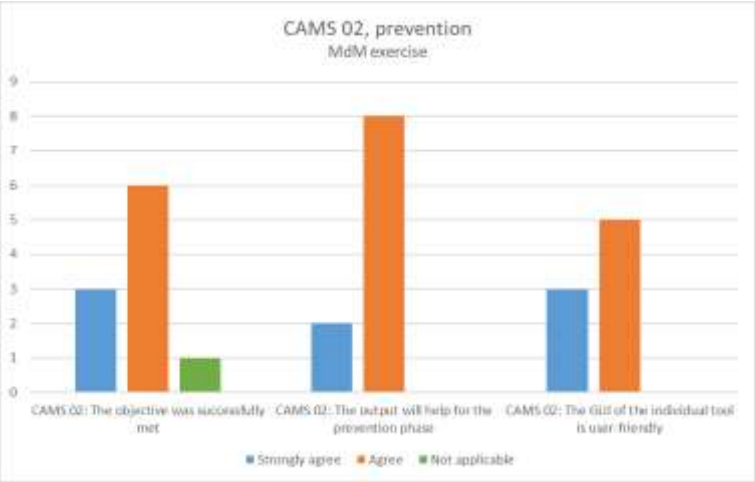
14:00	**Opening ceremony including presentation of agenda and methodology**				MdM, FhG[15], ETRA
PREVENTION PHASE - WORKSHOPS/TRAINING					
14:30	BB3D-Bomb Blast Simulation without door and indoor effects (Civil Construction Department)	RINA	14:30	iCrowd - Outdoor stampede due to bomb blast. Assessment CCTV configurations for detecting blindspots (SecurityDepartment)	NCSRD
15:20	CAMS - Proactive asset management and preparedness (Maintenance Department)	RMIT	15:20	SecuRail-Offline risk assessment (Security Department)	STAM
16:10	TISAIL/OSINT-Identification of existing vulnerabilities in the cyber domain (ALL)				TREE/INNO
16:40	PRIGM-Detailed report regarding hardware-based vulnerabilities, supporting countermeasures (ALL)				ERARGE
17:10	First debriefing session with end-users for evaluation (ALL)				LAU
17:40	End of secondday				
THURSDAY 10th - SIMULATION EXERCISE (ALL)					
PREVENTION PHASE-WORKSHOPS/TRAINING					
08:30	DATAFAN-Prediction of passenger flow in stations and related what-if-scenarios (ALL)				FhG
09:00	CaESAR-Cascading effects and resilience analysis (ALL)				FhG
09:50	RAM2-Vulnerability and security gaps assessment (ALL)				ELBIT
10:40	Second debriefing session with end-users for evaluation (ALL)				LAU
11:10-11:20	Break				
RESPONSE & DETECTION PHASE - FUNCTIONAL SIMULATION EXERCISE					
11:20-11:35	WINGSPARK–General Presentation (ALL)				WINGS

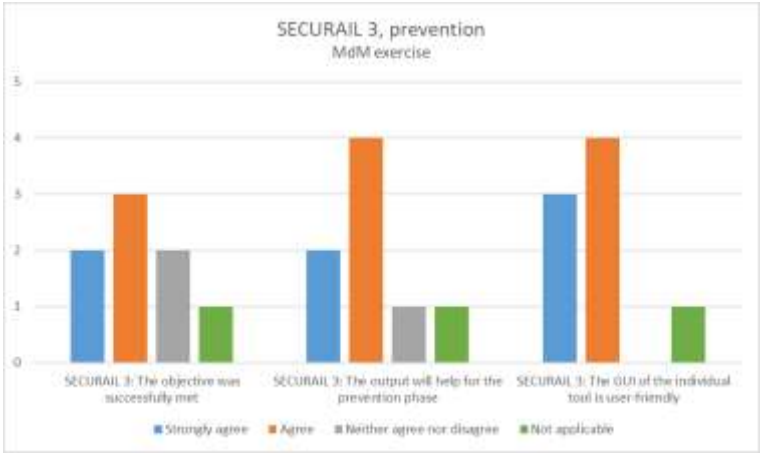
[15] Here and in other places in the Annexes the Fraunhofer acronym has been shortened to FhG.

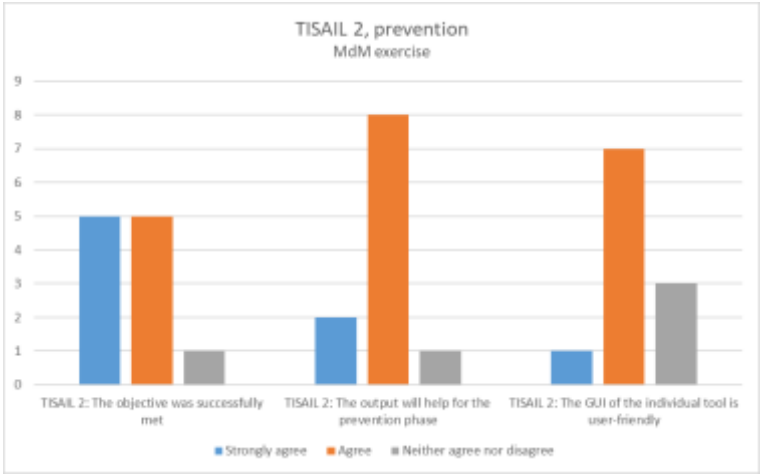
11:35-11:50	CuriX – GeneralPresentation (ALL)				IC
11:50-12:00	SAFETY4RAILS Information Systems (S4RIS) Graphical User Interface				UNEW
12:00	S4RIS platform (+alltools*) tackling a combined cyber-physical attack (ALL)				* IC, ELBIT, TREE/INNO, WINGS, NCSRD, FhG
13:30	Third debriefing session with end-users for evaluation (ALL)				LAU
14:00-15:00	Lunch break				
RECOVERY PHASE - WORKSHOPS/TRAINING					
15:00	BB3D-Bomb Blast Simulation with outdoor and indoor effects (Civil Construction Department)	RINA	15:00	CAMS - Proactive asset management and preparedness (Maintenance Department)	RMIT
15:50	Final debriefing session with end-users for evaluation (ALL)				LAU
17:00	End of last day				

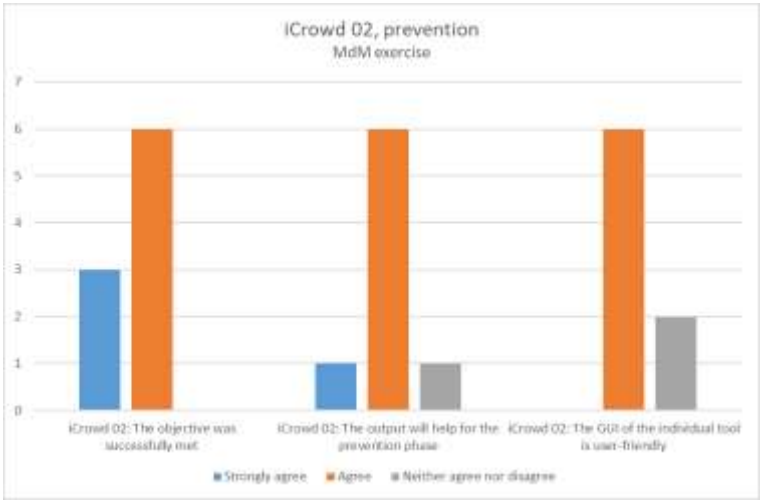
MDM PREVENTION PHASE QUESTIONNAIRES 1 AND 2

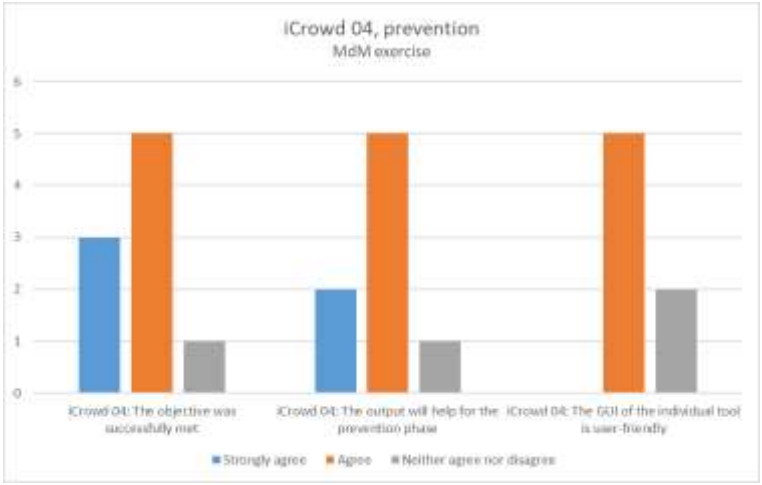
BB3d	**Objective :** Provide bomb blast simulations in order to understand how a bomb could affect the metro infrastructure, particularly the tunnels and the development of an event. This information will further support the Civil Construction Department in MDM for building more resilient physical structures (e.g. the tunnels) and reduce damage to passengers.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • The simulation • Making the connection with impact/frequency in relation to deaths and (fatal) injuries • I specialize in the cybersecurity part so, although I found it to be an interesting tool, I do not have the necessary knowledge to determine what the added value would be for the prevention phase. How could this tool be improved in the context of this scenario? • Maybe can be implemented cascading effects of blast • Running it with even more accurate data and comparing

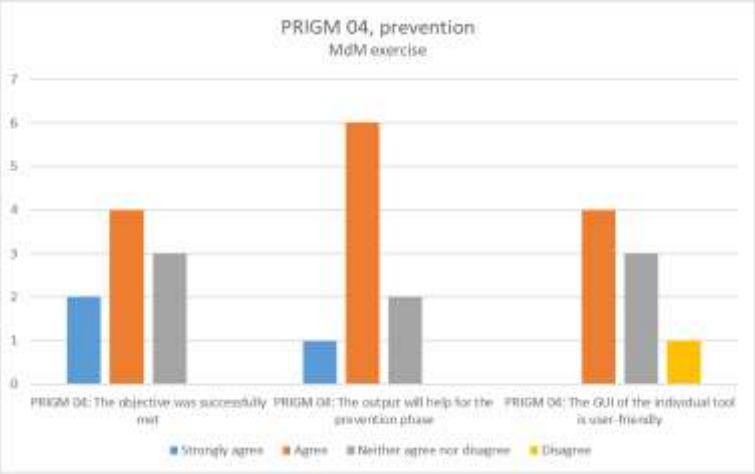
CAMS	**Objective :** The individual tool will be used to inform the metro operator to allocate to repair/maintain/ rehabilitate the infrastructure after a set of possible events, therefore providing the necessary input to make a proactive plan and be ready in case of an attack. The metro operator will also be provided with information regarding the asset condition and degradation due to normal ageing, enabling timely response ahead of malfunctioning.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • The economic study • It helps a lot to plan budgets in advance • I think it could improve asset obsolescence management, especially those in OT environments How could this tool be improved in the context of this scenario? • Running it with more accurate data • Integration with the SAP, databases and inventory systems used in the Maintenance Department of Metro de Madrid

SECURAIL	**Objective :** Enable off-line risk analysis of the metro infrastructure to understand the level of risk for each critical asset during a given hazardous event.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Prior information • Automatic risk assessment • Making the impact of a scenario and the measures that can be taken quantitative. This makes it possible to compare different measures and make choices. • I think there is an added value in the GUI. It is quite user friendly and it certainly helps to see the interrelations between the assets and the potential cascading effects. It is an easy way to view all your assets while assessing potential mitigation measures. Of course, the user of this tool needs to know the assets quite well. • Help to carry out risk analyses in a more agile and centralized way. How could this tool be improved in the context of this scenario? • There are many variables to consider • With preconfigured assets and prices. For example, If user select room, it can automatically add door, window etc. • At some point I found hard to follow how the damage costs of the assets are calculated, but it was perhaps due to the fact that the tool was being presented live. I guess I found that some values that are interpretable have to be introduced by the end-user. • In the cyber part, I would recommend that the tool be aligned (if it is not already) with the IEC-62443-3-2 standard and with TS 50701. That is, that it allows grouping assets into zones, which should also be taken into account vulnerabilities, etc.

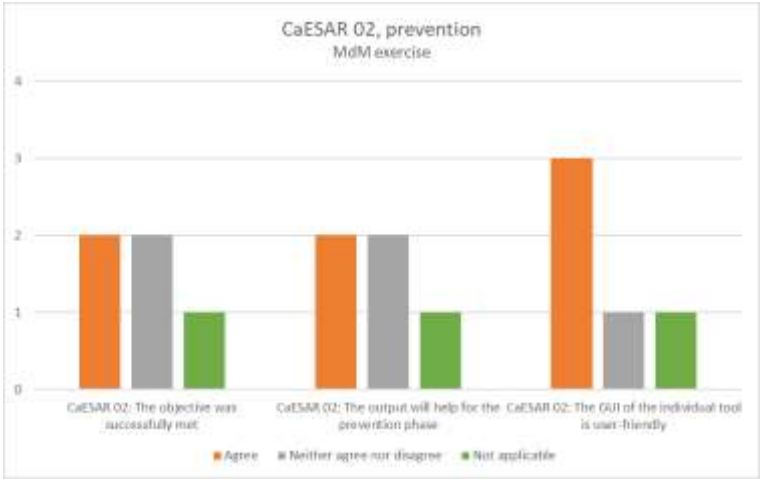
TISAIL	**Objective :** Provide vulnerability and security gaps assessment, along with risk assessment for each of the operational units in the metro system.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Automatic detection • Discover possible or additional vulnerabilities not detected by existing IT software in Metro de Madrid • Cybersecurity is relatively new into our company. Having a threat intelligence service to detect vulnerabilities can certainly help creating awareness for these threats and expand the cyber security knowledge among the Railway Operators • We are currently using a similar tool (it also feeds into, among others, the MISP platform). We understand that this tool would not provide us with added value. How could this tool be improved in the context of this scenario? • Integration with existing tools (monitoring, alarm systems, etc.) in Metro de Madrid

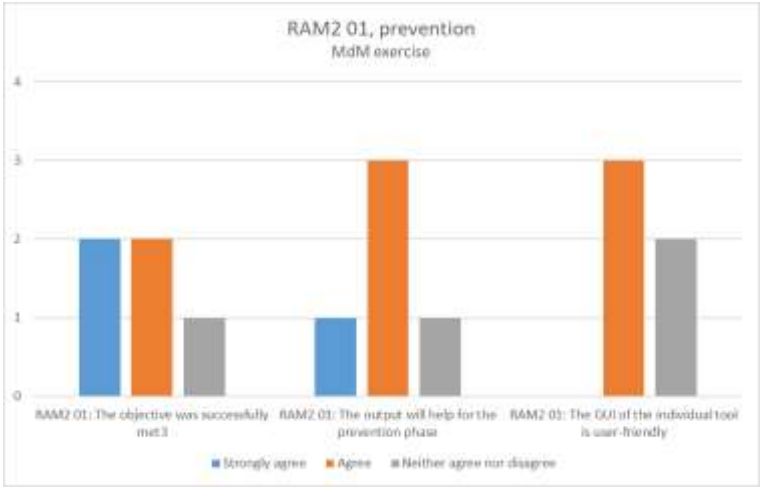
iCrowd	**Objective :** Provide simulation capabilities to understand better the chances of detection during infiltration/escape per configuration (camera and guards locations) and infiltration/escape total times.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Preparation of devices • Understanding crowd behaviour in stations where the platform area is closed with gates and turnstiles could help understand if there is adequate exit space to evacuate from the platform. • iCrowd seems like an easy way to simulate the crowd behaviour for different events. The fact that the tool is user friendly and complete in terms of detail (pressure map, waiting times…) can mean that a railway operator can check this tool when considering modifications in the infrastructure. • Taking into account that this tool applies more to the physical security part, I cannot value it because I specialize above all in the cybersecurity part. How could this tool be improved in the context of this scenario? • Take into account more variables • Not sure if trampling is an effect already implemented as I only heard it mentioned once, but could be something to help estimate potential casualties at exits or chokes. • Not sure if it has this already, but it could maybe get fed from RT data and update the input data accordingly. But maybe it already has this and I missed it in the session.

iCrowd	**Objective :** Revealing blind spots and other related vulnerabilities in case of a threat actor trying to escape.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Blind spots are consistently a problem when planning CCTV in stations. Could be potential for efficient camera placement in stations. • Useful to check the blind spots. Don't think we have a similar solution. How could this tool be improved in the context of this scenario? • N/A

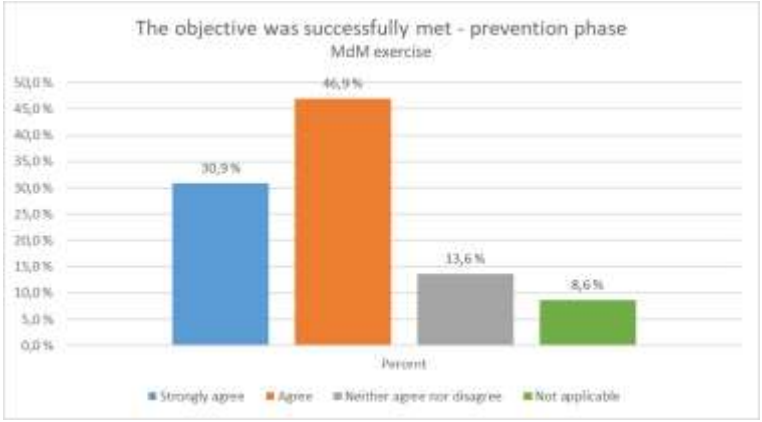
PRIGM	**Objective :** Provide detailed report regarding vulnerabilities and attack surfaces within the system (mainly hardware-based attacks), supporting Network Security Expert or Cybersecurity Officer in the definition and development of countermeasures against cyber and/or cyber-physical attacks.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Discover additional vulnerabilities in Metro systems • I found it difficult to see the tool part here. It looked like a clever registration of scenario's and visualization of a system which it seems could also be done in excel and PowerPoint. With all due respect to the presenter. • The added value would be that, for example, a cybersecurity responsible can detect vulnerabilities from hardware asset • I think it could improve the security of communications How could this tool be improved in the context of this scenario? • Integration in COMMIT systems

DATAFAN	**Objective :** Provide information about the expected number of passengers to happen in the day of the sporting event. The end-user will be able to run what-if scenarios to analyse how they will affect the number of passengers and delays in the infrastructure (e.g., the closure of a station). For a more precise prediction of the delays, the output data from iCrowd (NCSRD) will be used.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Prior knowledge of events • Planning capability of the schedule can be increased • I think it's an easy tool to use to evaluate different scenarios • This tool is very closely connected to station management. Since station management in the Netherlands is the responsibility of the main TOC, this tool would not be used by ProRail. However, I can image the information that the tool generates could be useful in deciding about measures with regard to passenger flow in stations. • I understand that this tool applies to the physical security part, so it does not apply to the cybersecurity part. For this reason, I cannot comment on it. How could this tool be improved in the context of this scenario? • Take into account more variables in the movements • Maybe the recommendations for the end-user when a simulation is run could be applied automatically

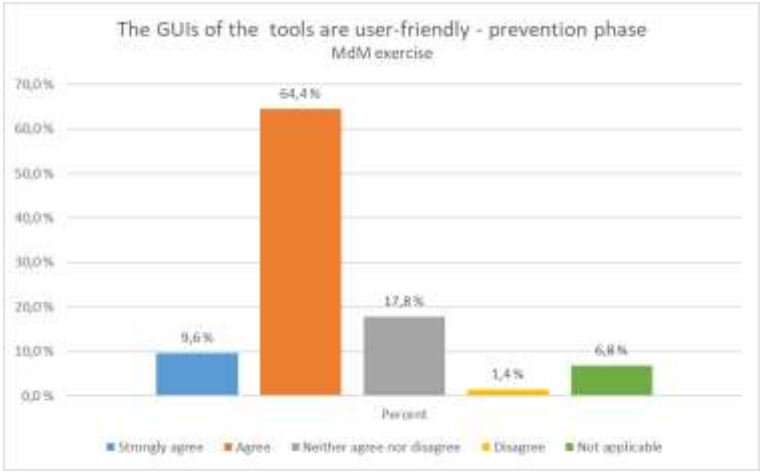
CaESAR	**Objective :** The weakest/most critical components and associated cascading effects will be identified. An overall resilience analysis of the infrastructure will be done before the event.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Anticipation of situations • Help to take predictive actions (precautions) • I would like to review the tool because I missed the presentation. • Quantifying resilience and rating measures is very much done on the basis of expert judgement. Added value of this tool is that this judgement can be backed up by data. This would make the acceptability of measures easier. • I understand that the tool will provide us with added value when it includes both the physical and cybersecurity aspects. In that case, it would allow us to assess the impact from the point of view of comprehensive security. How could this tool be improved in the context of this scenario? • Quick response • Better integration with other tools

RAM2	**Objective :** Provide vulnerability and security gaps assessment, along with risk assessment for each of the operational units in the metro system.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Help to enhance the risk management • The added value is that users with little knowledge about cybersecurity can find motivation in creating awareness and tackling the vulnerabilities • It was difficult to assess the value of this tool for my organisation. I can image that it has its values but colleagues from the IT department are more able to judge that • Although I should analyse the tool in more detail, I understand that the added value would be high since it would help us automate certain risk and vulnerability management tasks. How could this tool be improved in the context of this scenario? • I will check more in detail

Overall achievement of objective and GUIs for prevention phase

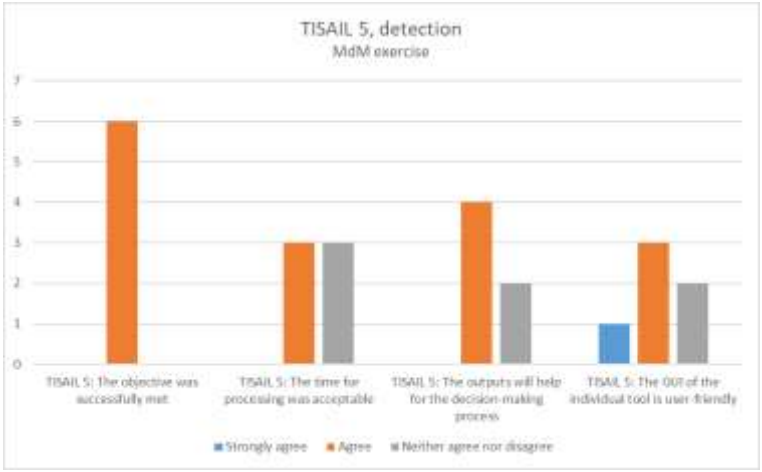


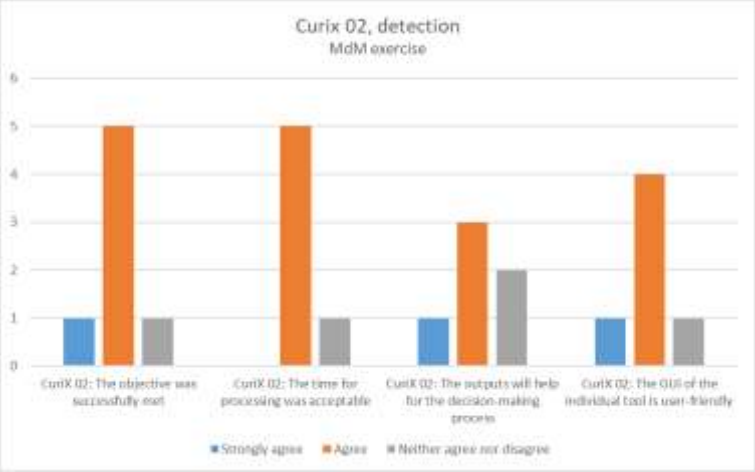
The achievement of the objectives of all the tools in Prevention phases 1 and 2 based on the feedback of the tools' evaluation is presented in the figure. The percentages are based on the replies of 13 respondents in Prevention phase 1 and five (5) in Prevention phase 2. "Not applicable"-answers are because not all the respondents have participated to every tool's performance, or the objective has been unclear.

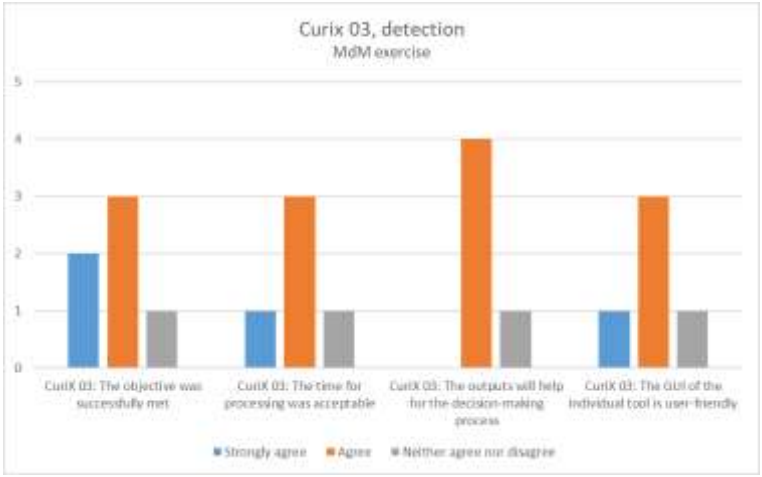


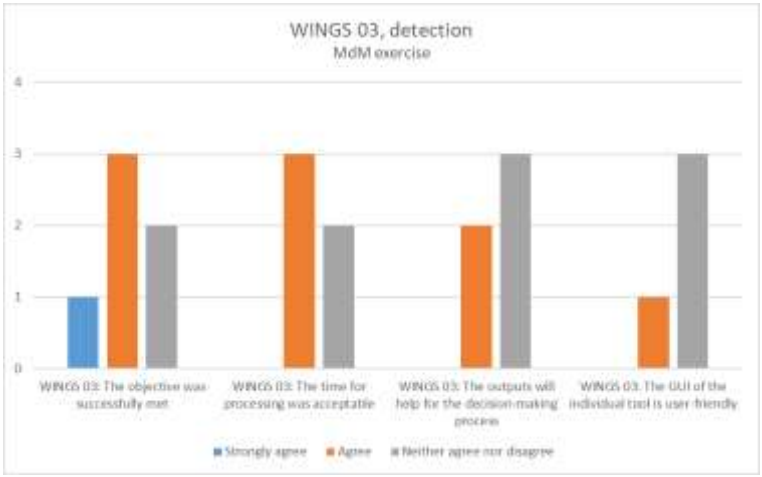
The achievement of the objectives of all the tools in Prevention phases 1 and 2 based on the feedback of the tools' evaluation is presented in the figure below. The percentages are based on the replies of 13 respondents in Prevention phase 1 and five (5) in Prevention phase 2. "Not applicable"-answers are because not all the respondents have participated to every tool's performance, or the objective has been unclear.

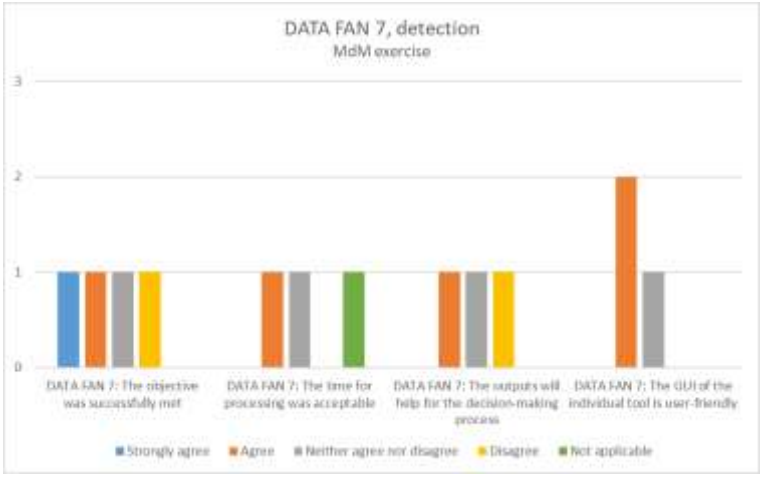
MDMDETECTION AND RESPONSE PHASE QUESTIONNAIRE 3

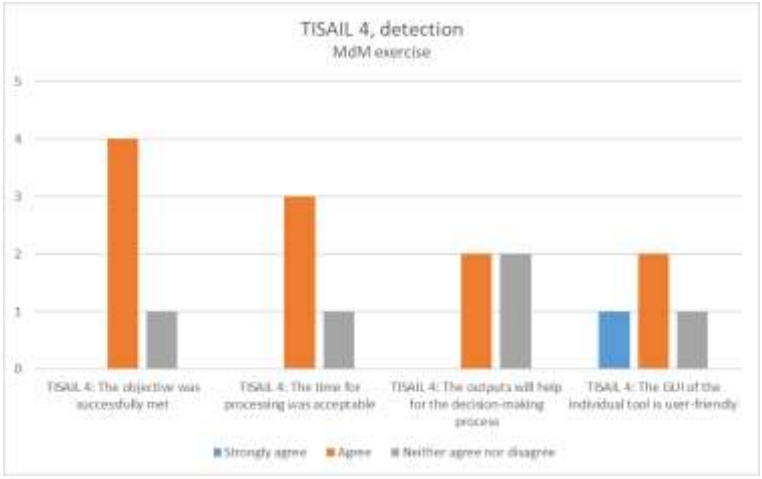
TISAIL	**Objective :** Inform the Crisis Manager about possible spear-phishing campaigns targeting mail domains of the MDM personnel.
	What would be your acceptable time to be processed? • 30 minutes • In real time What is the added value to the detection/response phase that you know from your current daily work? • We already have systems like this • Automatic detection • Have information to be able to assess the possible impact of threats and make decisions about the need or not to implement additional measures What could be improved in the context of this scenario? • N/A

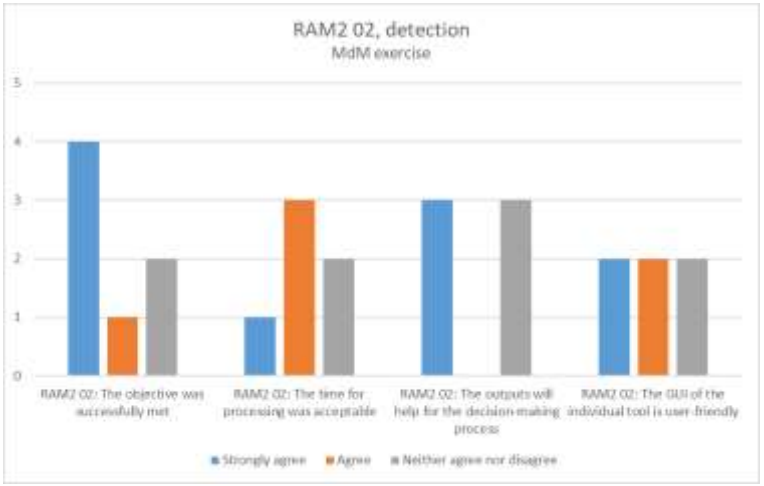
CuriX	**Objective :** Crisis Manager will be alerted when deviations from normal behaviour (anomalies) or potentially upcoming disruptions of technical systems (IT and OT) from their monitoring data are detected. The crisis manager can check metrics and which technical devices are responsible for causing the major change in the system behaviour. In the scenario, detection of anomalies regarding sound intensity level, state of the doors and lights.
	What would be your acceptable time to be processed? • 5 minutes • In real time What is the added value to the detection/response phase that you know from your current daily work? • real time information to support decision making • No added value, we already receive alerts. • To be able to take precautions • Detection of anomalies with CCTV systems and servers could assist with detecting when these systems are not functioning at the stations especially at remote sites. • It would allow the detection of security incidents in real time, which would allow us to implement corrective / mitigation actions. What could be improved in the context of this scenario? • N/A

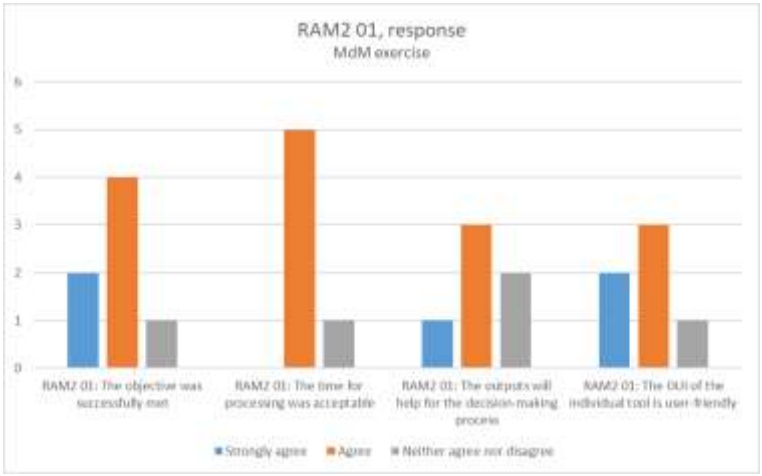
CuriX	**Objective :** The crisis manager can monitor the health of the monitored technical system.
	What would be your acceptable time to be processed? • 5 minutes • In real time What is the added value to the detection/response phase that you know from your current daily work? • real time information to support decision making • No added value, we already receive this alerts • Overview • Early detection • I was unable to attend this part of the drill What could be improved in the context of this scenario? • N/A

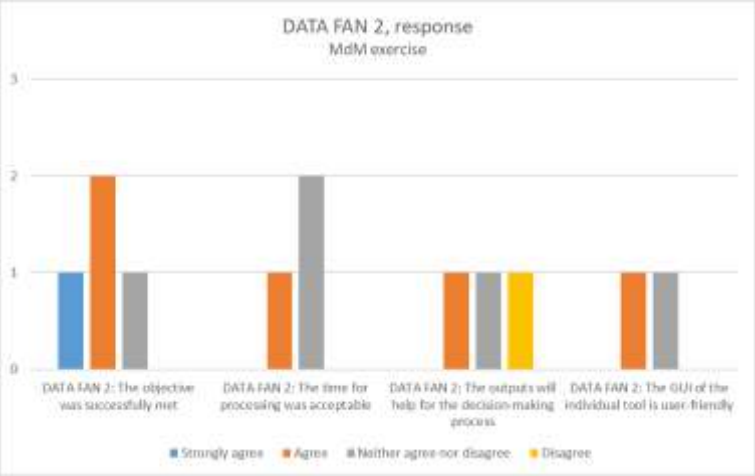
WINGSPARK	**Objective :** Analyse anomalies in the train speed so that an alert can be sent to the system team/driver. Check if there is an overcrowded area in the facility and raise an alert.
	What would be your acceptable time to be processed? • 5 minutes • Real time • Within minutes What is the added value to the detection/response phase that you know from your current daily work? • No added value, system already send alerts • To be able to take precautions • Identifying overcrowding rapidly can assist with resource management of personnel in stations and create response strategies to alleviate the overcrowding. • I cannot rate this tool since my experience is related to the field of cybersecurity. What could be improved in the context of this scenario? • N/A

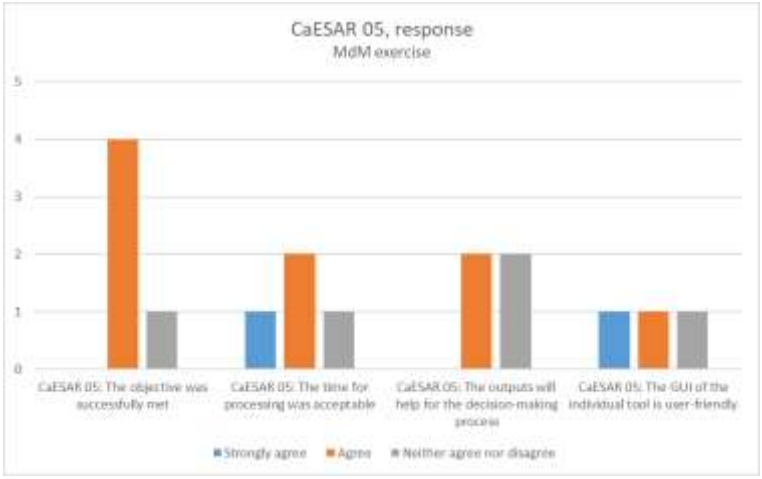
DATAFAN	**Objective :** Data gathered regarding the flow of passengers will be used to detect significantly high passenger volumes in stations and trains, also considering days with really crowded events.
	What would be your acceptable time to be processed? • already answered What is the added value to the detection/response phase that you know from your current daily work? • Better insights • This information is not useful when you are in an event • I cannot rate this tool since my experience is related to the field of cybersecurity. What could be improved in the context of this scenario? • No added value, we already work with this information in real time

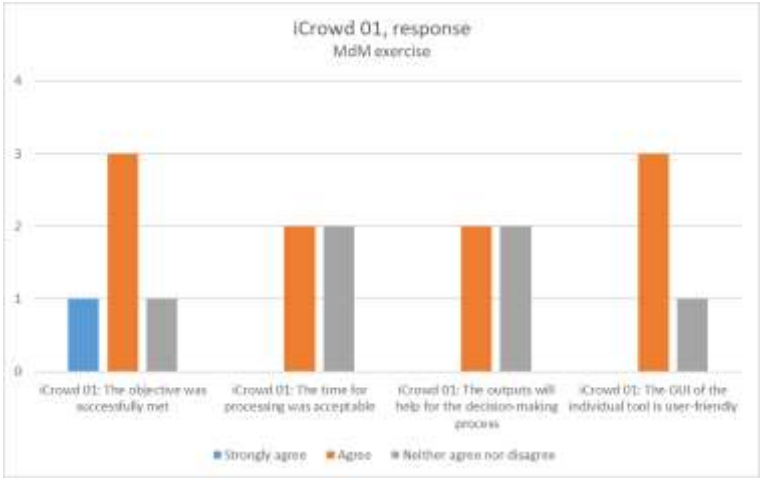
TISAIL	**Objective :** The Crisis Manager will be able to correlate the information (e.g., IoCs) provided by TISAIL for detecting threats in their networks using their security tools (e.g., IDS, SIEMs). CCTV camera vulnerability detected in the scenario. **Objective :** Provide detailed report regarding vulnerabilities and attack surfaces within the system (mainly hardware-based attacks), supporting Network Security Expert or Cybersecurity Officer in the definition and development of countermeasures against cyber and/or cyber-physical attacks.
	What would be your acceptable time to be processed? • already answered • In real time What is the added value to the detection/response phase that you know from your current daily work? • No added value, we already have this information. • Faster response • Early detection • We currently have a tool similar to this, so it would not provide us with added value. However, we understand that it can bring a lot of added value to other companies. What could be improved in the context of this scenario? • N/A

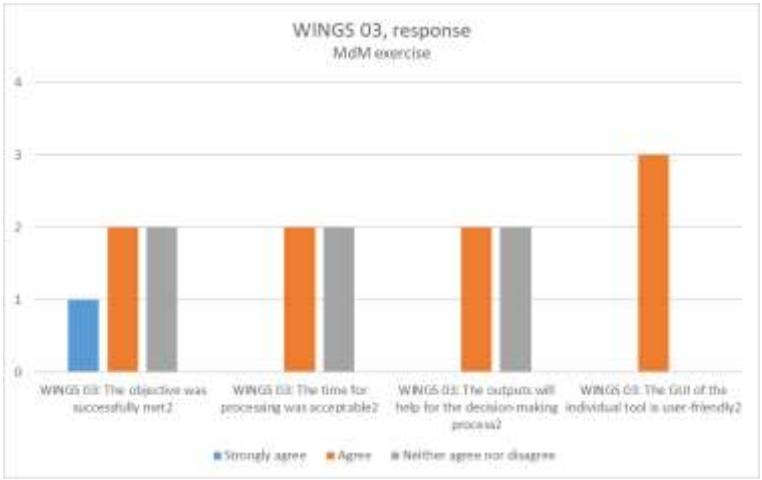
RAM2	**Objective :** Correlation of data gathered from multiple monitoring sources in order to detect potential threats. For example, it will be able to correlate the different attack vectors happening in the station.
	What would be your acceptable time to be processed? • minutes • Real time What is the added value to the detection/response phase that you know from your current daily work? • Reduces time of response • No added value in an event • Anything to help ease the correlation of events for proactive responses will assist station managers and security teams stay on top of or ahead of threats • High added value. We would have the necessary information to assess the impact from the point of view of comprehensive security. What could be improved in the context of this scenario? • N/A

RAM2	**Objective :** Risk-based prioritisation of issues, case management for tracking response actions. End-user consumes the data through RAM2 Dashboards display. The user follows the prioritised alerts and mitigation steps for each of the alerts for risk reduction and response to detection of ongoing threats.
	What would be your acceptable time to be processed? • 5 minutes • Real time What is the added value to the detection/response phase that you know from your current daily work? • realtime information to support decision making • More accurate decisions • High added value. We would have the necessary information to define the action plan prioritizing the risks with the greatest impact. What could be improved in the context of this scenario?

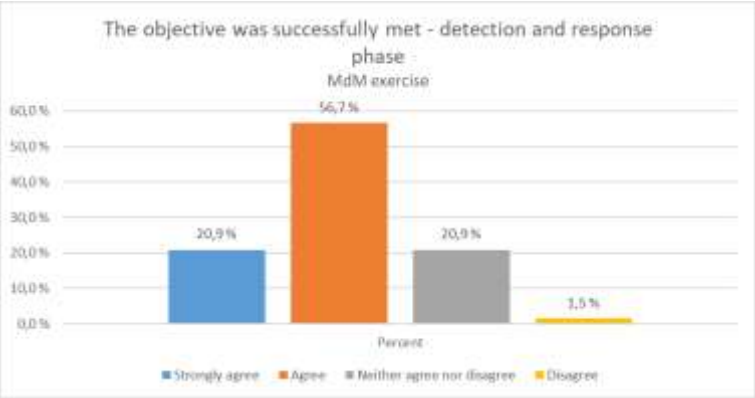
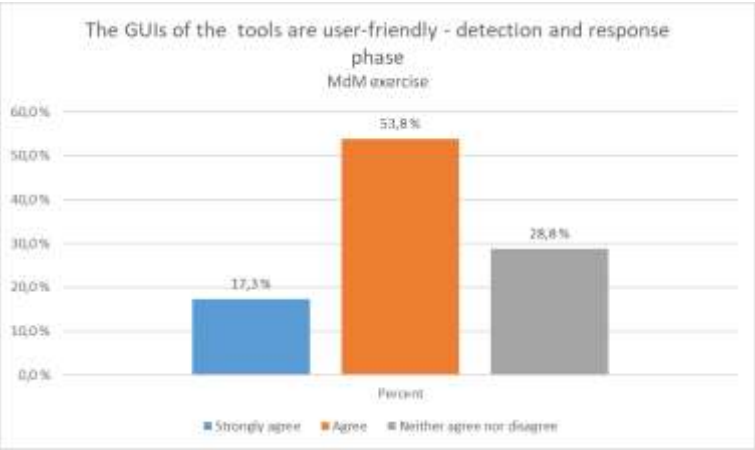
DATAFAN	**Objective :** Predict the passenger load in real-time in other stations once another is closed, helping to better respond the situation and re-locate the passengers.
	What would be your acceptable time to be processed? • already answered • 15 minutes What is the added value to the detection/response phase that you know from your current daily work? • More helpful decisions • It depends on the event. • I cannot rate this tool since my experience is related to the field of cybersecurity. What could be improved in the context of this scenario? • N/A

CaESAR	**Objective :** Evaluate mitigation steps regarding their influence on the resilience, including cascading effects computation. As a pre-condition, CAESAR will count with the system topology provided by SecuRail.
	What would be your acceptable time to be processed? • already answered • 5 minutes • Real time What is the added value to the detection/response phase that you know from your current daily work? • No need of software, it depends on the incident. • Better insights • It depends on the event and how are you managing • We understand that this tool applies more to the physical security part. However, we consider that it could help us assess the impact from the point of view of comprehensive security. What could be improved in the context of this scenario? • N/A Further note based on on-site discussions: The CAESAR application was not considered as relevant for use during an ongoing threat. Concerns about application during an ongoing crisis was expressed. Primarily, end-users require fast and efficient decision-support and crisis management capabilities. Simulation tools not connected to real-time data were considered more relevant for dimensioning spaces and defining strategies in the Prevention phase.

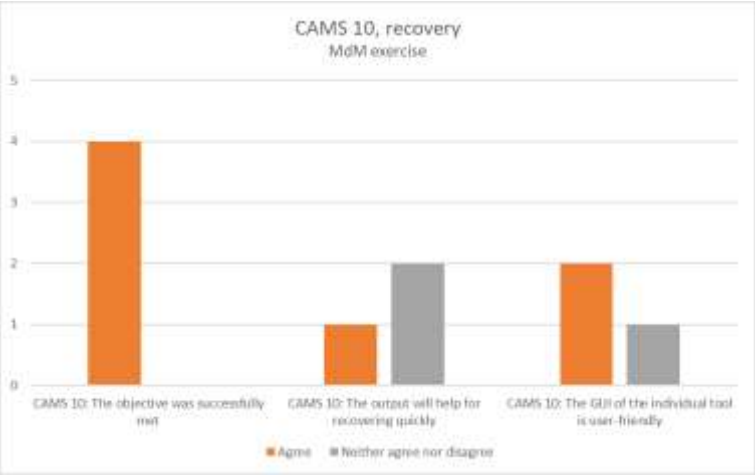
iCrowd	**Objective :** Crowd simulator providing advanced insights regarding crowd movement and behaviour for a set of boundary conditions related to the event.
	What would be your acceptable time to be processed? • 15 minutes • Real time What is the added value to the detection/response phase that you know from your current daily work? • real time information to support decision making • Information only useful for design phase, nor in incident management • More accurate decisions • It depends on the event and the managing process • I cannot rate this tool since my experience is mainly related to the field of cybersecurity. What could be improved in the context of this scenario? • N/A

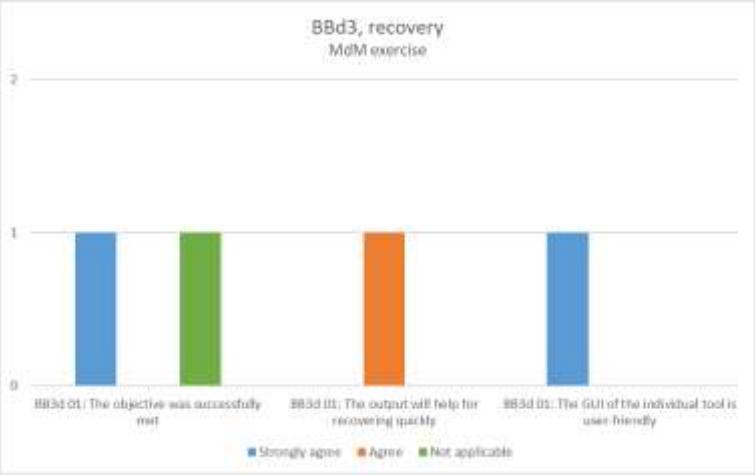
WINGSPARK	**Objective :** Provide details, alerts of the detected issue in the train speed to aid the response action. Alerts are also raised in the case of overcrowded areas and guidelines in case of evacuation are provided.
	What would be your acceptable time to be processed? • 15 minutes • Real time What is the added value to the detection/response phase that you know from your current daily work? • real time information to support decision making • More accurate decisions • It depends on the kind of event and the managing process • I cannot rate this tool since my experience is mainly related to the field of cybersecurity. What could be improved in the context of this scenario? • N/A

Overall achievement of objective and GUIs for detection and responsephase

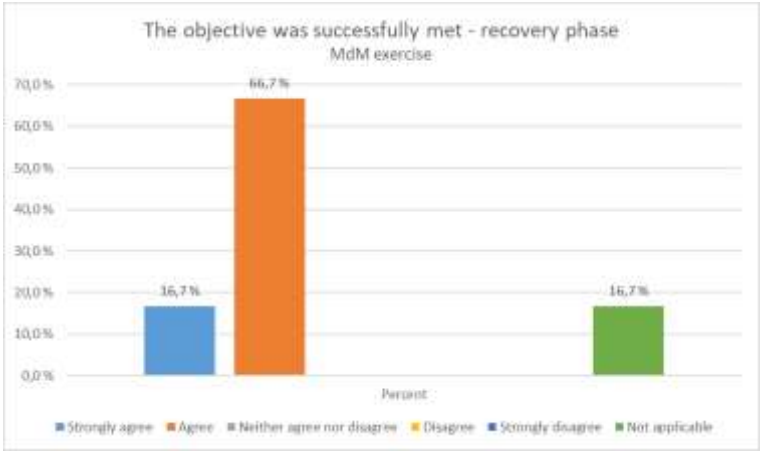
	The achievement of the objectives of all the tools in Detection and Response phase based on the feedback of the tools' evaluation is presented in the figure. The percentages are based on the replies of seven (7) respondents.
	The end-users' opinion of the tools' GUIs in Detection and Response phase based on the feedback of the tools' evaluation is presented in the figure. The percentages are based on the replies of seven (7) respondents.

MDMRECOVERY PHASE QUESTIONNAIRE 4

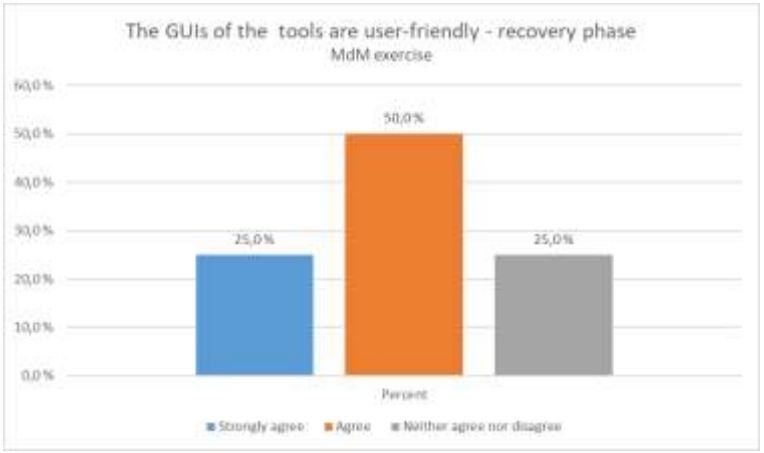
CAMS	**Objective :** Crisis Manager will be provided with time and cost needed to respond to the crisis and restore normal functioning, so that resource deployment and reaction is based on proactive actions planned. Railway operator will be aware of vulnerability and fragility of the asset after the incident, so to improve resource deployment and control financial loss in the future.
	What is the added value to the recovery phase that you know from your current daily work? • At this moment I would see the added value in the general LCC management of infrastructure and not specifically with regard to crisis management • It would facilitate decision-making regarding the action plan to undertake to manage the crisis. What could be improved in the context of this scenario? • N/A

BB3d	**Objective :** Safety managers in the metro system will leverage the information provided by the bomb blast simulations in order to create mitigation countermeasures (e.g. safety distance, protective hardening, etc.). Number of casualties and people injured for out-door bomb attack scenarios are provided.
	What is the added value to the recovery phase that you know from your current daily work? • N/A What could be improved in the context of this scenario? • N/A

Overall achievement of objective and GUIs for recovery phase



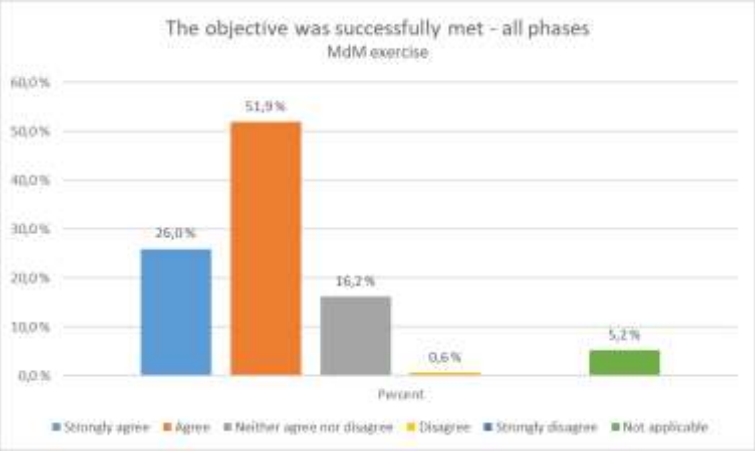
The achievement of the objectives of all the tools in Recovery phase based on the feedback of the tools' evaluation is presented in the figure. The percentages are based on the replies of five (5) respondents. "Not applicable"-answers are because not all the respondents have participated to every tool's performance, or the objective has been unclear.



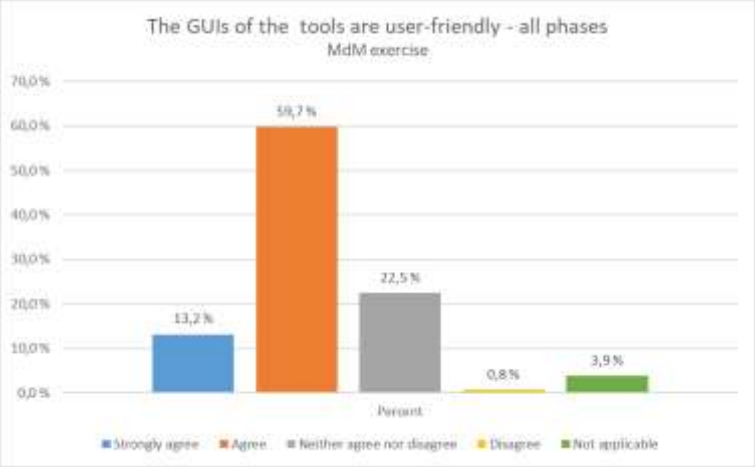
The end-users' opinion of the tools' GUIs in Recovery phase based on the feedback of the tools' evaluation is presented in the figure. The percentages are based on the replies of five (5) respondents.

MDM RESILIENCEPHASES

Overall achievement of objective and GUIs all resilience phases: prevention, detection & response, recovery

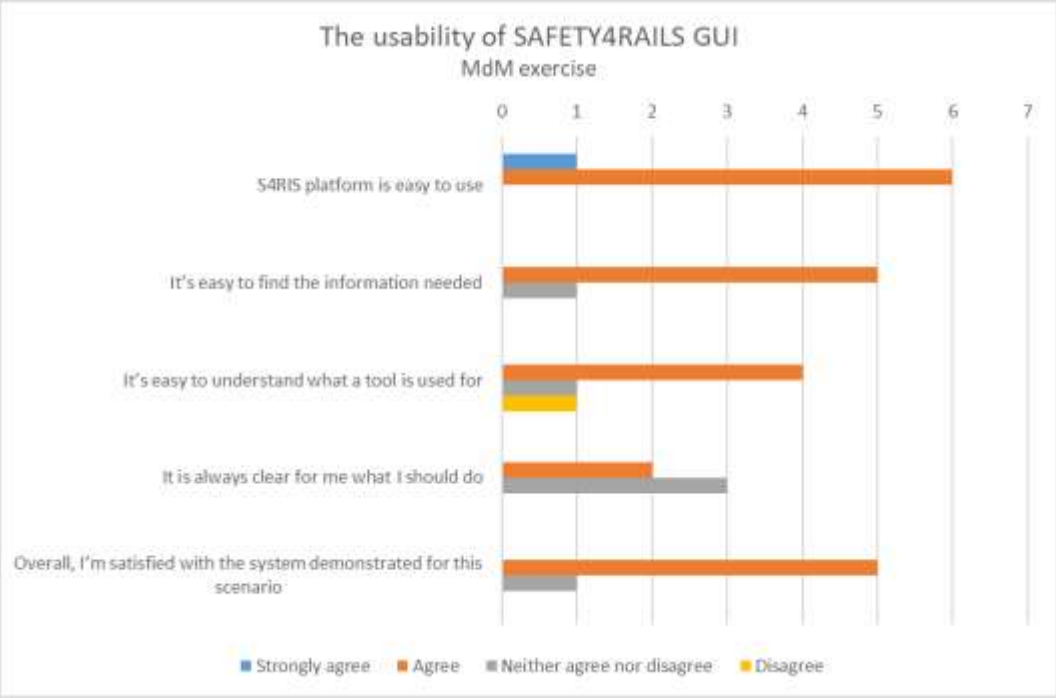


The achievement of the objectives of all the tools and in all the phases commonly based on the feedback of the tools' evaluation is presented in the figure. The percentages are based on the replies of 16 respondents who have answered to this question: 13/16 in Prevention phase 1, 5/16 in Prevention phase 2, 7/16 in Detection and Response phase and 5/16 in Recovery phase.

	The end-users' opinion of the tools' GUIs generally based on the feedback of all the tools is presented in the figure. The percentages are based on the replies of 16 respondents who have answered to this question: 13/16 in Prevention phase 1, 5/16 in Prevention phase 2, 7/16 in Detection and Response phase and 4/16 in Recovery phase.

MDM SAFETY4RAILS GUI AND PLATFORM SPECIFIC QUESTIONNAIRE4

GUI



What could be improved in the GUI?

- The overall managing process
- More end-users
- The GUI is clear. I think it is a good GUI and all the tools are clear.
- I'd have to look at the tools in more detail to give an answer. In general, I found the graphical interface of all the tools to be friendly.

What complexity / functions are not necessary and can be deleted or reduced?

- Passenger flows is not realistic in an event or emergency
- Perhaps more adapted to the crisis

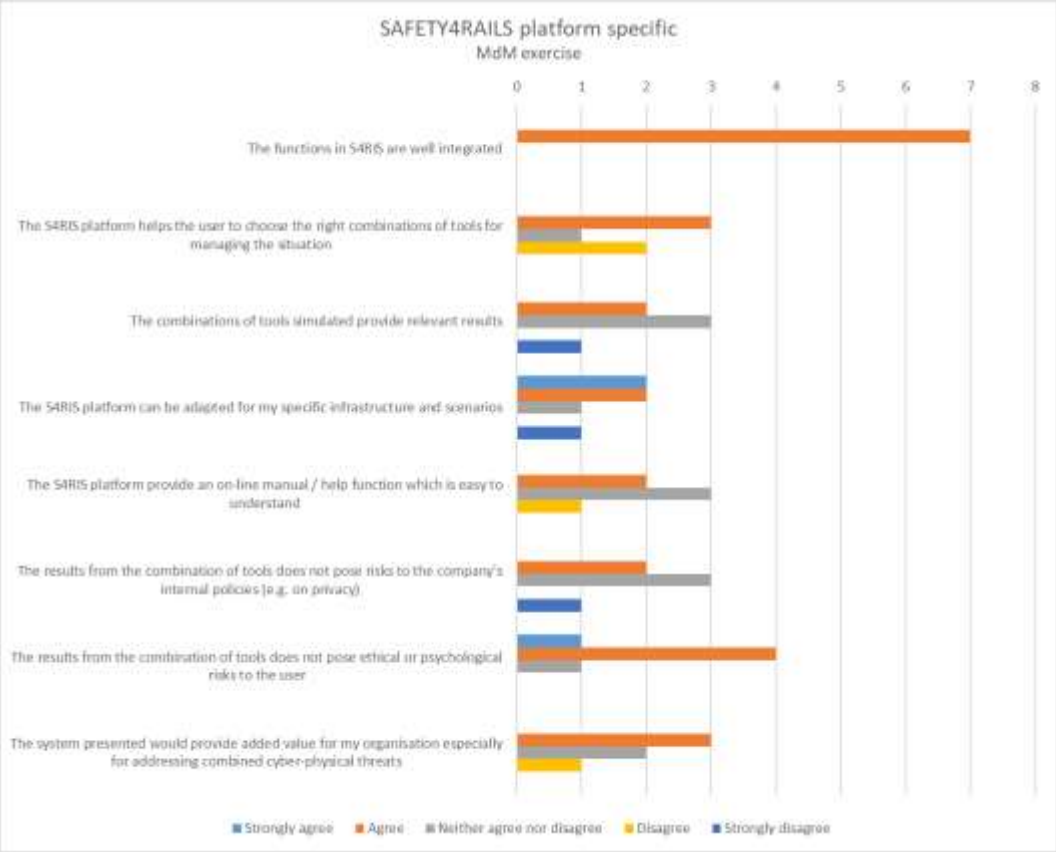
What could be improved to make the handling more transparent?

- It is okay

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- Focus on the crisis management take into account existing cybersecurity regulations for the railway sector and industrial control systems. If they have already been taken into account, it would be useful to document how each of the tools contributes to meeting the requirements specified in these standards.

Platform



Were there situations where you did not understand what the system was doing?

- Yes. I already wrote in my comments yesterday that I did not get all of the presentations yesterday.
- No
- Yes. Sometimes I didn't understand the order of actions when sensors detect anomalies. Additionally, sometimes the output of an action item were not clear

Would you recommend the system presented to your colleagues and why?

- Certainly; some of the presentations and tools are relevant for specific colleagues within my company because they would be the users. I have already alerted some of them.
- Yes, It is so helpful
- Not sure
- Yes, I would recommend it to show what technology can do. But I would also do it with the perspective of improving the tool. Asking questions like "what would you need from the tool?"
- Yes. I think it can help improve the safety of rail systems.

What could be improved in the context of this scenario?

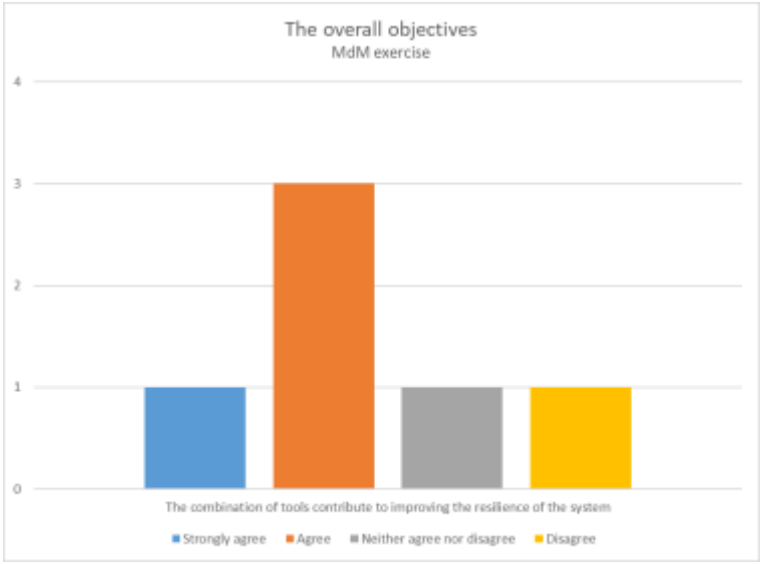
- More focused to the management of the crisis
- More interactive sessions. More live demos of the tools and the S4RIS. Participation of more end-users actors

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- Try to add more user requirements

MDMOVERALL OBJECTIVES AND ORGANIZATION OF THE EXERCISE QUESTIONNAIRE 4

Overall objectives



Which capabilities are the most important/useful for this scenario?

- Data that supports decision making (which at this moment is mainly done based on expert judgement)
- From the area that concerns me (cybersecurity) the tools that seemed most useful to me are: RAM2 and CAMS

What are the current obstacles for adopting such a system?

- Data sensitivity, maintain initial configurations
- Not solve real problems
- The current context of the end-users is the main obstacle in my opinion
- To determine the obstacles, we would have to analyse the tools in more detail in order to know the requirements / costs of implementing them.

What could be improved in the context of this scenario?

- N/A

Has any limitation of tools been discovered during the exercise? If so, please specify.

- Some of the tools have not yet been adapted to the railway world.

What is the overall added value as may be assessed from your own experience in your current daily work?

- Once again it is very important that the system delivers data/information that supports decision making (which at this moment mainly is done on the basis of expert judgement)
- Better insights
- Understanding crisis and add value into a tool will be able to help crisis managers
- I believe that these tools can help improve the safety of rail systems.

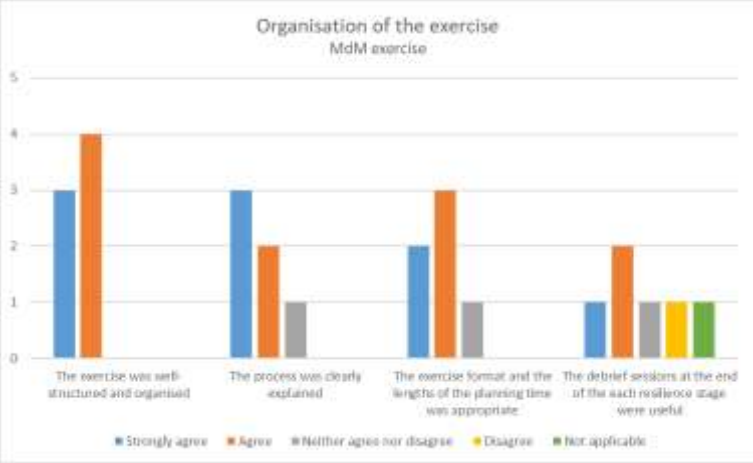
What were the main lessons learnt by you and why?

- Many little lessons that help understand the complexity of the railway sector
- Technological advances existing in the market that can help manage the safety of rail transport operators from a comprehensive point of view.

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- N/A

The organization of the exercise



Which part of the exercise did you find the most useful and why?

- In general it was very good to see some of the tools "in action" because it gives a better picture of how they can contribute
- Manage the incident/accident
- To know the real working of the tool
- I found the individual tool sessions that had a live and interactive part very useful to understand the scope of the tools. It was the best way to evaluate the potential implementation of the solution in our services.
- all in general

Were there any parties missing whose participation would have given added value for the exercise?

- Other control centre managers from others railways operators
- More end-users
- More end-users and, inside of the end-user group, different actors (operation planners, crisis managers, cybersecurity experts, etc.)

What can be done differently for the next exercises or what improvement need to be made?

- I imagine that it is a challenge to organize a hybrid session, but that was handled quite well. Maybe there could be a little more time between presentations and questionnaires; sometimes you need some time to digest first
- Spending more time in the management process
- More railway adapted
- Show, for the same exercise, what would have been done in the current situation (without S4RIS) and compare it showing how S4RIS can add value to the management of these kind of events

What are the main lessons learnt for you and why?

	• The reality is much more complex • The real working of the tools • Putting that many tools together is totally a challenge. Besides, implementing such a change in a current scheme that has worked for many years, is a long and process and depends strongly on the context of the end-user. • Technological advances that can be useful to manage the risks of physical security and cybersecurity from a comprehensive point of view.

ANNEX IV Assessment of how far the MdM scenario objectives were met based on end-users' evaluation

The correspondence of the evaluation results with the objectives set for the tools in each exercise phase is presented in following tables. In the estimation of the achievement of objectives the following classification has been used:

- Fulfilled according to the majority – more than half of the respondents have answered "strongly agree" or "agree" to question "The objective was successfully met"
- Partially fulfilled according to the majority – half of more of the respondents have answered "neither agree nor disagree" to question "The objective was successfully met"
- Not fulfilled according to the majority – more than half of the respondents have answered "disagree" or "strongly disagree" to question "The objective was successfully met"

WARNING: The "good faith" evaluation is based on the data provided in the Annex III which can include only limited responses and was based on what was seen at the simulation exercise.

MDM SIMULATION EXERCISE - REQUIREMENTS FOR THE PREVENTION PHASE

No	***Req.-ID - from D1.4***	**Short name**	**MDM Scenario objectives**	**Integrated in S4RIS (Y/N)**	**Result of evaluation**
MDM-PRE-1	BB3d_01	Bomb blast loading	Provide bomb blast simulations in order to understand how a bomb could affect the metro infrastructure, particularly the tunnels and the development of an event.This information will further support the Civil Construction Department in MDM for building more resilient physical structures (e.g. the tunnels) and reduce damage to passengers.	N	Fulfilled according to the majority

No	*Req.-ID - from D1.4*	**Short name**	**MDM Scenario objectives**	**Integrated in S4RIS (Y/N)**	**Result of evaluation**
MDM-PRE-2	CAMS_02	Maintenance and repair budget calculation	The individual tool will be used to inform the metro operator to allocate to repair/maintain/ rehabilitate the infrastructure after a set of possible events, therefore providing the necessary input to make a proactive plan and be ready in case of an attack. The metro operator will also be provided with information regarding the asset condition and degradation due to normal ageing, enabling timely response ahead of malfunctioning.	Y	Fulfilled according to the majority
MDM-PRE-3	SECURAIL_3	Computation of Risk	Enable off-line risk analysis of the metro infrastructure to understand the level of risk for each critical asset during a given hazardous event	Y	Fulfilled according to the majority
MDM-PRE-4	TISAIL_2	Detection of cyber-threats related to the railway sector: Internet-Exposed Assets and credential leakage	Provide vulnerability and security gaps assessment, along with risk assessment for each of the operational units in the metro system.	Y	Fulfilled according to the majority
MDM-PRE-5	DATAFAN-2	High prediction performance of results, e.g. anomaly detection	Provide information about the expected number of passengers to happen in the day of the football match. The end-user will be able to run what-if scenarios to analyse how they will affect the number of passengers and delays in the infrastructure (e.g., the closure of a station). For a	N	Fulfilled according to the majority

No	*Req.-ID - from D1.4*	Short name	MDM Scenario objectives	Integrated in S4RIS (Y/N)	Result of evaluation
			more precise prediction of the delays, the output data from iCrowd (NCSRD) will be used.		
MDM-PRE-6	CaESAR_02	CaESAR should identify weak points in the railway/metro system	The weakest/most critical components and associated cascading effects will be identified. An overall resilience analysis of the infrastructure will be done before the event	N	Partially fulfilled according to the majority
MDM-PRE-7	iCrowd_02	Simulate an evacuation because of terrorism (bomb, gas release) or natural disaster (fire/flood)	Provide simulation capabilities to understand better the chances of detection during infiltration/escape per configuration (camera and guards locations) and infiltration/escape total times.	*Y*	Fulfilled according to the majority
MDM-PRE-8	iCrowd_04	Detect blind-spots because of guards' movements and insufficient cameras	Revealing blind spots and other related vulnerabilities in case of a threat actor trying to escape	Y	Fulfilled according to the majority
MDM-PRE-9	RAM2_01	RAM2 should provide risk assessment and prioritisation	Provide vulnerability and security gaps assessment, along with risk assessment for each of the operational units in the metro system.	Y	Fulfilled according to the majority

No	*Req.-ID - from D1.4*	Short name	MDM Scenario objectives	Integrated in S4RIS (Y/N)	Result of evaluation
MDM-PRE-10	PRIGM_04	PRIGM should give service for end nodes and create outputs for end-users	Provide detailed report regarding vulnerabilities and attack surfaces within the system (mainly hardware-based attacks), supporting Network Security Expert or Cybersecurity Officer in the definition and development of countermeasures against cyber and/or cyber-physical attacks.	N	Fulfilled according to the majority

MDM SIMULATION EXERCISE - REQUIREMENTS FOR THE DETECTION PHASE

No	*Req.-ID - Need.-ID*	Short name	Objective for the MDM exercise	Integrated (Y/N)	Result of evaluation
MDM-DET-1	TISAIL_5	Detection of cyber-threats related to the railway sector: Spear Phishing	Inform the Crisis Manager about possible spear-phishing campaigns targeting mail domains of the MDM personnel.	Y	Fulfilled according to the majority
MDM-DET-2	CuriX_02	Catalogue-Based Outage Prevention	Crisis Manager will be alerted when deviations from normal behaviour (anomalies) or potentially upcoming disruptions of technical systems (IT and OT) from their monitoring data are detected. The crisis manager can check metrics and which technical devices are responsible for causing the major change in the system behaviour. in the scenario, detection of anomalies regarding sound intensity level, state of the doors, Lights	Y	Fulfilled according to the majority

No	*Req.-ID - Need.-ID*	Short name	Objective for the MDM exercise	Integrated (Y/N)	Result of evaluation
MDM-DET-3	CuriX_03	Infrastructure Monitoring (including cyber threats)	The crisis manager can monitor the health of the monitored technical system.	Y	Fulfilled according to the majority
MDM-DET-4	WINGS_03	Support of A.I. techniques	Analyse anomalies in the train speed so that an alert can be sent to the system team/driver. Check if there is an overcrowded area in the facility and raise an alert.	N	Fulfilled according to the majority
MDM-DET-5	DATAFAN-7	Manner of the applied anomaly detection	Data gathered regarding the flow of passengers will be used to detect significantly high passenger volumes in stations and trains, also considering days with really crowded events	N	Partially fulfilled according to the majority
MDM-DET-6	TISAIL_4	Detection of cyber-threats related to the railway sector: Vulnerabilities	TheCrisis Manager will be able to correlate the information (e.g., IoCs) provided by TISAIL for detecting threats in their networks using their security tools (e.g., IDS, SIEMs). CCTV camera vulnerability detected in the scenario	Y	Fulfilled according to the majority
MDM-DET-7	RAM2_02	RAM2 should generate correlated insights	Correlation of data gathered from multiple monitoring sources in order to detect potential threats. For example, it will be able to correlate the different attack vectors happening in the station	Y	Fulfilled according to the majority

MDM SIMULATION EXERCISE - REQUIREMENTS FOR THE RESPONSE PHASE

No	*Req.-ID - Need.-ID*	Short name	Objective for the MDM exercise	Integrated (Y/N)	Result of evaluation
MDM-RES-1	RAM2_01	RAM2 should provide risk assessment and prioritisation	Risk-based prioritisation of issues, case management for tracking response actions. End-user consumes the data through RAM2 Dashboards display. The user follows the prioritised alerts and mitigation steps for each of the alerts for risk reduction and response to detection of ongoing threats.	Y	Fulfilled according to the majority
MDM-RES-2	DATAFAN-2	High prediction performance of results, e.g. anomaly detection	Predict the passenger load in real-time in other stations once another is closed, helping to better respond the situation and re-locate the passengers.	N	Fulfilled according to the majority
MDM-RES-3	CaESAR_05	Implementation and evaluation of mitigation measures	Evaluate mitigation steps regarding their influence on the resilience, including cascading effects computation. As a pre-condition, CAESAR will count with the system topology provided by SecuRail.	N	Fulfilled according to the majority
MDM-RES-4	iCrowd_01	Simulate realistic crowd congestion levels	Crowd simulator providing advanced insights regarding crowd movement and behaviour for a set of boundary conditions related to the event.	Y	Fulfilled according to the majority
MDM-RES-5	WINGS_03	Support of A.I. techniques	Provide details, alerts of the detected issue in the train speed to aid the response action. Alerts are also raised in the case of overcrowded areas and guidelines in case of evacuation are provided.	Y	Fulfilled according to the majority

MDM SIMULATION EXERCISE - REQUIREMENTS FOR THE RECOVERY PHASE

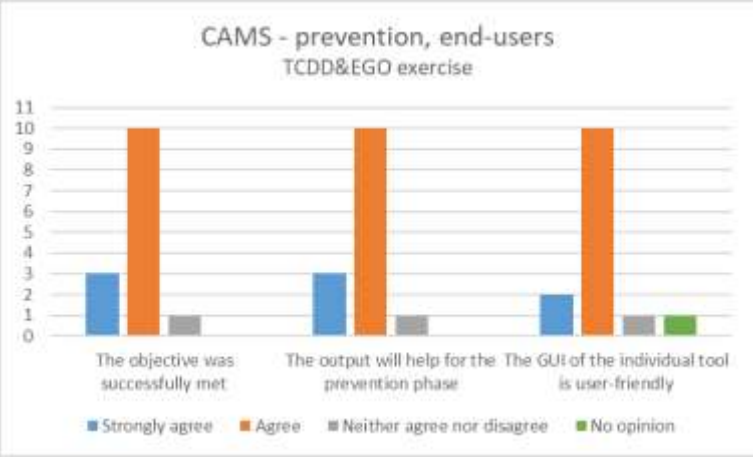
No	*Req.-ID - Need.-ID*	Short name	Objective for the MDM exercise	Integrated (Y/N)	Result of evaluation
MDM-REC-1	CAMS_10	Assessment of recovery	Crisis Manager will be provided with time and cost needed to respond to the crisis and restore normal functioning, so that resource deployment and reaction is based on proactive actions planned. Railway operator will be aware of vulnerability and fragility of the asset after the incident, so to improve resource deployment and control financial loss in the future.	Y	Fulfilled according to the majority
MDM-REC-2	BB3d_01	Bomb blast loading	Safety managers in the metro system will leverage the information provided by the bomb blast simulations in order to create mitigation countermeasures (e.g. safety distance, protective hardening, etc.). Number of casualties and people injured for out-door bomb attack scenarios are provided.	N	Fulfilled according to the majority

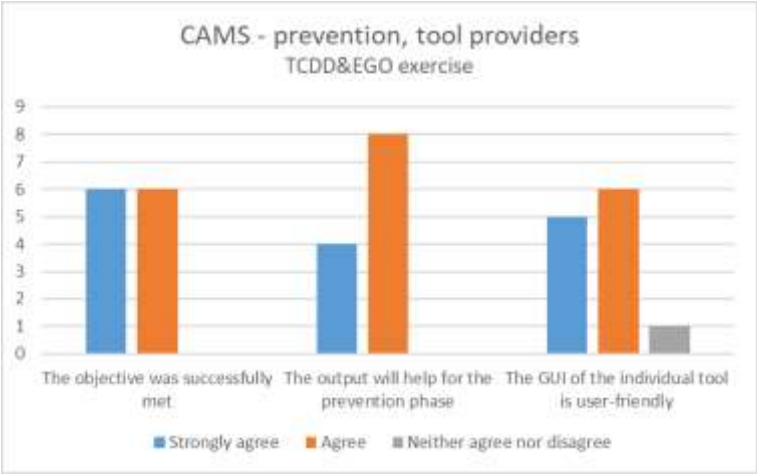
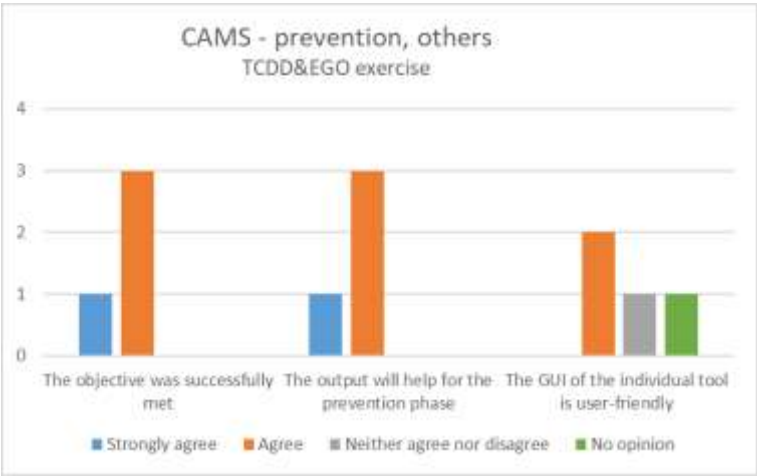
ANNEX V Ankara (TCDD&EGO) exercise schedule

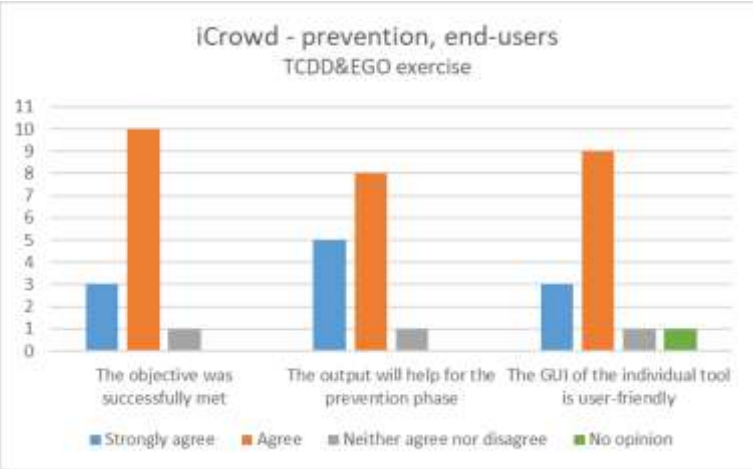
DAY 1 SIMULATION EXERCISE (SE) 27 April 2022		End-user audiences targeted
OPENING CEREMONY		
09:00-09.15	Welcome Speech by (EGO & TCDD)	All taking part in SE
09.15-09.30	Project Presentation by Coordinator (FhG)	All taking part in SE
09.30-09.35	Presentation about the implementation of the Exercise (ERARGE)	All taking part in SE
INDIVIDUAL TOOL DEMONSTRATIONS FOR PREVENTION & RECOVERY (PR) PHASES in ANKARA SIMULATION EXERCISE (SE)		
09.35-09.50	Introduction: objectives of the simulation during the **PREVENTION & RECOVERY** phases in this session	All taking part in this session
09.50-10.40	**Individual Exercises for PR Slot1** – - Very short presentation of the tool within the concept of Ankara Exercise & Progress beyond MDM exercise (5 minutes) / Simulation (10 minutes) / Discussion (5 minutes) CAMS (30 minutes) / iCrowd (20 minutes)	e.g. Maintenance planners, security managers, risk managers
10.40-10.55	**Online survey/questionnaire for the debriefing of PR sessions Slot1**	All taking part in this session
10.55-11.10	Tea & coffee break	
11.10-12.20	**Individual Exercises for PR Slot2** – - Very short presentation of the tool within the concept of Ankara Exercise & Progress beyond MDM exercise (5 minutes) / Simulation (10 minutes) / Discussion (5 minutes) SECURAIL (20 minutes) / CaESAR (10 minutes) / DATAFAN (20 minutes) / TISAIL/OSINT (20 minutes)	e.g. Maintenance planners, security managers, risk managers
12.20-12.50	**Presentation of the S4RIS Platform User interface and progress so far with contributory tool integration**	All taking part in SE
12.50-13.30	**Online survey/questionnaire for the debriefing of PR sessions Slot2 + S4RIS Platform User Interface sessions + Discussions of the results**	All taking part in SE
	End of Day #1	

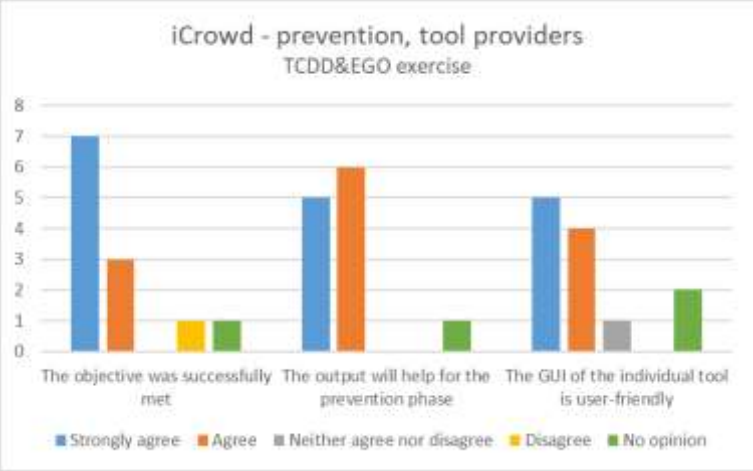
DAY 2 SIMULATION EXERCISE (SE) 28 April 2022		End-user audiences targeted
08.30-08.45	Wrap up of first day & presentation of objectives of the simulation during the PREVENTION through to RECOVERY phases in this session	All taking part in this session
JOINT TOOL DEMONSTRATIONS FOR PREVENTION - DETECTION -RESPONSE - RECOVERY phases (focus DETECTION & RESPONSE) in ANKARA SIMULATION EXERCISE (SE) SCENARIO		
08.45-09.30	**PREVENTION &DETECTION & RESPONSE &RECOVERY** Full JOINT scenario exercise (RAM2 lead decision support tool) - Progress beyond MDM exercise - Simulation - Discussion	Maintenance planners, security managers, risk managers, Control Centre personnel, Cyber security personnel
09:30-10:00	**Online survey/questionnaire for the debriefing of DR session - joint exercise**	All taking part in this session
INDIVIDUAL TOOL DEMONSTRATIONS FOR DETECTION & RESPONSE (DR) PHASES in ANKARA SIMULATION EXERCISE (SE) SCENARIO		
10.00-11.05	**Individual Exercises for DR Slot1** – - Very short presentation of the tool within the concept of Ankara Exercise & Progress beyond MDM exercise (5 minutes) / Simulation (10 minutes) / Discussion (5 minutes) CURIX (20 minutes) / PRIGM-SENSTATION (20 minutes) / GANIMEDE (25 minutes)	Security managers, risk managers, Control Centre personnel, Cyber security personnel
11.05-11.20	**Online survey/questionnaire for the debriefing of DR sessions Slot1**	All taking part in this session
11.20-11.30	Tea & coffee Break	
11.30-12.20	**Individual Exercises for RD Slot2** – - Very short presentation of the tool within the concept of Ankara Exercise & Progress beyond MDM exercise (5 minutes) / Simulation (10 minutes) / Discussion (5 minutes) DATAFAN (10 minutes) / SECURAIL (20 minutes) / TISAIL/OSINT (10 minutes) / CaEASAR (10 minutes)	Security managers, risk managers, Cyber security personnel
12.20-12.35	**Online survey/questionnaire for the debriefing of RD Slot2**	All taking part in SE
12.35-13.00	**Final remarks and Closure of the event**	

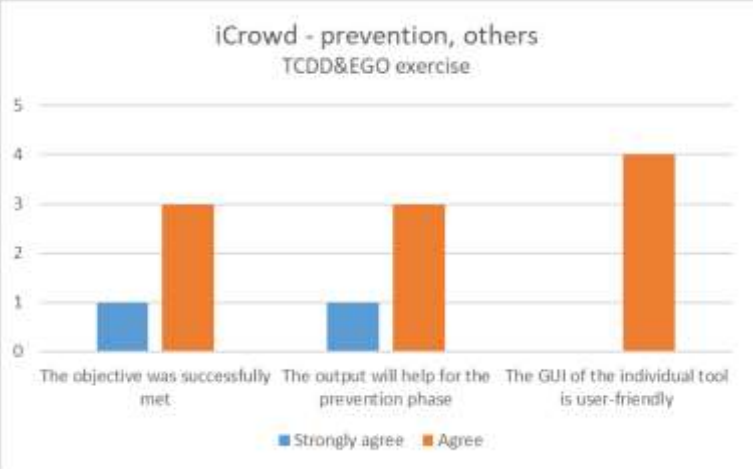
TCDD&EGO PREVENTION PHASE QUESTIONNAIRES 1 AND 2

CAMS	**Objective :** The individual tool will be used to inform the metro operator on the budget to allocate to repair/maintain/rehabilitate the infrastructure after a set of possible events, therefore providing the necessary input to make a proactive plan and be ready in case of an attack. The metro operator will be also provided with information regarding the asset condition and degradation due to normal ageing, enabling timely response ahead of malfunctioning.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Beter insights • will help for risk management • The help for implementing a plan in case of an attack • Positive • The added value of this tool is to have an organised structure for the information regarding the assets of a company and the corresponding resilience and degradation. Depending on the current situation of the end-user, this can be certainly helpful. How could this tool be improved in the context of this scenario? • give more information on the data to be provided to run the tool : importation of data, management of the updates... • Surely wit real data from the operator • By researching and practicing • The presentation was very interesting. However, in my opinion and considering that there is a limited time for the presentation, I would shorten the technical part (of how the tool works) and prepare a more interactive session for the end-users to get a clearer idea on how the tool works.

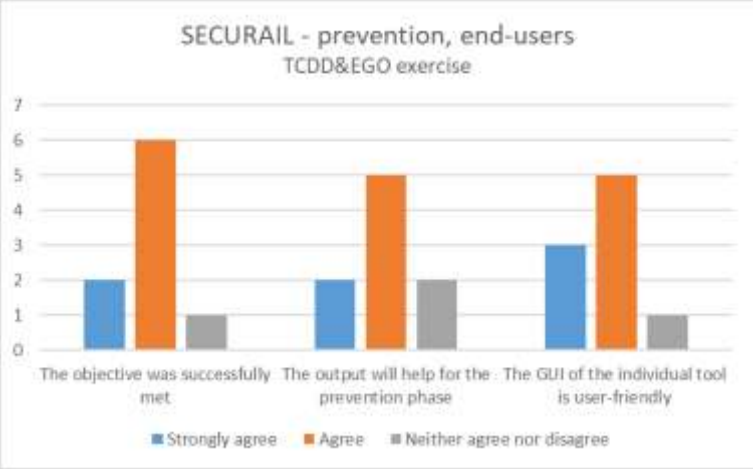
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Cost prediction • Can be used for further financial planning, and risk estimation • The end-users will be supported in quantifying the budget for a prevention scenario such as an incident • simulating and evaluating different scenarios which can help asset owners to make best monitoring and maintenance decisions How could this tool be improved in the context of this scenario? • Future Predictions adaptive to recent and future financial status that May happen • demo would be based on more clearly "actual" input data regarding e.g. cost • Maybe to give tipps for a better handling of the tool since it could be very complex for people not using it every day • More visualization and data access for another systems and more IoT-integrated plans can be maximize the performance and impact • to be integrated to other tools, as well as connection with sensor data
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Better knowledge of the importance/value of key infrastructure to the asset owner/user. How could this tool be improved in the context of this scenario? • Not sure without hands on experience

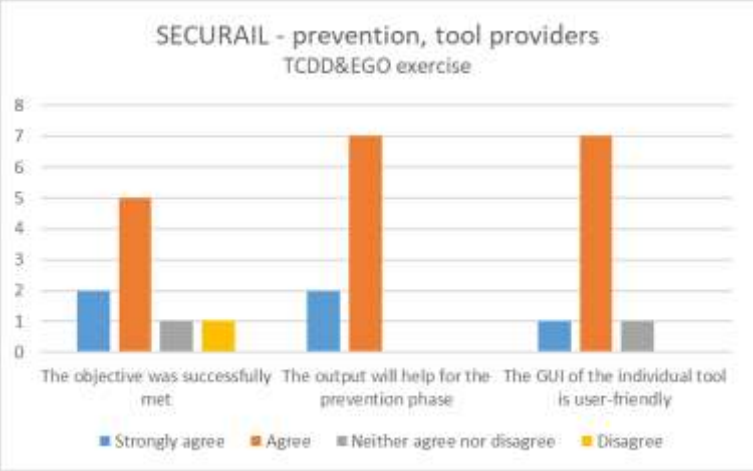
iCrowd	**Objective :** iCrowd will focus on the simulation of infiltration/escape scenarios to better understand the chance of detection for different CCTV cameras and guard configurations. It will provide simulation capabilities to understand the probability of detecting a malicious actor attempting to break into the EER, therefore assessing the effectiveness of CCTV camera location and guards to eventually improve them.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Take precautions • Simulation capabilities of the tool • Positive • To analyse the different CCTV cameras and guard configurations. How could this tool be improved in the context of this scenario? • With real data of the operator • By researching and practicing

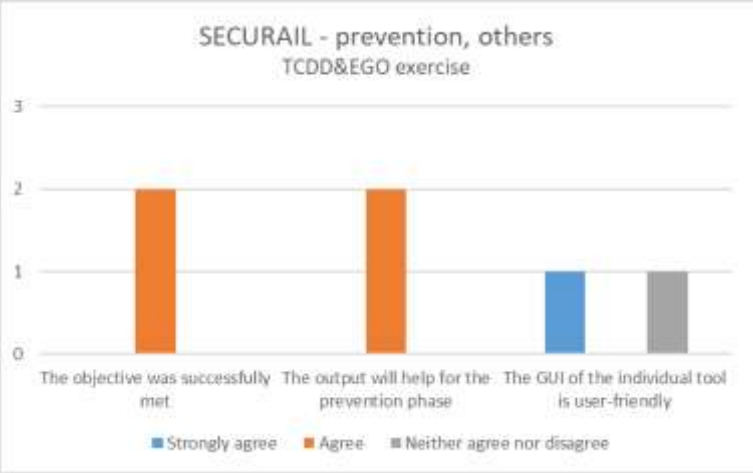
<table>
<tr>
<td> 
</td>
<td>What is the added value of this tool to the prevention phase that you know from your current daily work?
• Crowd management
• A good overview with visual interface
• The end-user will be supported in preparing a prevention scenario for a better estimation of needed times or expected delays

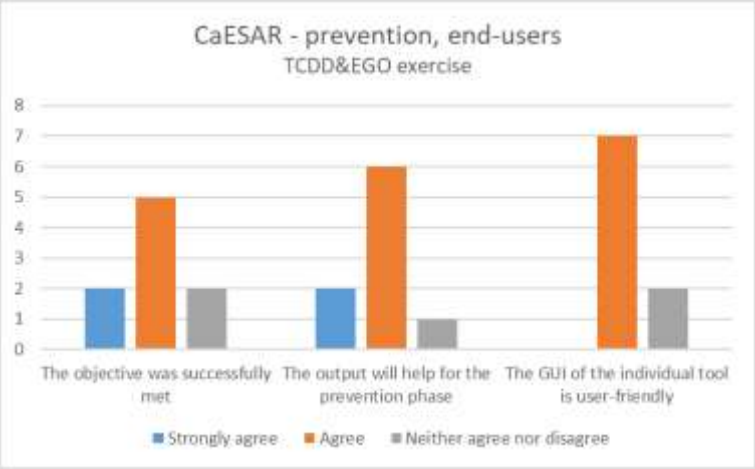
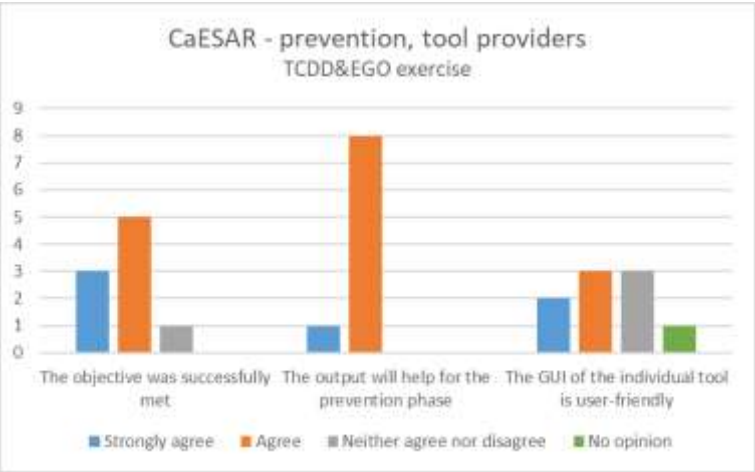
How could this tool be improved in the context of this scenario?
• Can be integrated with İot and Ai-based services to enable recent monitoring of the environment
• "simulation of infiltration/escape scenarios to better understand the chance of detection for different CCTV cameras and guard configurations" not so clearly analysed in terms of what the decisons could be for decision makers.d specific to the SE
• Maybe to give tipps for a better handling of the tool since it could be very complex for people not using it every day</td>
</tr>
<tr>
<td> 
</td>
<td>What is the added value of this tool to the prevention phase that you know from your current daily work?
• Enables facility design/construction as is or with changes, to best/safely meet potential demands hence minimising risk.

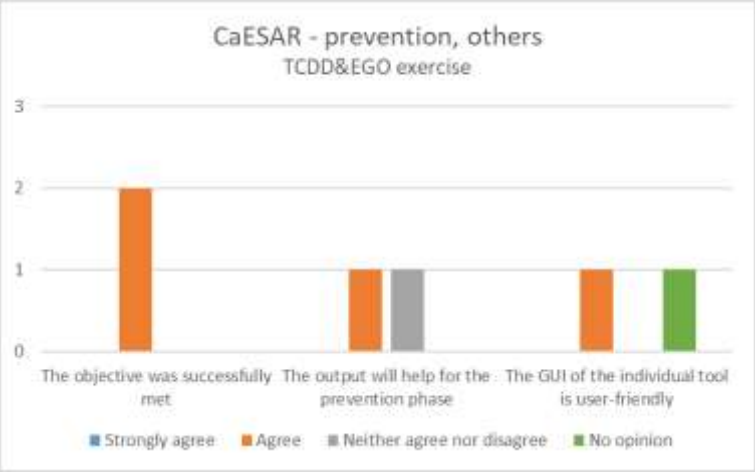
How could this tool be improved in the context of this scenario?
• Presume it can provide outputs for various facility design changes?</td>
</tr>
</table>

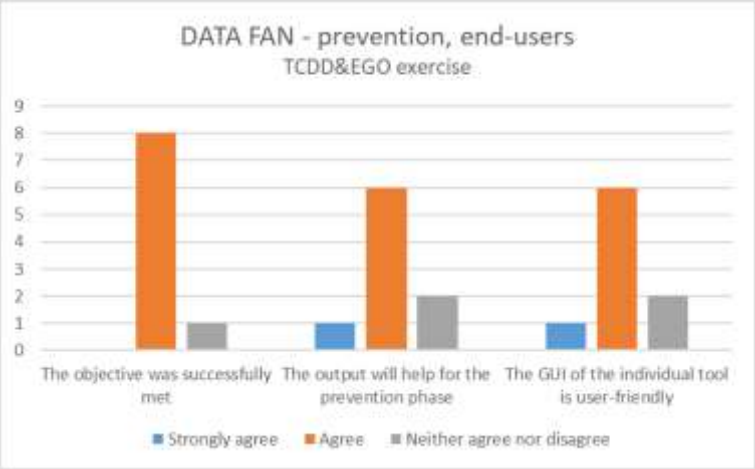
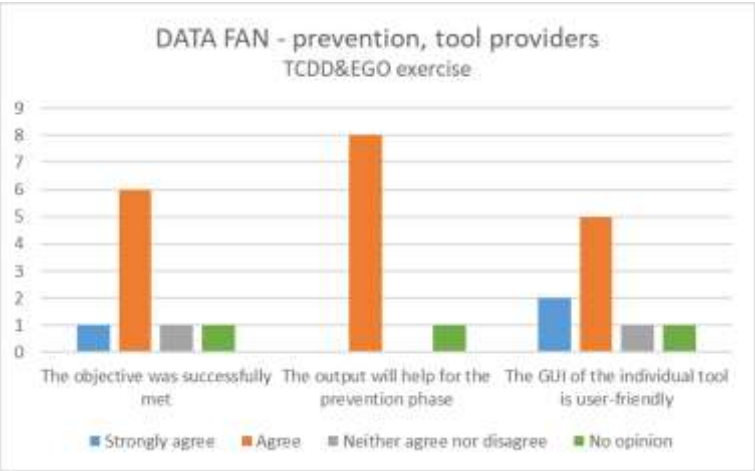
SECURAIL	Objective: Allow off-line risk analysis of the metro infrastructure to understand the level of risk for each critical asset during a given hazardous event. Perform a cost benefit analysis of the infrastructure to understand which of the solutions analysed to reduce the risk level is the best, considering both costs and benefits.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Risk assestment • Positive • To perform a cost benefit analysis of the infrastructure for different events. I think this tool looks very useful for that. How could this tool be improved in the context of this scenario? • By researching and practicing

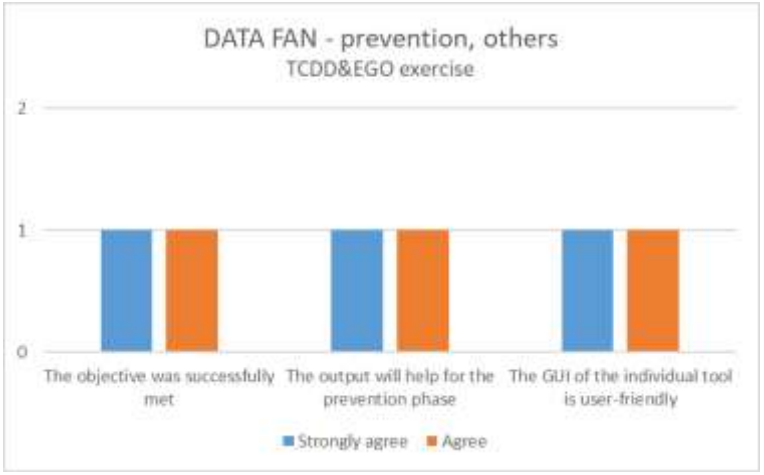
<table>
<tr>
<td> 
</td>
<td>What is the added value of this tool to the prevention phase that you know from your current daily work?
• The end-users are supported in a better planning of a prevention scenario
• Surveilance and Monitoring

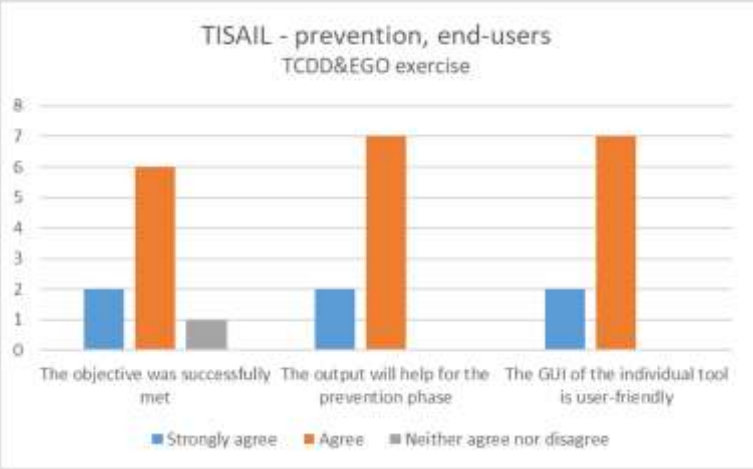
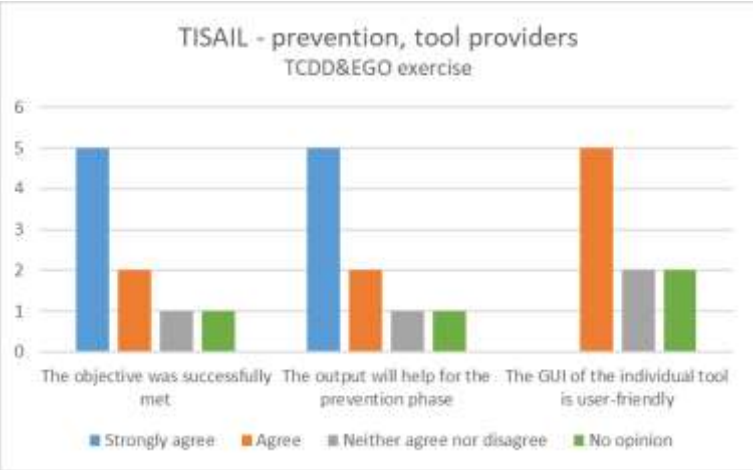
How could this tool be improved in the context of this scenario?
• "Allow off-line risk analysis of the metro infrastructure to understand the level of risk for each critical asset during a given hazardous event" - agree this was met. "Perform a cost benefit analysis of the infrastructure to understand which of the solutions analysed to reduce the risk level is the best, considering both costs and benefits." - not met (asl aso said in presentation). This for the future.
• Maybe to give some tipps on the functionalities since it might be very complex for people not using the tool every day
• Provide early warning and offer continousmonitroing of correct operation
• The methodology for estimating the cost of countermeasures is not clear. MAybe the developers can give more information about the methodolgy behind</td>
</tr>
<tr>
<td> 
</td>
<td></td>
</tr>
</table>

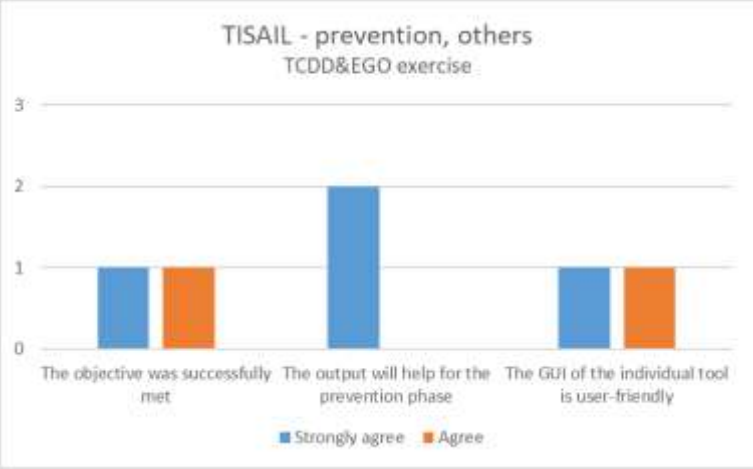
CaESAR	**Objective :** CaESAR will focus on the analysis of weak components, mitigation measures, and the overall resilience of the system. The Operational Centre Supervisor asks the user to implement mitigation measures to test which of them would work better on the infrastructure.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Counter measuse • Positive • To analyse the resilience of the system How could this tool be improved in the context of this scenario? • By researching and practicing
	What is the added value of this tool to the prevention phase that you know from your current daily work? • The end-users are supported in getting an idea of the cascadung effects and critical nodes caused in a specific situation • Secure communication • It presents a strong simulation-based computation model for understanding the transportation dynamics and potential cascading effects at city scale. How could this tool be improved in the context of this scenario? • "CaESAR will focus on the analysis of weak components, mitigation measures, and the overall resilience of the system. " Done with dtabase don assumptions. "The Operational Centre Supervisor asks the user to implement mitigation measures to test which of them would work better on the infrastructure." - did not see comparison of actual mitigation measures.

	• Maybe to give some tipps on the functionalities since it might be very complex for people not using the tool every day • Implied • Integration with other transportation modalities can be improved. End-users need to understand the targeted scale of the simulation in terms of geographical area and time
	

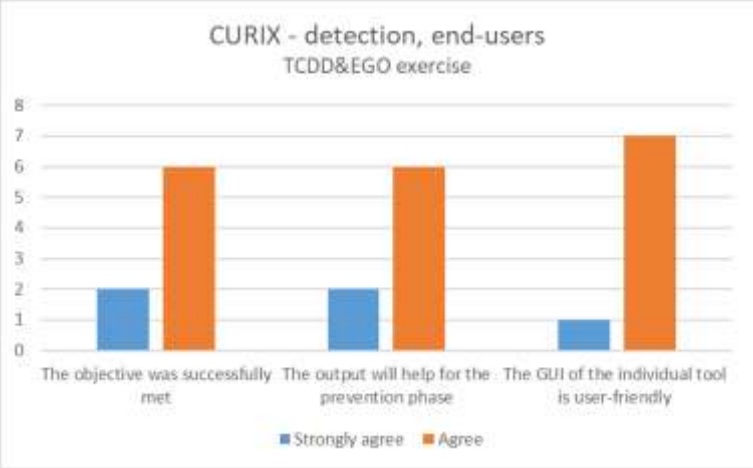
DATAFAN	Objective: DATAFAN will focus on the reliable prediction of passenger load on specific metro stations and provides information about the expected number of passengers to happen in the day of the event. The end-user will be able to run what-if scenarios to analyse how they will affect the number of passengers and delays in the infrastructure (e.g., the closure of a station).
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Better insights • Positive How could this tool be improved in the context of this scenario? • By researching and practicing
	What is the added value of this tool to the prevention phase that you know from your current daily work? • crowd management • The end-user is supported in the evaluation of the passenger load for a specific scenario and how to re-direct the passengers to the surrounding stations • It presents a strong reliability scoring mechanism, especially when combined with realistic data (e.g. long-term How could this tool be improved in the context of this scenario? • "The end-user will be able to run what-if scenarios to analyse how they will affect the number of passengers and delays in the infrastructure (e.g., the closure of a station)." Not seen in demo/presentation. • The GUI should be more easy to handle. • If the reliability scoring mechanism gets more standardisedi this may be great conribution

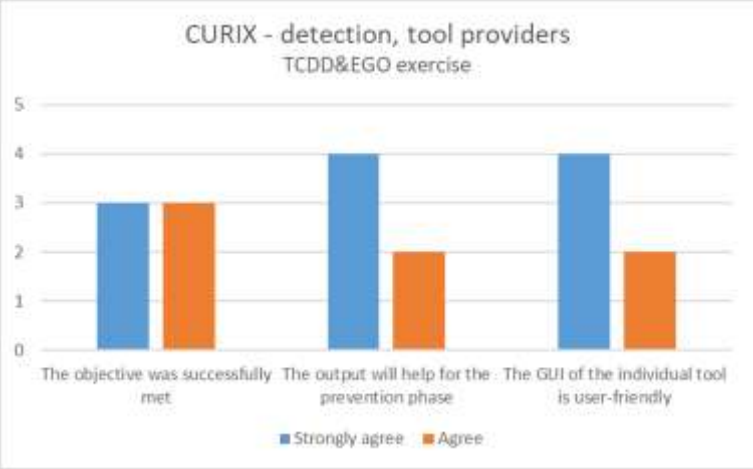
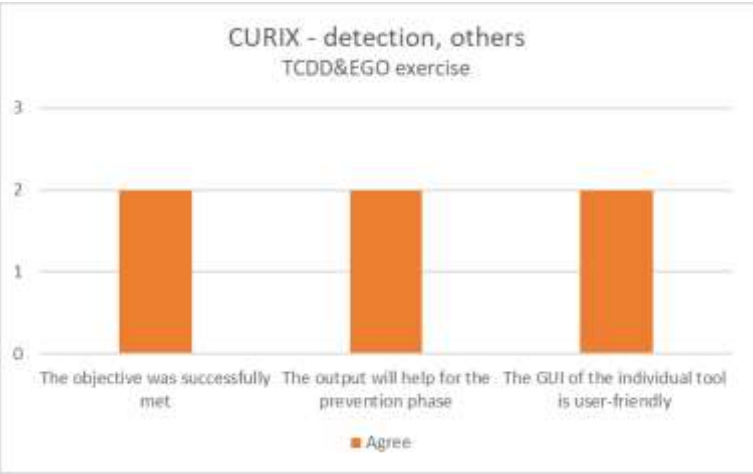

DATA FAN - prevention, others
TCDD&EGO exercise
2
1
0
The objective was successfully met
The output will help for the prevention phase
The GUI of the individual tool is user-friendly
Strongly agree
Agree

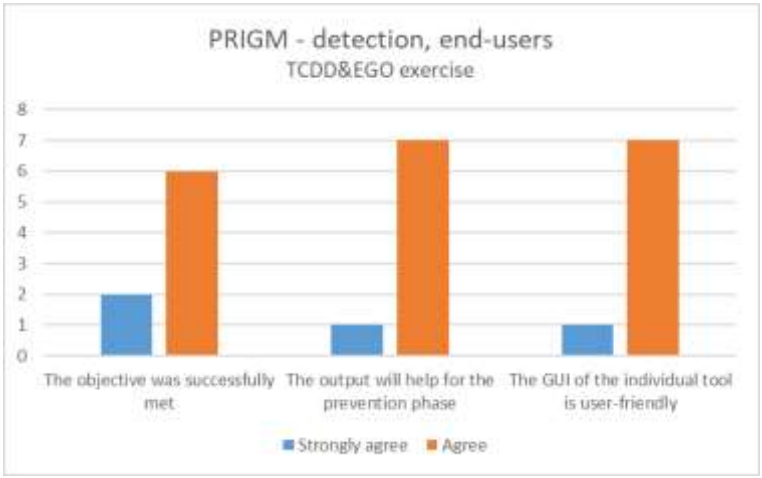
TISAIL	**Objective:** Provide situational awareness about vulnerabilities that could be exploited by attackers: e.g. CCTV, Power Grid, Windows 10.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Vulnerability assesment • Positive • To add into the current sources additional ones that help preventing potential threats How could this tool be improved in the context of this scenario? • By researching and practicing
	What is the added value of this tool to the prevention phase that you know from your current daily work? • The end-users are supported in the prevention phase for a scenario. • Both tools provide an adaptive mechanism to redefine the risks and can get aligned with new topics of interest. How could this tool be improved in the context of this scenario? • Regarding OSINT have examples which are closer to the geographical location of the project (i.e. not USA) and also in railway/metro domain. • Maybe to give some tipps on the functionalities since it might be very complex for people not using the tool every day • language independency can be promoted well. Especially for agglutinative languages like Finnish, Turkish...

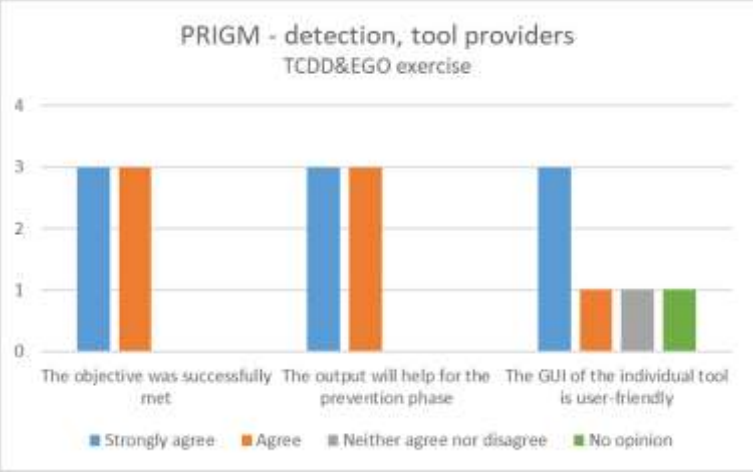
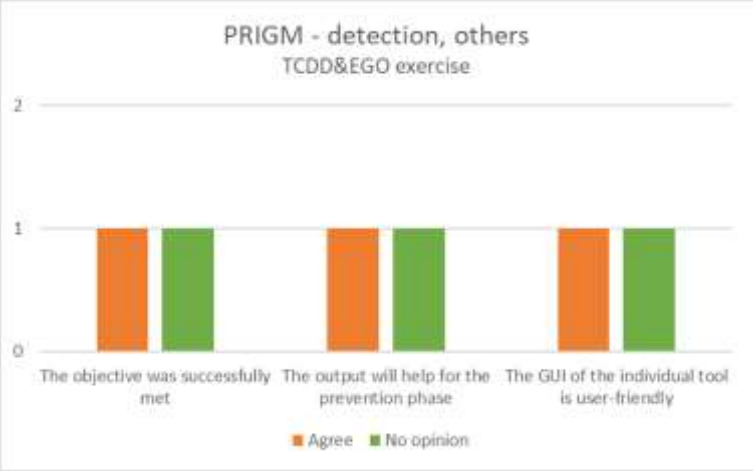

TISAIL - prevention, others
TCDD&EGO exercise
3
2
1
0
The objective was successfully met
The output will help for the prevention phase
The GUI of the individual tool is user-friendly
Strongly agree
Agree

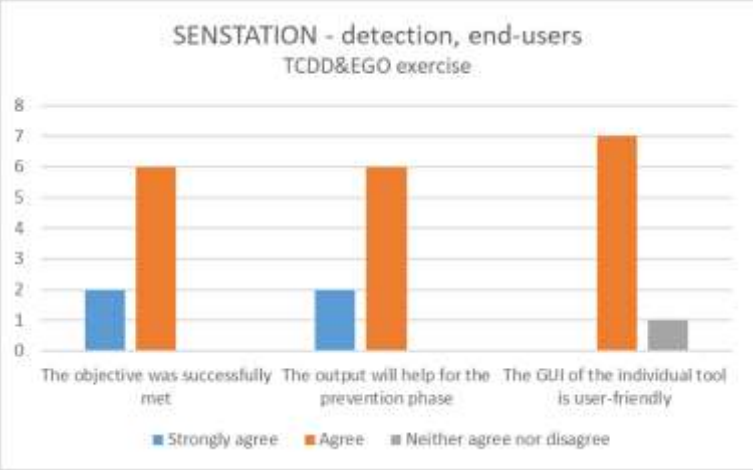
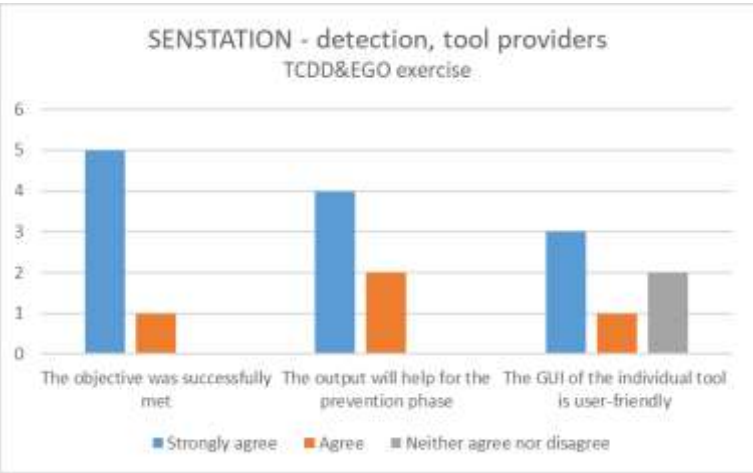
TCDD&EGO DETECTION PHASE QUESTIONNAIRES 4 AND 5

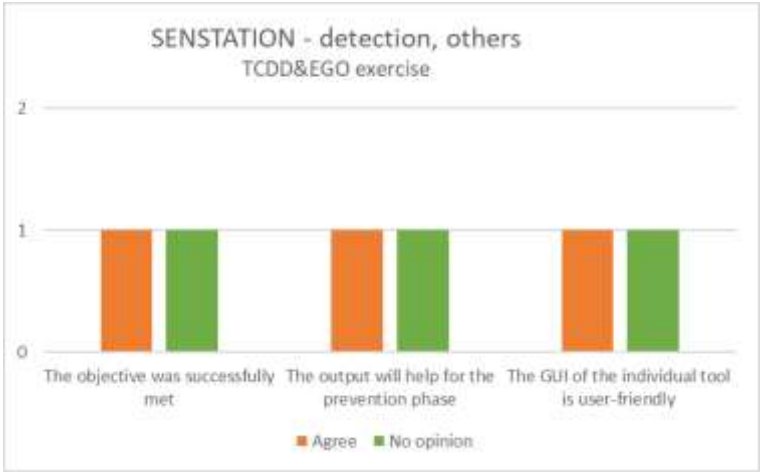
CURIX	**Objective:** Crisis Manager will be able to be alerted when deviations from normal behaviour (anomalies) or potentially upcoming disruptions of technical systems (IT and OT) from their monitoring data are detected. The crisis manager can check metrics and which technical devices are responsible for causing the major change in the system behaviour. The crisis manager can monitor the health of the monitored technical system.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Process is automated and does not require human interferecence • Positive • early detection of anomaly and integration of the tools with the others to get more accurate information • Alarm system make easier to detect anomalies • Centralised status and alerts for many technical systems. Easy to check metrics and alerts. How could this tool be improved in the context of this scenario? • By researching and practicing • Perhaps a more graphical view of the systems together with the dashboard. Also, in the components tab, there is maybe some space to put the whole name of the component so it is not necessary to place the cursor on it to see the name.

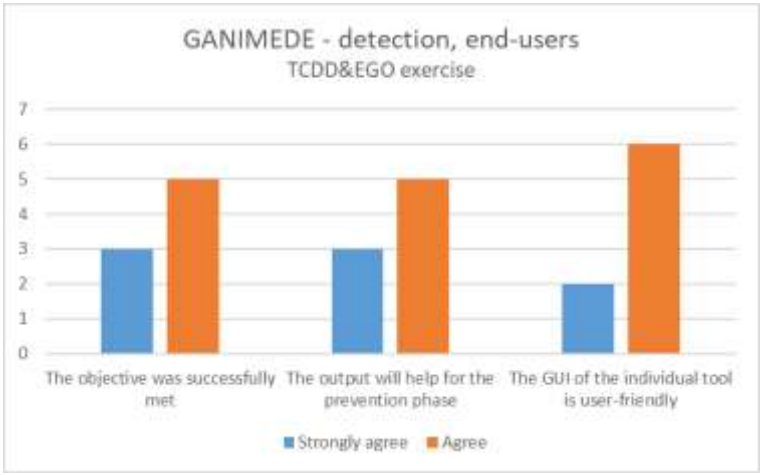
	What is the added value of this tool to the prevention phase that you know from your current daily work? • It proides a good situational awareness supporting multidimensional data flows. How could this tool be improved in the context of this scenario? • Examples with more data from different technical systems (IT and OT) • More content analysis for different languges can be added
	

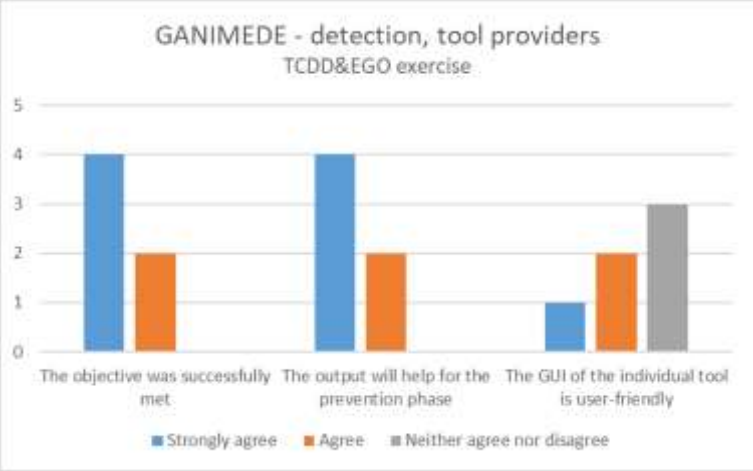
PRIGM	**Objective:** Analysis of log data of main security operations (e.g., authentication, encryption, key exchange, etc) to determine anomalies, monitor the authentication flow for misuses/spoofing and help to discriminate between flooding data and normal flow. Furthermore, tracing and detection of cyber anomalies will be enabled, therefore assisting other countermeasure tools for enhanced resilience.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • (better) use of available data to detect an abnormal situation • Positive • early detection of anomaly to be able to react as soon as possible and also secure communication with encryption • it makes possible secure communication between edges and center • Detecting possible cyberanomalies earlier. The example is very clear. How could this tool be improved in the context of this scenario? • By researching and practicing

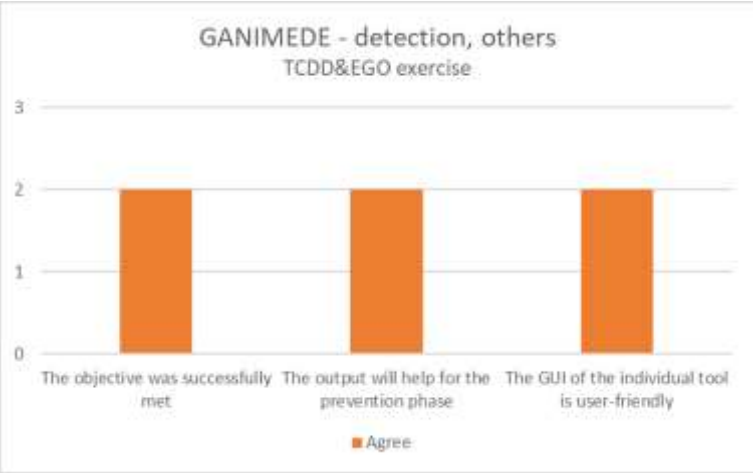
	How could this tool be improved in the context of this scenario? • In presentation / demo did not see e.g. of spoofing detection
	

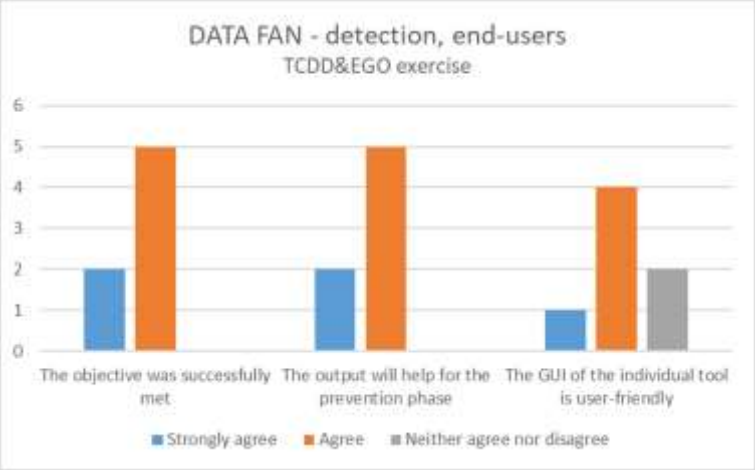
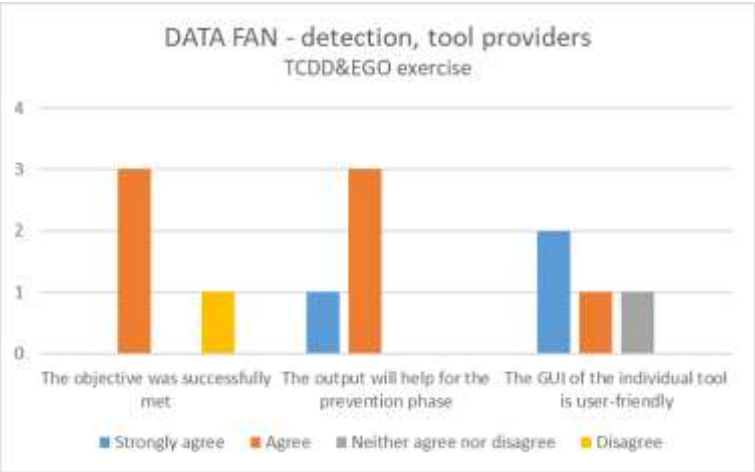
SENSTATION	**Objective:** Secure Gateway at edge nodes responsible from data protection where data is generated. It allows receive some instant information from the Electronic Equipment room to monitor unauthorised physical access, so that the operator can alert the security guard and the main Command and Control Centre.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • (better) use of available data to detect an abnormal situation • Positive • early detection of the intrusion • It allows gather information without exposing IP or ports to public access. • Detecting possible intrusions earlier. The example is very clear How could this tool be improved in the context of this scenario? • By researching and practicing • The GUI is clear in the video part, but I would suggest to make a simpler GUI for the end-users (less tabs and screens).
	

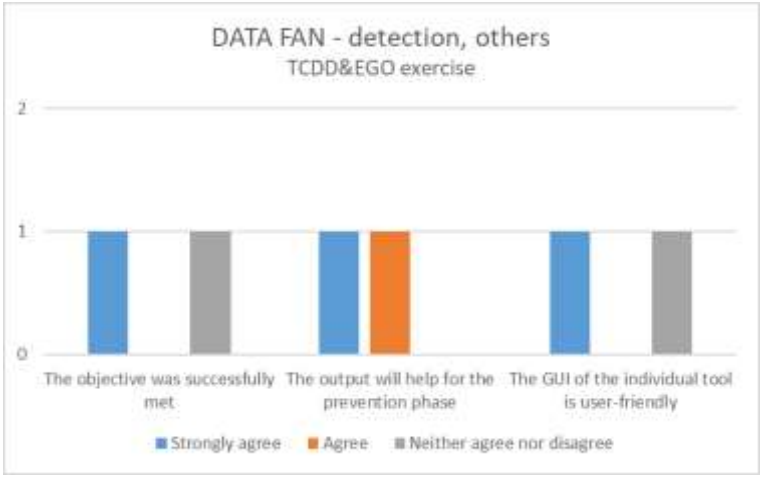

SENSTATION - detection, others
TCDD&EGO exercise
2
1
0
The objective was successfully met
The output will help for the prevention phase
The GUI of the individual tool is user-friendly
Agree
No opinion

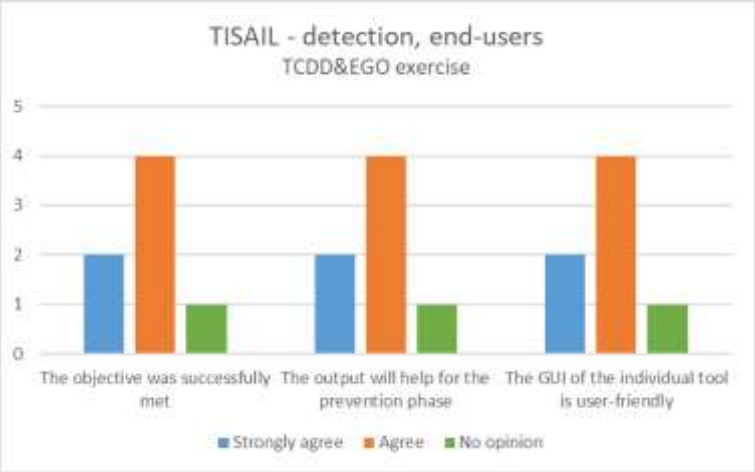
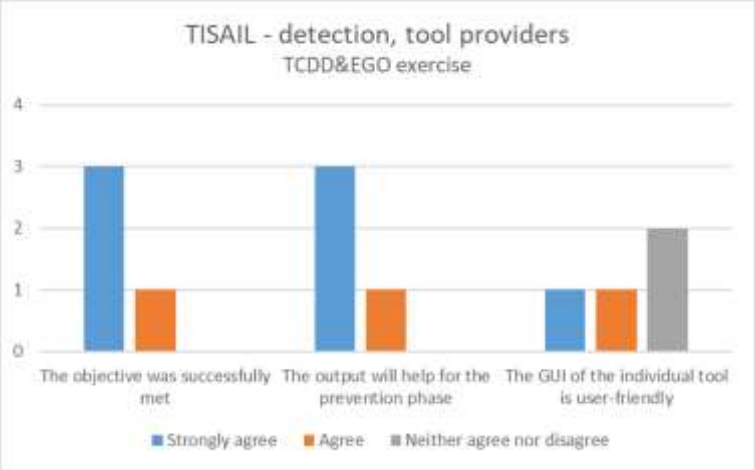
GANIMEDE	**Objective:** Ganimede will be focused on the detection of objects and people in each frame and their movement to determine if the object is candidate for being abandoned.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Usage of algoritms and deep learning with regard to abandoned objects is not being used at the moment. Human surveillance is standard • Positive • early detection • It helps security team to identify and notice the threats • Detecting potential threats swiftly. It is clear what the tool can provide and also there was a complete explanation on how the algorithm for abandoned objects was applies in the Ankara scenario. How could this tool be improved in the context of this scenario? • How does it work in busy environment (stations in peak hour traffic) when an abandoned object is placed in a crowded area • By researching and practicing • there are many unattended luggages in daily operations, the main challlenge is to identify if it is suspicious and if an intervention is needed

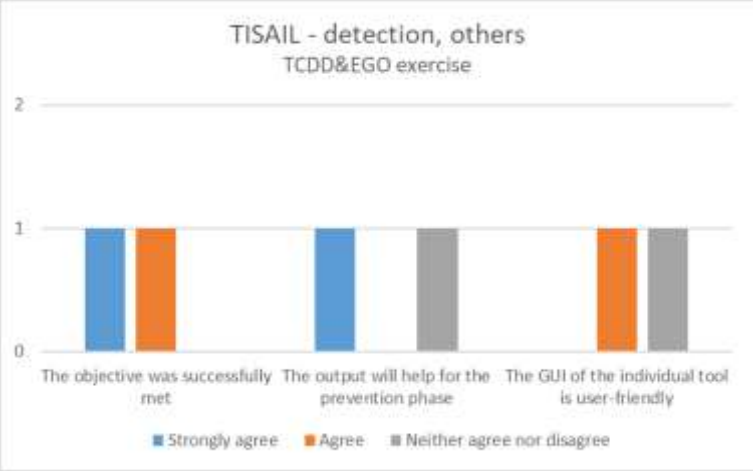
<table>
<tr>
<td> 
</td>
<td>What is the added value of this tool to the prevention phase that you know from your current daily work?
• It provides a good basis for detecting the abandoned luggages

How could this tool be improved in the context of this scenario?
• Presentation of the UI of the Ganimede tool (or the LDO tool in which it would be running).
• There is more test needed to identify luggages in crowded areas</td>
</tr>
<tr>
<td> 
</td>
<td></td>
</tr>
</table>

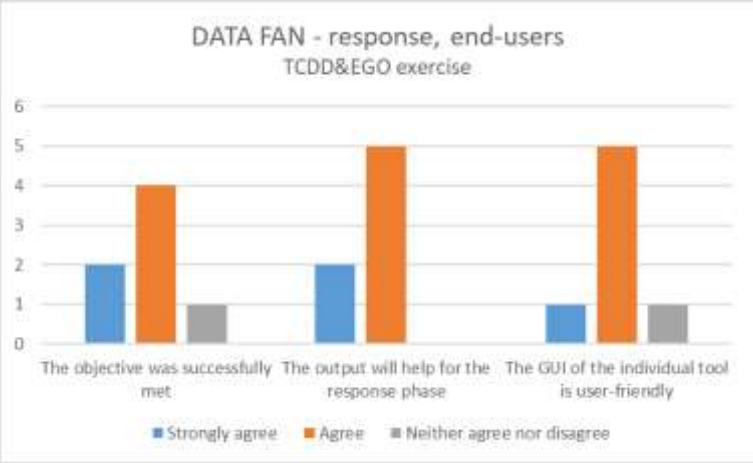
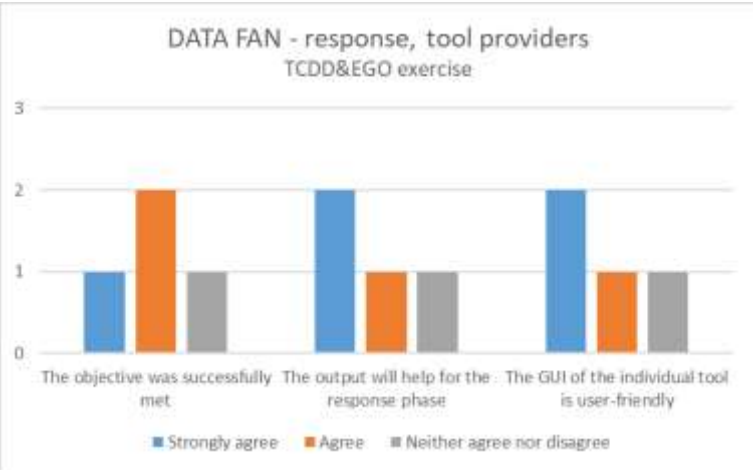
DATAFAN	**Objective:** Data gathered regarding the flow of passengers will be used to detect significantly high passenger volumes in stations and trains, also considering days with really crowded events.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • decision making with regard to measures to be taken on the basis of factual data. Not on basis of expert judgement • Positive • early detection • It Helps to make more accurate desicions • Detecting anomalies on the passenger flows. How could this tool be improved in the context of this scenario? • By researching and practicing • Integrated in RAM2. The GUI is helpful if you want to understand the metrics and the calculations, but if you are the end-user, sometimes you just want to see the alert in a visual environment.
	How could this tool be improved in the context of this scenario? • Objective need to match what is presented and vice vera. "Data gathered regarding the flow of passengers will be used to detect significantly high passenger volumes in stations and trains, also considering days with really crowded events". what was presented was station closed i.e. 0 passengers and the number which would have been expected. would have expected presentation of anomaly detection with data received as stream (even if simulated) and then an anomaly detection (for lower/higher amounts, but not just "0")

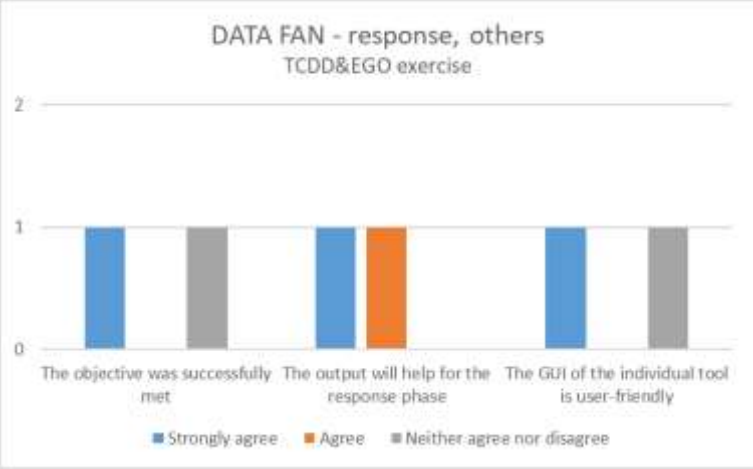

DATA FAN - detection, others
TCDD&EGO exercise
2
1
0
The objective was successfully met
The output will help for the prevention phase
The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree

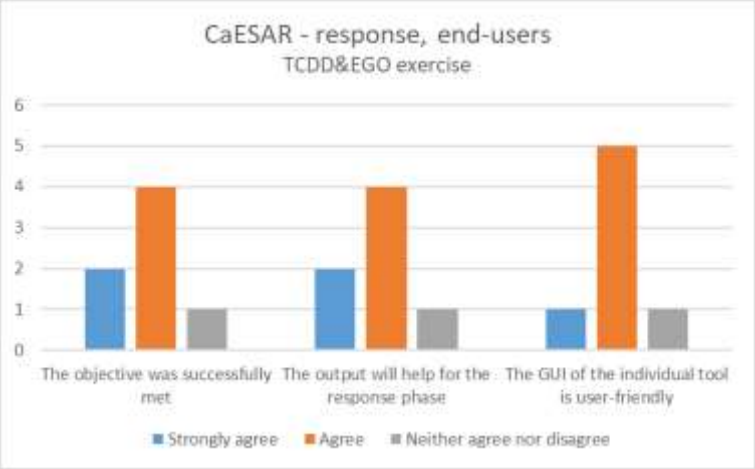
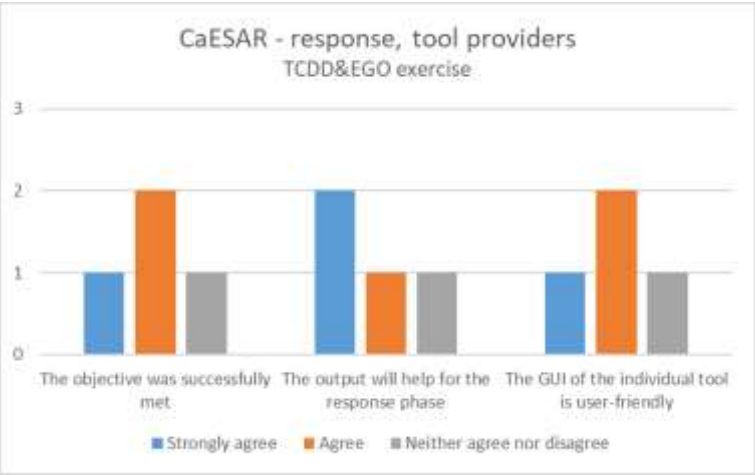
TISAIL	**Objective:** Crisis Manager will be able to correlate the information (e.g., IoCs) provided by TISAIL for detecting threats in their networks using their security tools (e.g., IDS, SIEMs).
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Positive • combination with other cyber detection tools • After defining the assets, it doesn't need manual research about the assets one by one • Update the defense mechanisms of the system and be ready for the threats How could this tool be improved in the context of this scenario? • By researching and practicing
	

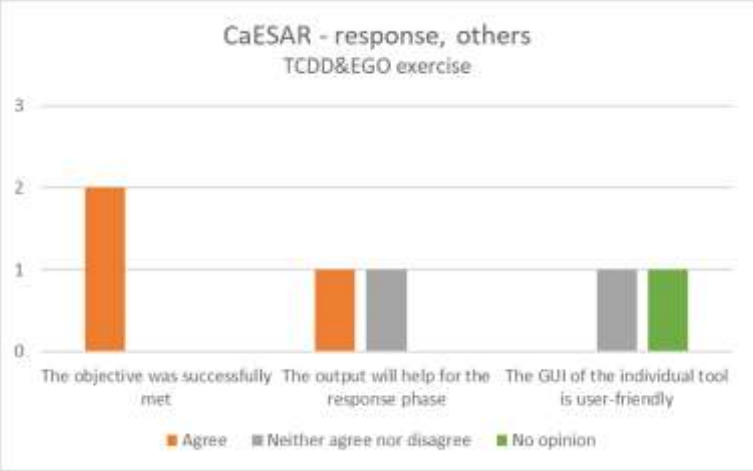
	How could this tool be improved in the context of this scenario? • maybe the contentgvernance can be improved by considering multimodal sources of information.

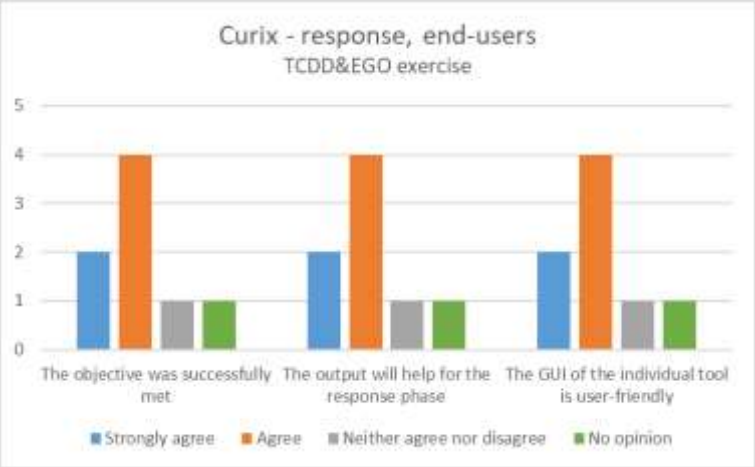
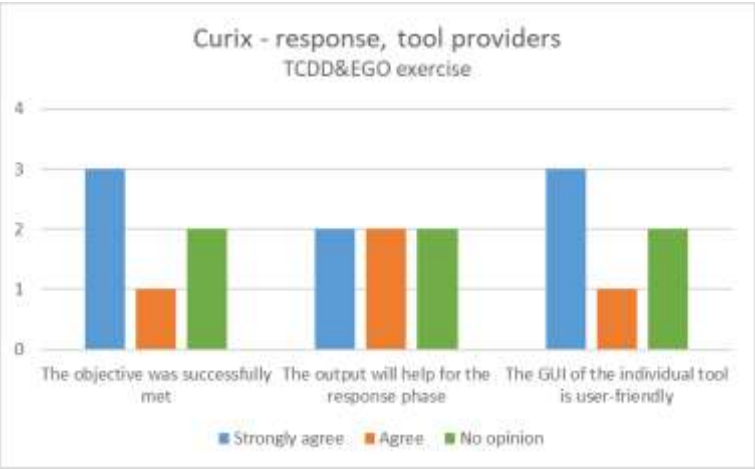
TCDD&EGO RESPONSE PHASE QUESTIONNAIRES 4 AND 5

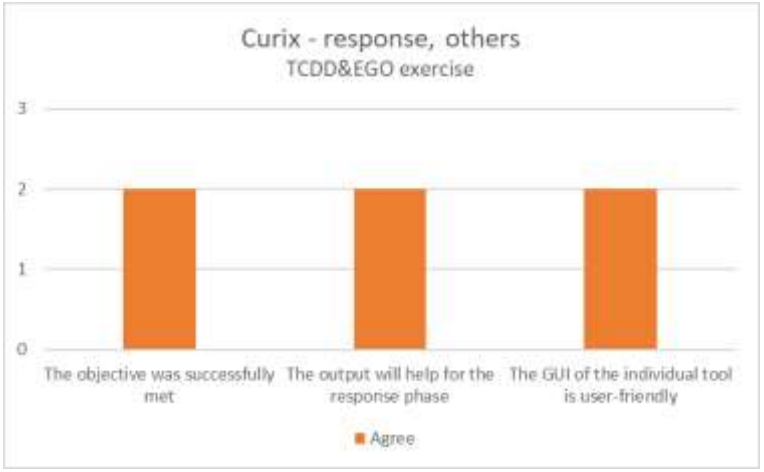
DATAFAN	**Objective:** Crisis Manager will be provided with time and cost needed to respond to the crisis and restore normal functioning, so that resource deployment and reaction is based on proactive actions planned. Railway operator will be aware of vulnerability and fragility of the asset after the incident, so to improve resource deployment and control financial loss in the future.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • decision making with regard to measures to be taken on the basis of factual data. Not on basis of expert judgement • Positive • help the decision process for puting in place mitigation measures : other transport means, information to passengers...t • It helps to respond fast in case of anormal crowd • Knowing what distribution of passengers you could have in front of an attack How could this tool be improved in the context of this scenario? • By researching and practicing • Same as for the DETECTION phase. Also, it could be taken into account that depending on the alert, all the surrounding stations (and perhaps the whole network) would be shut down.
	How could this tool be improved in the context of this scenario? • Was n tclear what "mitigation steps for each of the alerts for risk reduction and response to detection of ongoing threats" were. Also, concept does not seem to consider that if a station is close d it will lead ot passengers getting on / off at other stations over at east the period of time that the station is closed i.e. prediction and/or anomaly detection at surronding stations also over a longer time duration.


DATA FAN - response, others
TCDD&EGO exercise
2
1
0
The objective was successfully met
The output will help for the response phase
The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree

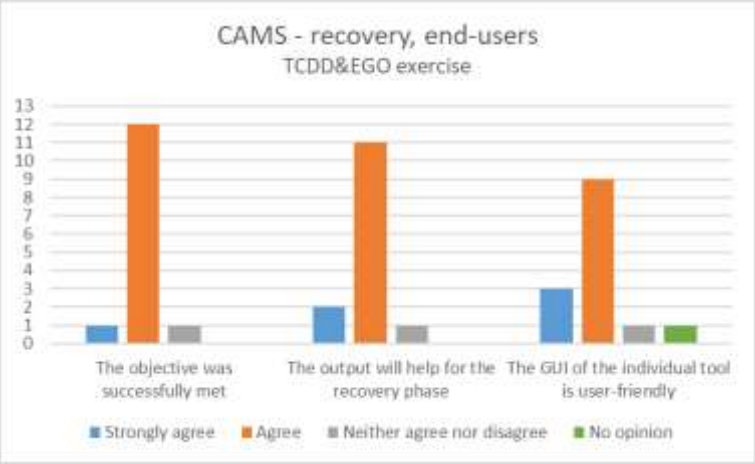
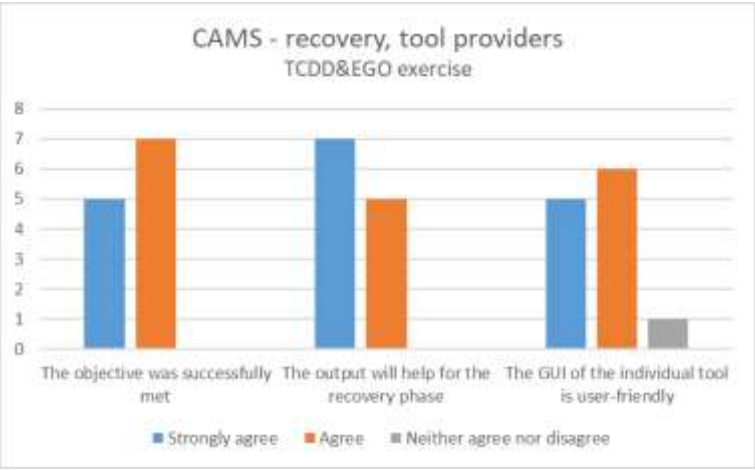
CaESAR	**Objective:** Support to end-user to select the appropriate mitigation measure to respond against different event int the Turkish infrastructure.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Data based decision making with regard to measures to be taken. Therefore objective and not on basis of expert judgement • Positive • help decision making in the crisis management • It help us to optimise crisis scenarios • With more defined rules, it would be helpful to understand the network behaviour How could this tool be improved in the context of this scenario? • By researching and practicing • Replace assumptions with real data
	How could this tool be improved in the context of this scenario? • Tool would be propagated with data from scenario (needs end-user input) and therefore less assumptions, for better basis to demonstrate information basis for appropriate mitigation measures.

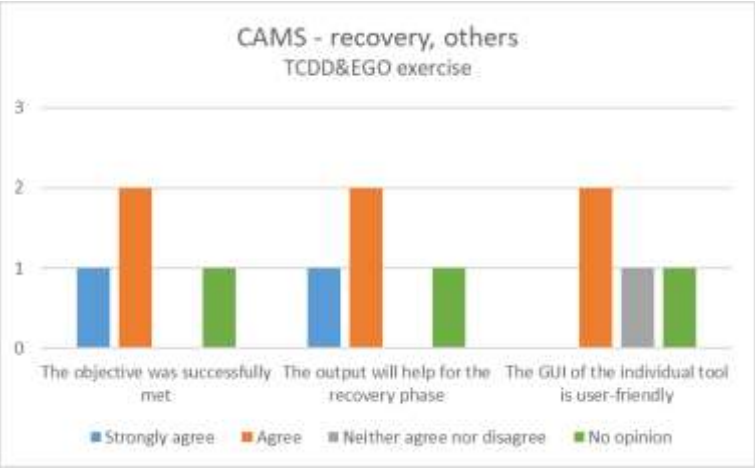
	What is the added value of this tool to the prevention phase that you know from your current daily work? • It presents a general overview of the cascading effects in a certain envirnment How could this tool be improved in the context of this scenario? • This can be improved with more multidimensional evidence-based simulations for more time-critical operations

CURIX	**Objective:** Evaluate how passenger flows correlate to each other, so to enhance/optimise the cascading effects analysis performed by the other S4RIS tools. Identify anomalies in passenger flows of other connected stations.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Positive • again the integration with the other tools gives a good picture of the situation and mitigation measures • It helps countermeasures • I don't see that CuriX detected correleted nor detected anomalies in passenger flows. How could this tool be improved in the context of this scenario? • By researching and practicing • management of high number of alerts : how to prioritize, identify false alert... • I don't see that CuriX detected correleted nor detected anomalies in passenger flows.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • It proides a good situational awareness supporting multidimensional data flows. How could this tool be improved in the context of this scenario? • DOn't see htis was done in the presentation / demo • More content analysis for different languges can be added. More explainable interfaces (for end-users) can be added.

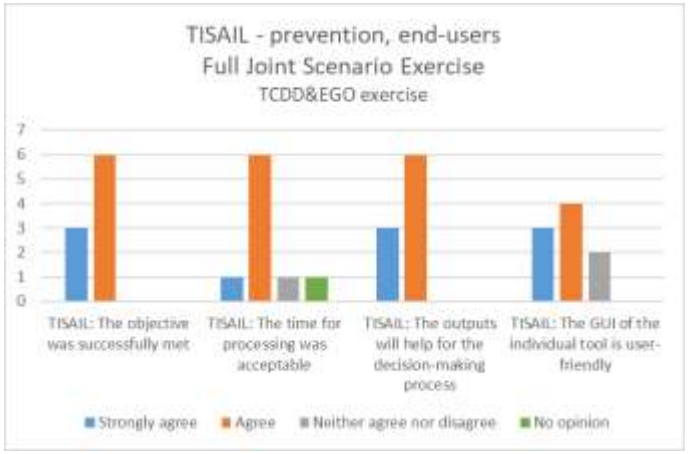

Curix - response, others
TCDD&EGO exercise
3
2
1
0
The objective was successfully met
The output will help for the response phase
The GUI of the individual tool is user-friendly
Agree

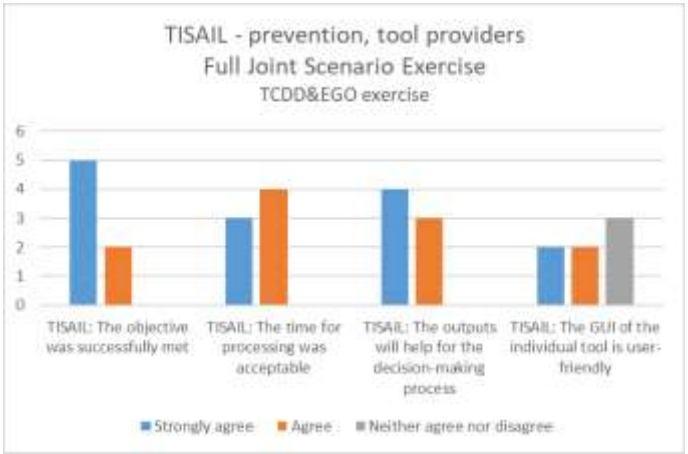
TCDD&EGO RECOVERY PHASE QUESTIONNAIRE 1

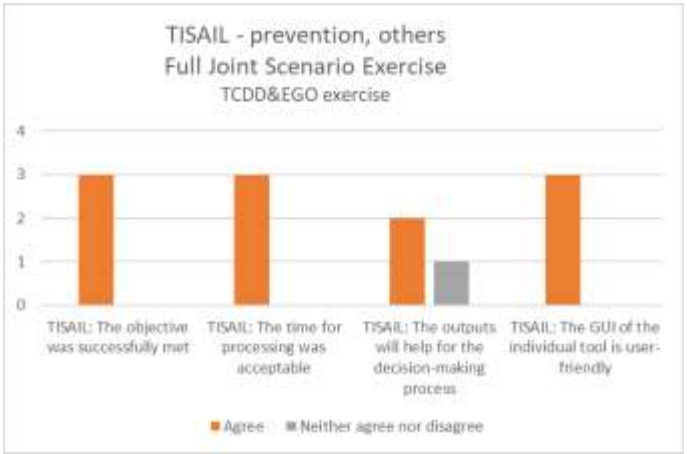
CAMS	**Objective:** Crisis Manager will be provided with time and cost needed to respond to the crisis and restore normal functioning, so that resource deployment and reaction is based on proactive actions planned. Railway operator will be aware of vulnerability and fragility of the asset after the incident, so to improve resource deployment and control financial loss in the future.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • help risk management process • The time and cost estimation in case of an attack and the awareness of the status of the assets after the attack • Positive • For the recovery phase, it is helpful to have a clear picture of what recovery or improvement activities are more adequate to control financial loss. How could this tool be improved in the context of this scenario? • With real data , seeing what is missing in the real sectario of each operator. Finetuning te customization • By researching and practicing • Same as the prevention phase.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Response planning • Can be used for the validation of recovery expenses • The end-users will be supported in quantifying the budget after an incident for a recovery scenario • capability to calculate the cost or recovery How could this tool be improved in the context of this scenario? • Can be integrated with other recovery tools • demo would be based on more clearly "actual" input data regarding e.g. cost • Maybe to give tipps for a better handling of the tool since it could be very complex for people not using it every day • estimate the time of recovery, too.

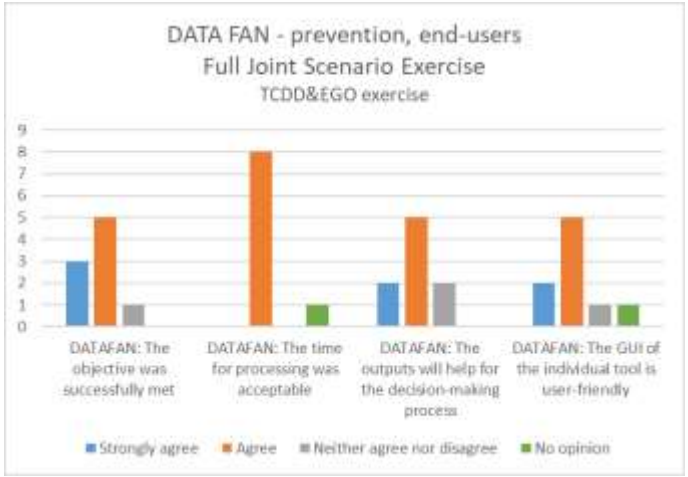
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Would help asset owner prioritise and focus response resources. How could this tool be improved in the context of this scenario? • As before needs hands on experience to really understand how best any improvement might be made.

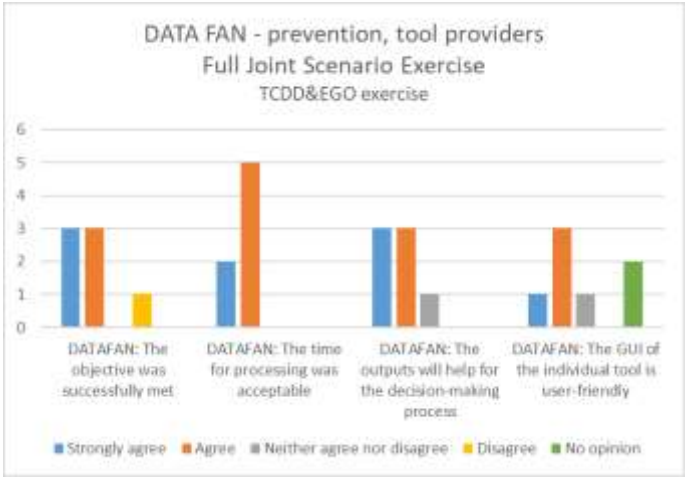
TCDD&EGO FULL JOINT SCENARIO EXERCISE QUESTIONNAIRE 3

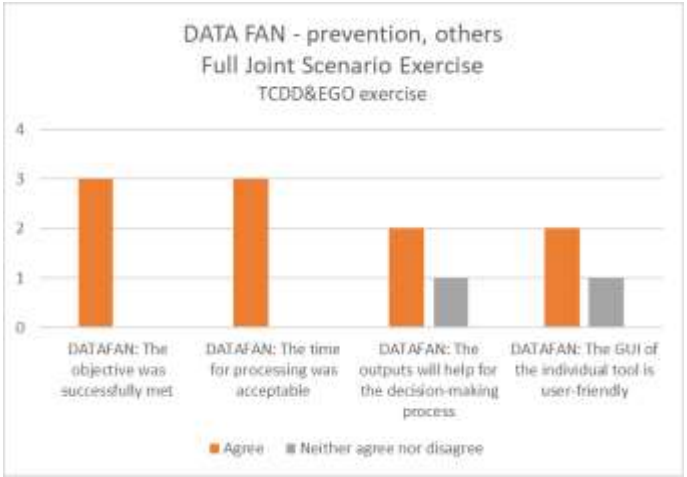

TISAIL - prevention, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
TISAIL: The objective was successfully met
TISAIL: The time for processing was acceptable
TISAIL: The outputs will help for the decision-making process
TISAIL: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

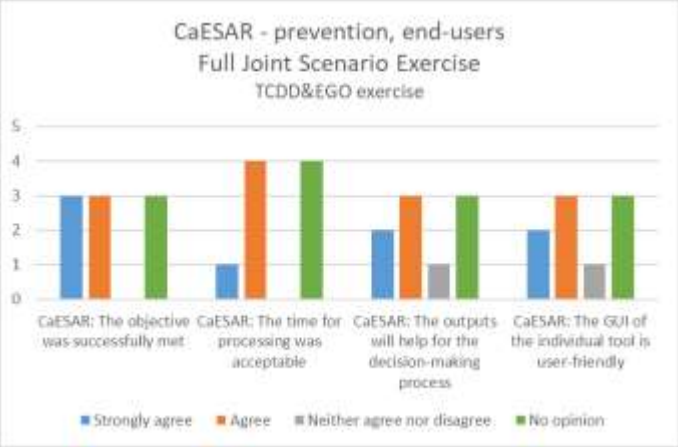

TISAIL - prevention, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
TISAIL: The objective was successfully met
TISAIL: The time for processing was acceptable
TISAIL: The outputs will help for the decision-making process
TISAIL: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree

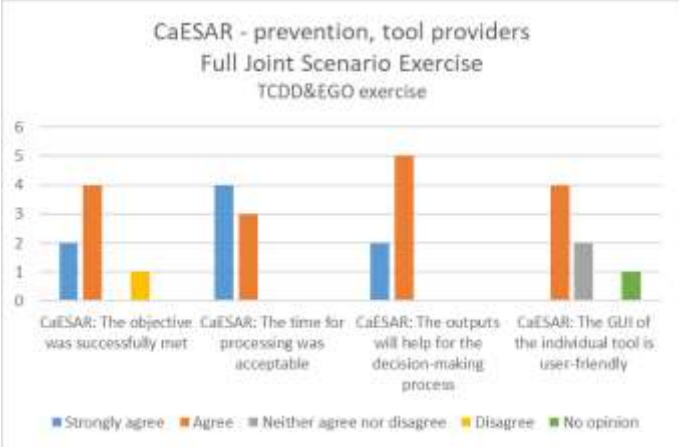

TISAIL - prevention, others
Full Joint Scenario Exercise
TCDD&EGO exercise
TISAIL: The objective was successfully met
TISAIL: The time for processing was acceptable
TISAIL: The outputs will help for the decision-making process
TISAIL: The GUI of the individual tool is user-friendly
Agree
Neither agree nor disagree

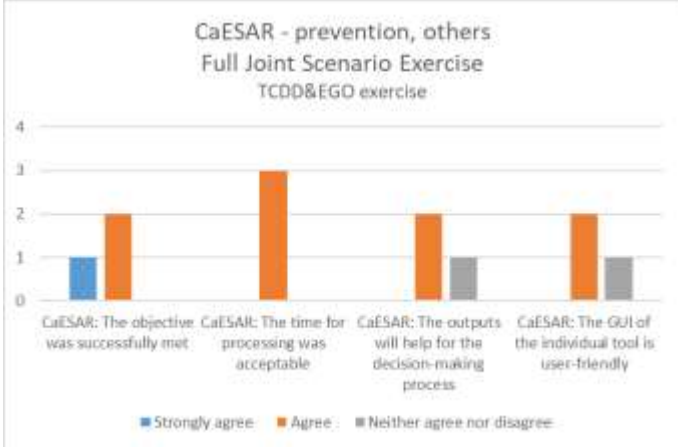

DATA FAN - prevention, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
DATAFAN: The objective was successfully met
DATAFAN: The time for processing was acceptable
DATAFAN: The outputs will help for the decision-making process
DATAFAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

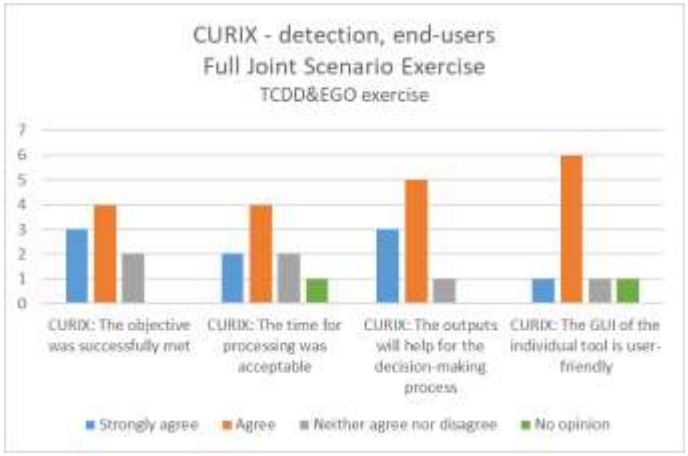

DATA FAN - prevention, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
DATAFAN: The objective was successfully met
DATAFAN: The time for processing was acceptable
DATAFAN: The outputs will help for the decision-making process
DATAFAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
Disagree
No opinion

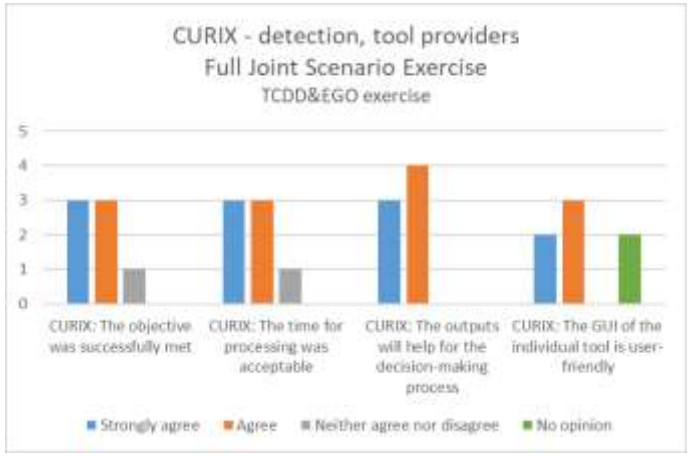

DATA FAN - prevention, others
Full Joint Scenario Exercise
TCDD&EGO exercise
DATAFAN: The objective was successfully met
DATAFAN: The time for processing was acceptable
DATAFAN: The outputs will help for the decision-making process
DATAFAN: The GUI of the individual tool is user-friendly
Agree
Neither agree nor disagree

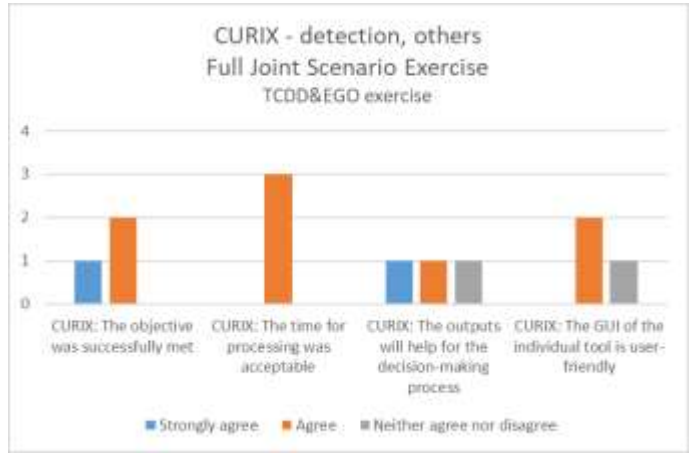

CaESAR - prevention, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
5
4
3
2
1
0
CaESAR: The objective was successfully met
CaESAR: The time for processing was acceptable
CaESAR: The outputs will help for the decision-making process
CaESAR: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

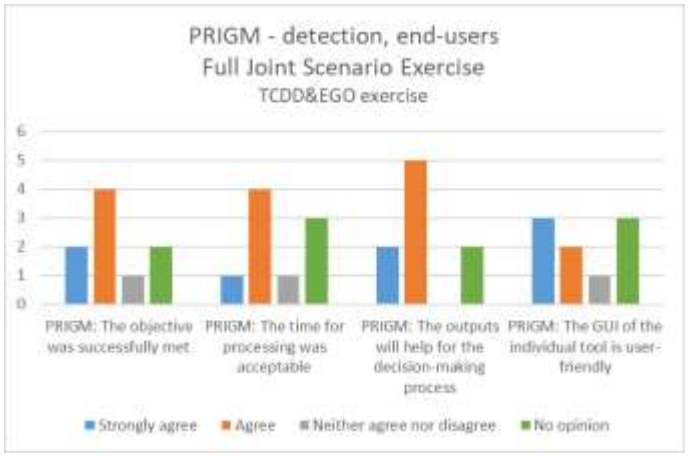

CaESAR - prevention, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
6
5
4
3
2
1
0
CaESAR: The objective was successfully met
CaESAR: The time for processing was acceptable
CaESAR: The outputs will help for the decision-making process
CaESAR: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
Disagree
No opinion

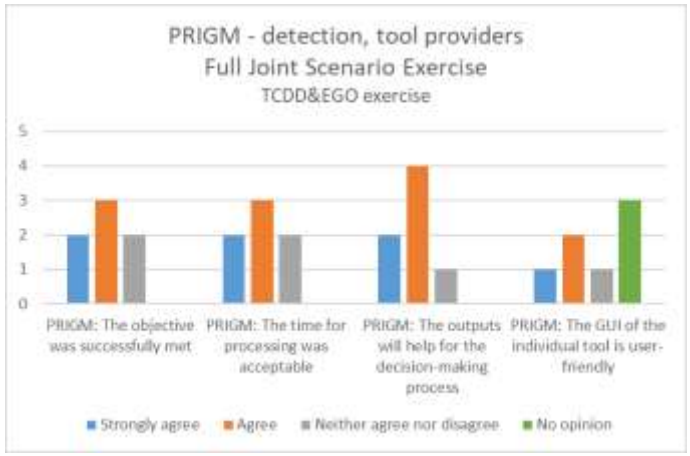

CaESAR - prevention, others
Full Joint Scenario Exercise
TCDD&EGO exercise
4
3
2
1
0
CaESAR: The objective was successfully met
CaESAR: The time for processing was acceptable
CaESAR: The outputs will help for the decision-making process
CaESAR: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree


CURIX - detection, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
CURIX: The objective was successfully met
CURIX: The time for processing was acceptable
CURIX: The outputs will help for the decision-making process
CURIX: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

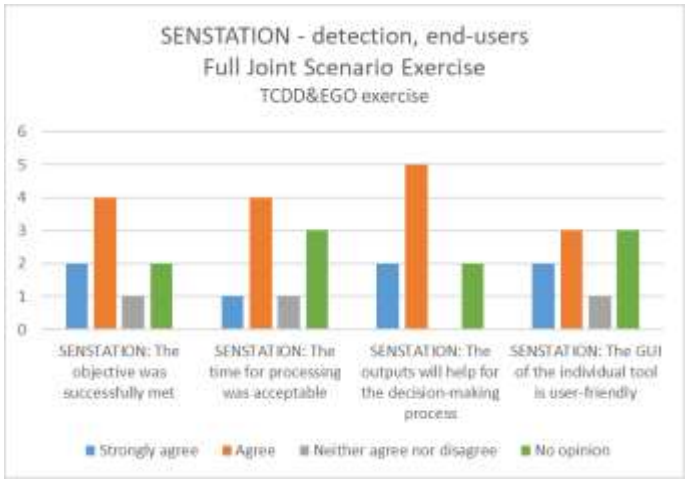

CURIX - detection, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
CURIX: The objective was successfully met
CURIX: The time for processing was acceptable
CURIX: The outputs will help for the decision-making process
CURIX: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

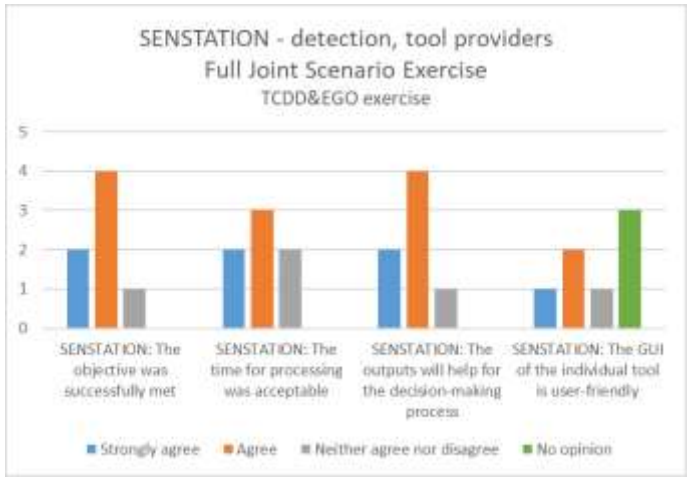

CURIX - detection, others
Full Joint Scenario Exercise
TCDD&EGO exercise
CURIX: The objective was successfully met
CURIX: The time for processing was acceptable
CURIX: The outputs will help for the decision-making process
CURIX: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree

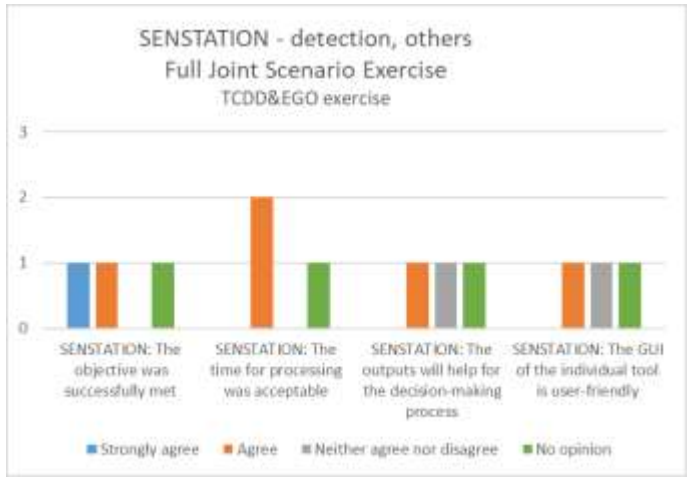

PRIGM - detection, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
PRIGM: The objective was successfully met
PRIGM: The time for processing was acceptable
PRIGM: The outputs will help for the decision-making process
PRIGM: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

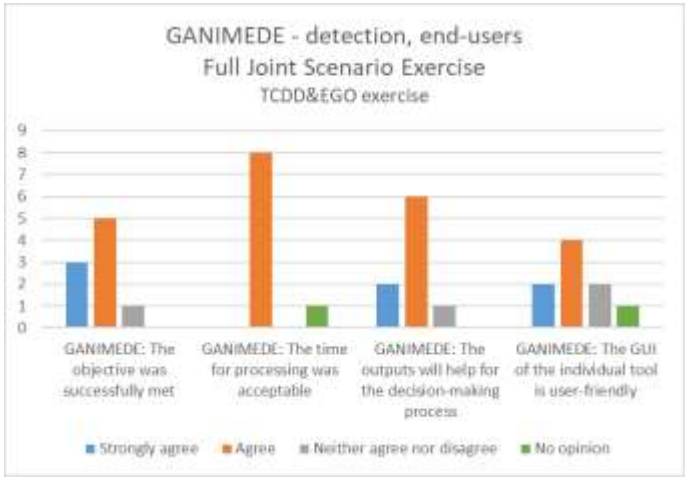

PRIGM - detection, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
PRIGM: The objective was successfully met
PRIGM: The time for processing was acceptable
PRIGM: The outputs will help for the decision-making process
PRIGM: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

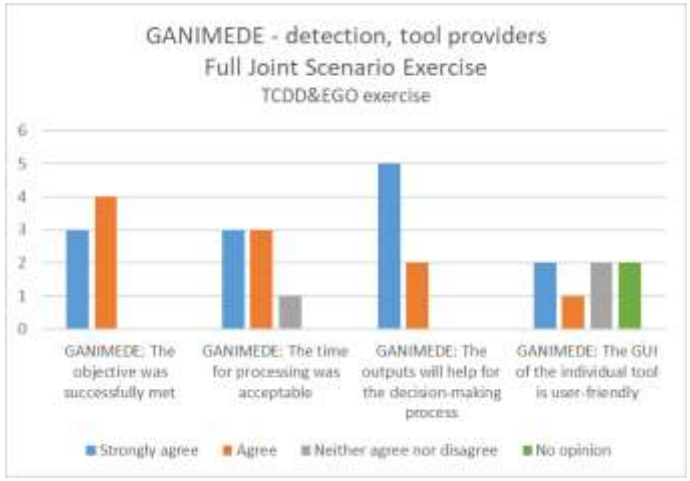

PRIGM - detection, others
Full Joint Scenario Exercise
TCDD&EGO exercise
PRIGM: The objective was successfully met
PRIGM: The time for processing was acceptable
PRIGM: The outputs will help for the decision-making process
PRIGM: The GUI of the individual tool is user-friendly
Agree
Neither agree nor disagree
No opinion

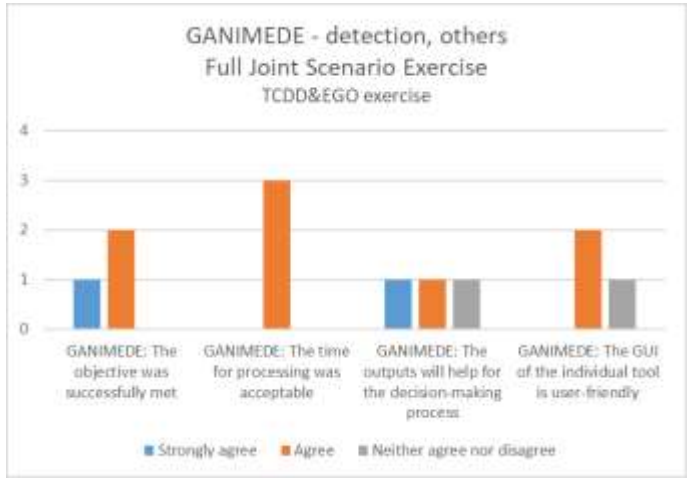

SENSTATION - detection, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
SENSTATION: The objective was successfully met
SENSTATION: The time for processing was acceptable
SENSTATION: The outputs will help for the decision-making process
SENSTATION: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

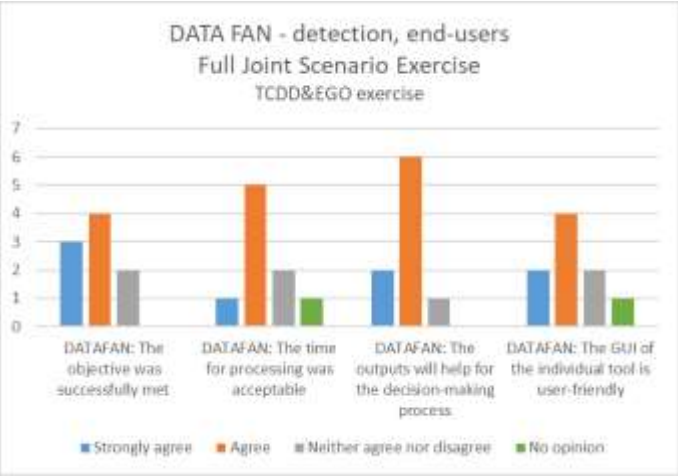

SENSTATION - detection, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
SENSTATION: The objective was successfully met
SENSTATION: The time for processing was acceptable
SENSTATION: The outputs will help for the decision-making process
SENSTATION: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

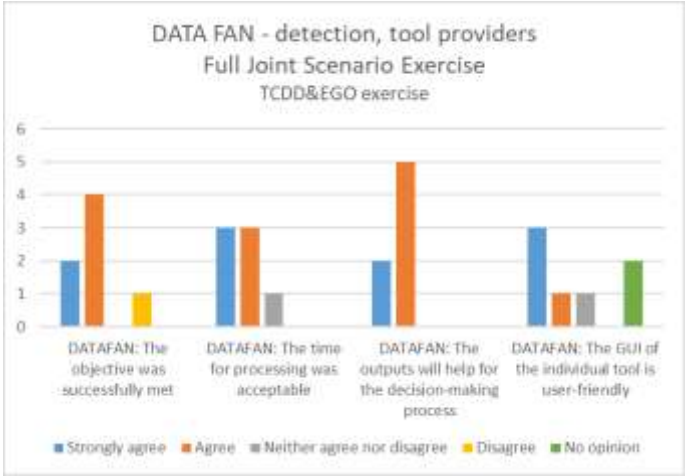

SENSTATION - detection, others
Full Joint Scenario Exercise
TCDD&EGO exercise
SENSTATION: The objective was successfully met
SENSTATION: The time for processing was acceptable
SENSTATION: The outputs will help for the decision-making process
SENSTATION: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

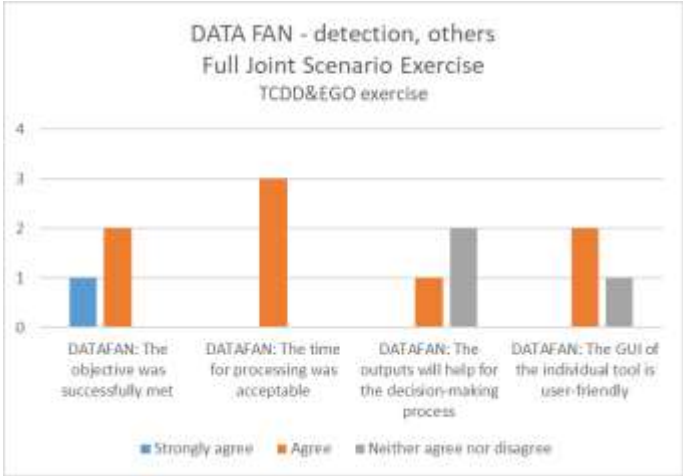

GANIMEDE - detection, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
GANIMEDE: The objective was successfully met
GANIMEDE: The time for processing was acceptable
GANIMEDE: The outputs will help for the decision-making process
GANIMEDE: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

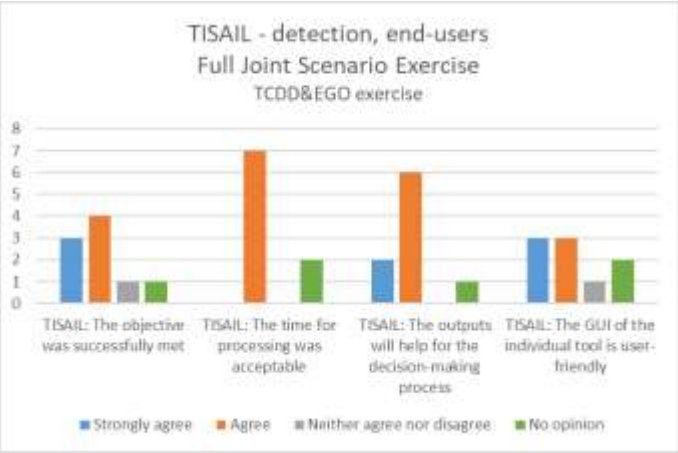

GANIMEDE - detection, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
GANIMEDE: The objective was successfully met
GANIMEDE: The time for processing was acceptable
GANIMEDE: The outputs will help for the decision-making process
GANIMEDE: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

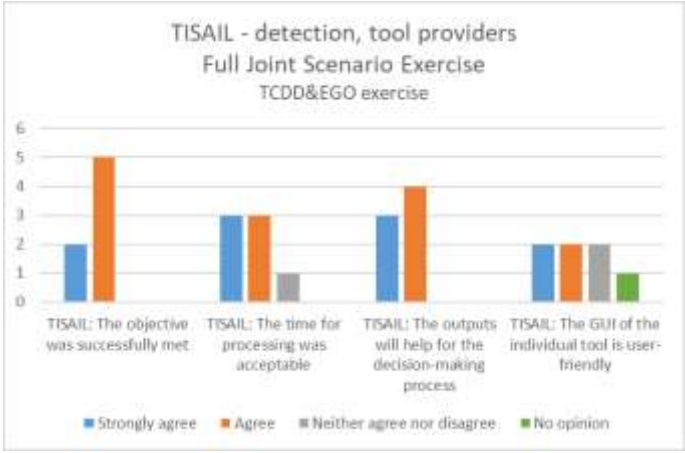

GANIMEDE - detection, others
Full Joint Scenario Exercise
TCDD&EGO exercise
GANIMEDE: The objective was successfully met
GANIMEDE: The time for processing was acceptable
GANIMEDE: The outputs will help for the decision-making process
GANIMEDE: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree

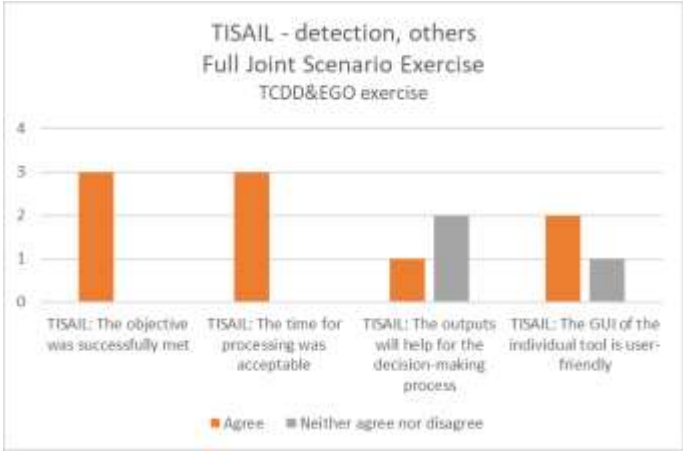

DATA FAN - detection, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
DATAFAN: The objective was successfully met
DATAFAN: The time for processing was acceptable
DATAFAN: The outputs will help for the decision-making process
DATAFAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

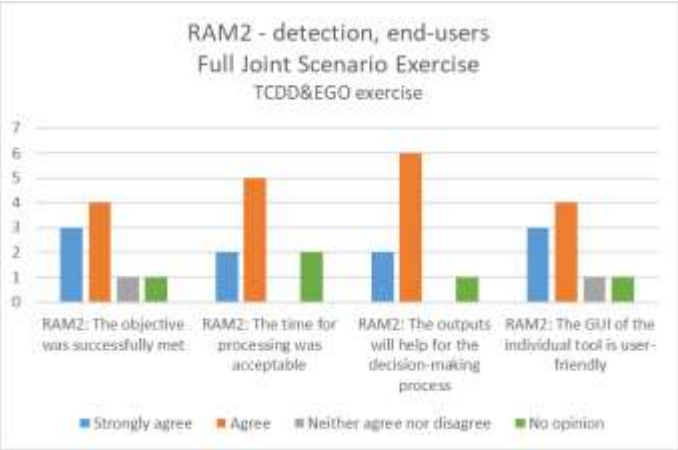

DATA FAN - detection, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
DATAFAN: The objective was successfully met
DATAFAN: The time for processing was acceptable
DATAFAN: The outputs will help for the decision-making process
DATAFAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
Disagree
No opinion

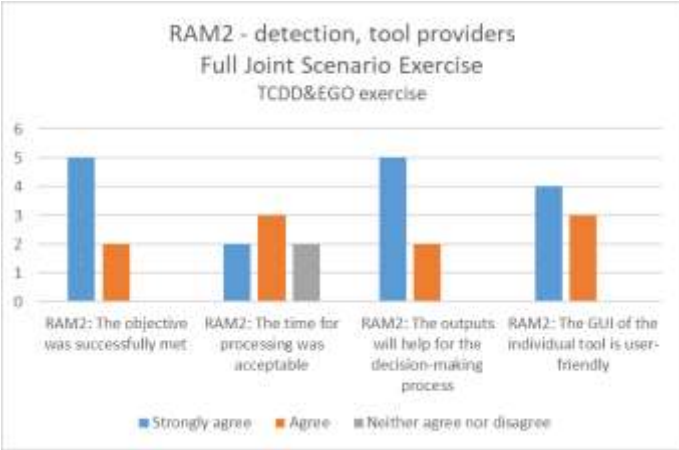

DATA FAN - detection, others
Full Joint Scenario Exercise
TCDD&EGO exercise
DATAFAN: The objective was successfully met
DATAFAN: The time for processing was acceptable
DATAFAN: The outputs will help for the decision-making process
DATAFAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree


TISAIL - detection, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
TISAIL: The objective was successfully met
TISAIL: The time for processing was acceptable
TISAIL: The outputs will help for the decision-making process
TISAIL: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

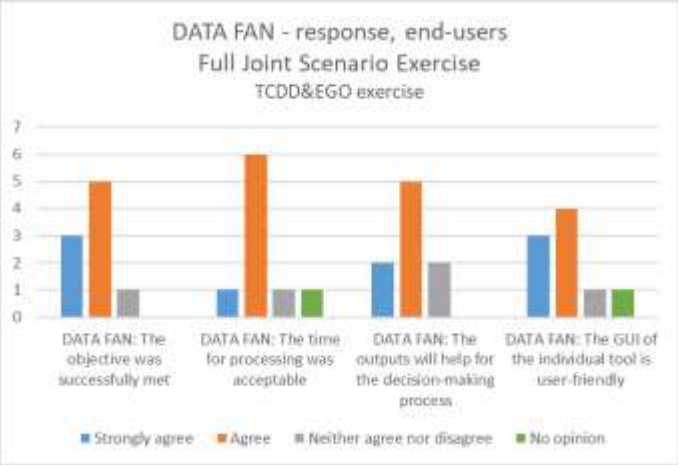

TISAIL - detection, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
TISAIL: The objective was successfully met
TISAIL: The time for processing was acceptable
TISAIL: The outputs will help for the decision-making process
TISAIL: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

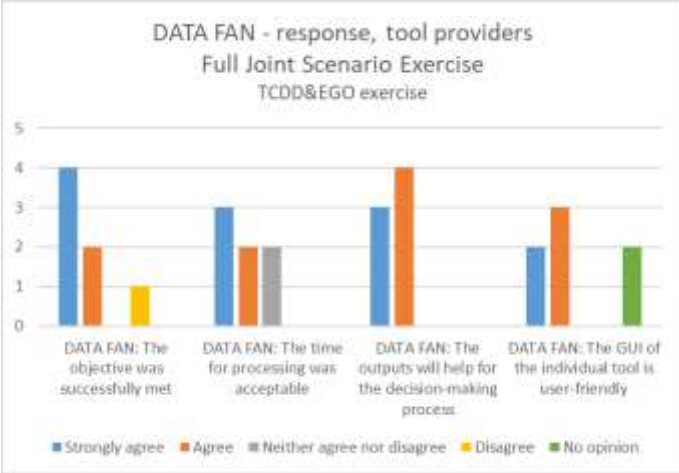

TISAIL - detection, others
Full Joint Scenario Exercise
TCDD&EGO exercise
TISAIL: The objective was successfully met
TISAIL: The time for processing was acceptable
TISAIL: The outputs will help for the decision-making process
TISAIL: The GUI of the individual tool is user-friendly
Agree
Neither agree nor disagree

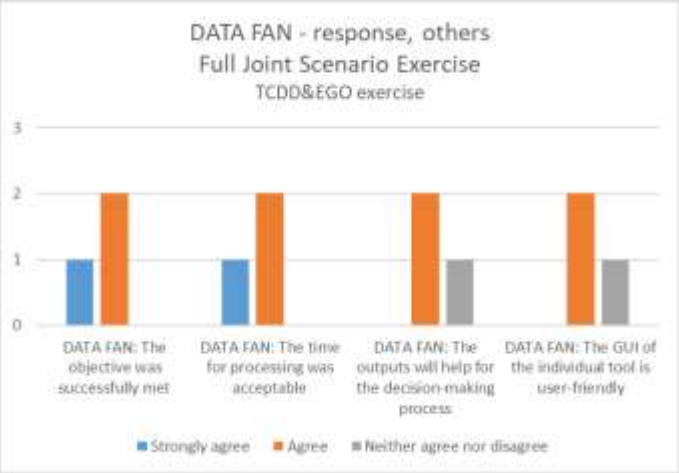

RAM2 - detection, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
7
6
5
4
3
2
1
0
RAM2: The objective was successfully met
RAM2: The time for processing was acceptable
RAM2: The outputs will help for the decision-making process
RAM2: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

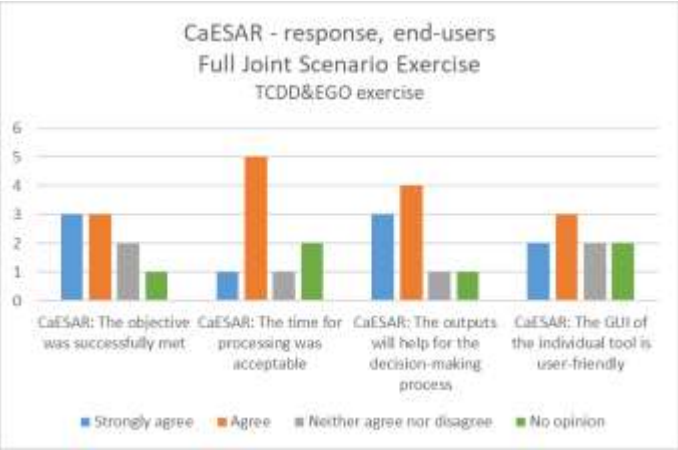

RAM2 - detection, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
6
5
4
3
2
1
0
RAM2: The objective was successfully met
RAM2: The time for processing was acceptable
RAM2: The outputs will help for the decision-making process
RAM2: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree

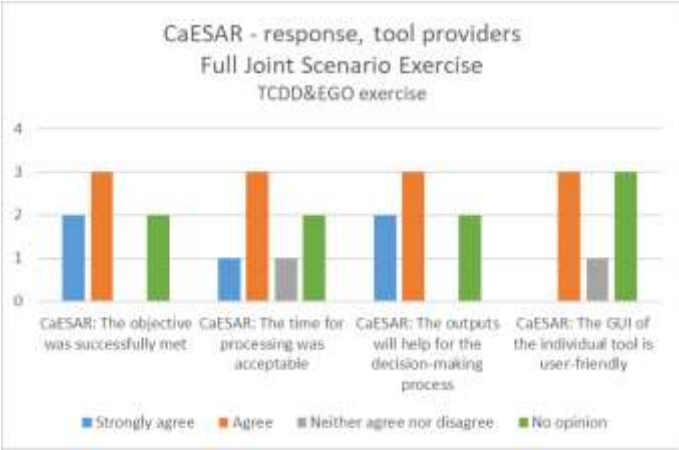

RAM2 - detection, others
Full Joint Scenario Exercise
TCDD&EGO exercise
4
3
2
1
0
RAM2: The objective was successfully met
RAM2: The time for processing was acceptable
RAM2: The outputs will help for the decision-making process
RAM2: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree

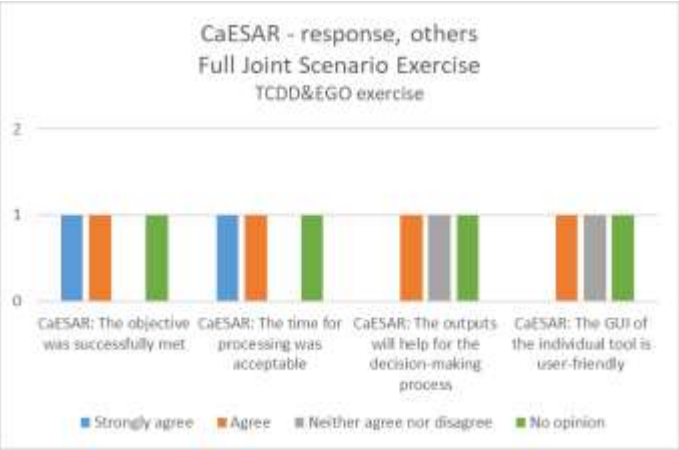

DATA FAN - response, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
DATA FAN: The objective was successfully met
DATA FAN: The time for processing was acceptable
DATA FAN: The outputs will help for the decision-making process
DATA FAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

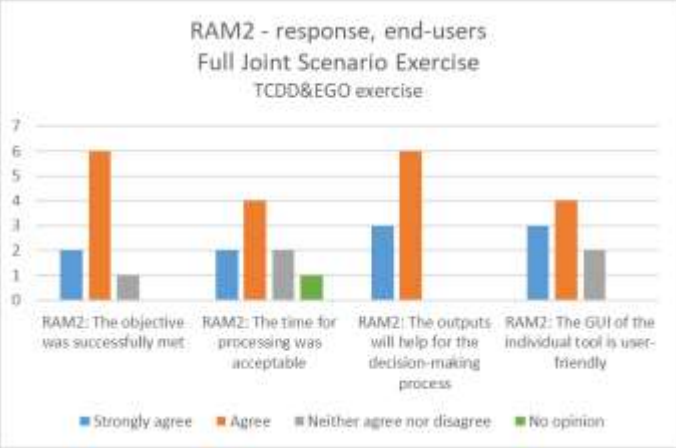

DATA FAN - response, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
DATA FAN: The objective was successfully met
DATA FAN: The time for processing was acceptable
DATA FAN: The outputs will help for the decision-making process
DATA FAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
Disagree
No opinion

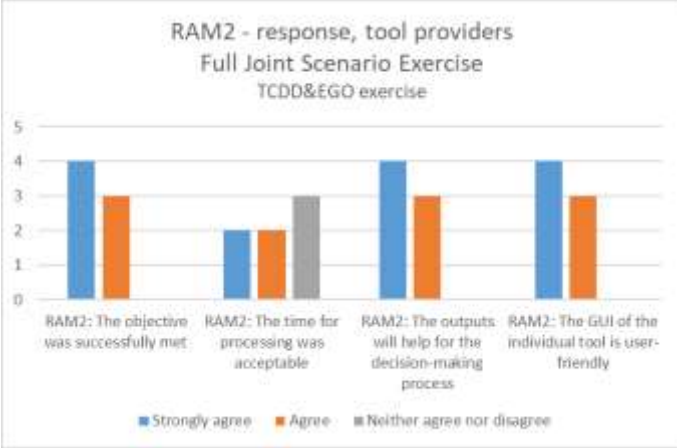

DATA FAN - response, others
Full Joint Scenario Exercise
TCDD&EGO exercise
DATA FAN: The objective was successfully met
DATA FAN: The time for processing was acceptable
DATA FAN: The outputs will help for the decision-making process
DATA FAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree


CaESAR - response, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
CaESAR: The objective was successfully met
CaESAR: The time for processing was acceptable
CaESAR: The outputs will help for the decision-making process
CaESAR: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

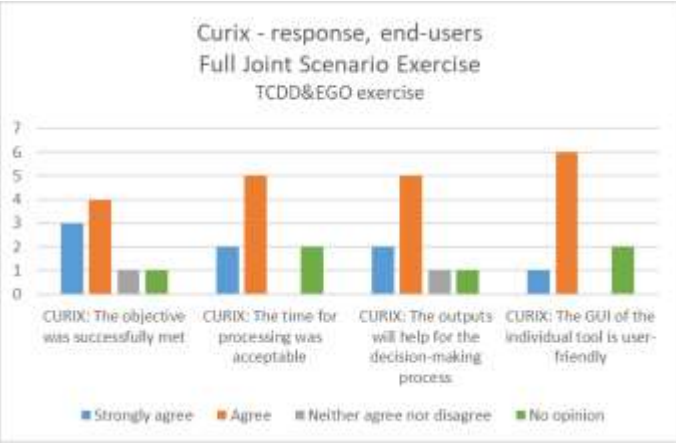

CaESAR - response, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
CaESAR: The objective was successfully met
CaESAR: The time for processing was acceptable
CaESAR: The outputs will help for the decision-making process
CaESAR: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

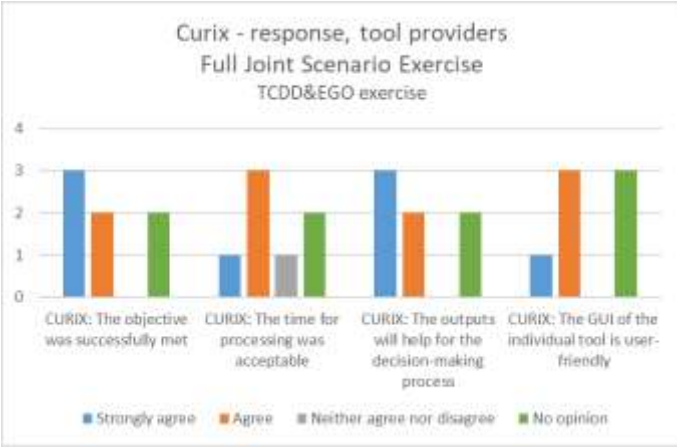

CaESAR - response, others
Full Joint Scenario Exercise
TCDD&EGO exercise
CaESAR: The objective was successfully met
CaESAR: The time for processing was acceptable
CaESAR: The outputs will help for the decision-making process
CaESAR: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

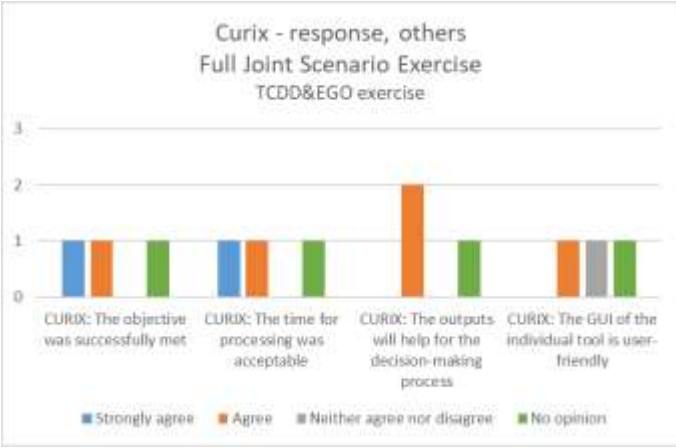

RAM2 - response, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
RAM2: The objective was successfully met
RAM2: The time for processing was acceptable
RAM2: The outputs will help for the decision-making process
RAM2: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion


RAM2 - response, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
RAM2: The objective was successfully met
RAM2: The time for processing was acceptable
RAM2: The outputs will help for the decision-making process
RAM2: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree

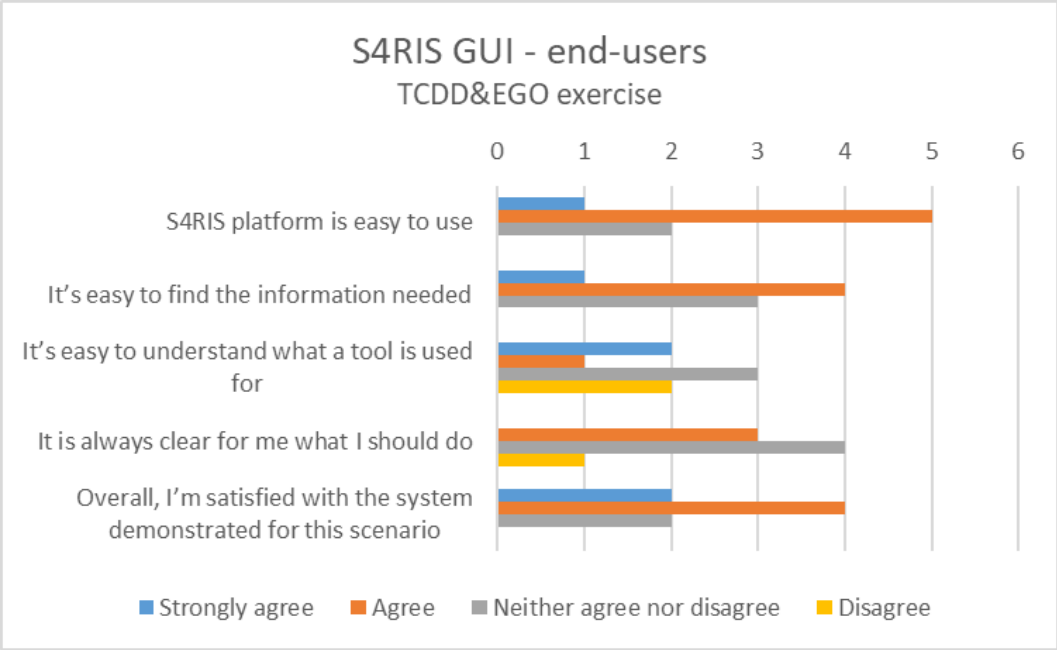

RAM2 - response, others
Full Joint Scenario Exercise
TCDD&EGO exercise
RAM2: The objective was successfully met
RAM2: The time for processing was acceptable
RAM2: The outputs will help for the decision-making process
RAM2: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree


Curix - response, end-users
Full Joint Scenario Exercise
TCDD&EGO exercise
CURIX: The objective was successfully met
CURIX: The time for processing was acceptable
CURIX: The outputs will help for the decision-making process
CURIX: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion


Curix - response, tool providers
Full Joint Scenario Exercise
TCDD&EGO exercise
CURIX: The objective was successfully met
CURIX: The time for processing was acceptable
CURIX: The outputs will help for the decision-making process
CURIX: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion


Curix - response, others
Full Joint Scenario Exercise
TCDD&EGO exercise
CURIX: The objective was successfully met
CURIX: The time for processing was acceptable
CURIX: The outputs will help for the decision-making process
CURIX: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

TCDD&EGO S4RIS GUI QUESTIONNAIRE 6



What could be improved in the GUI?

- Without experiencing it for a while, I can't say anything based on what's been told.
- better integration of the data provided by the tools
- An introduction to the scenarios could be added when you hit Madrid or Ankara. The fonts could be normalised (same font for all the system)

What complexity / functions are not necessary and can be deleted or reduced?

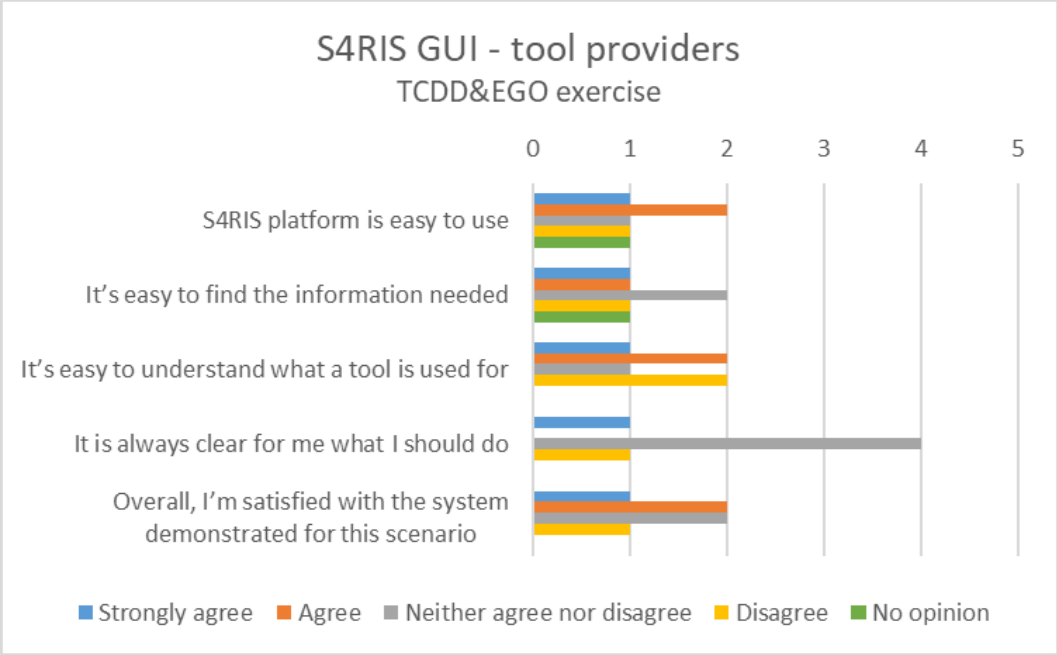
- Without experiencing it for a while, I can't say anything based on what's been told.

What could be improved to make the handling more transparent?

- Without experiencing it for a while, I can't say anything based on what's been told.
- Main point is that it should be very clear what the purpose and useability of a tool is and how the tools are connected to of differ from anotherer
- adapt the GUI to the type of user with the information/tools he needs to know depending on his position in the company
- One login should be enough to get to the different tools. I have tried the system and some tools do not work, others ask for another log in credentials different from the ones in S4RIS. For instance, I cannot create a user for CAMS, the system does not give me the option.

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- Without experiencing it for a while, I can't say anything based on what's been told.



What could be improved in the GUI?

- Diferent position of the menu
- Since it is evolving there is much work needed. But iframes can be larger.
- GUI is stil in development as such the "disagree" ansers given above.

What complexity / functions are not necessary and can be deleted or reduced?

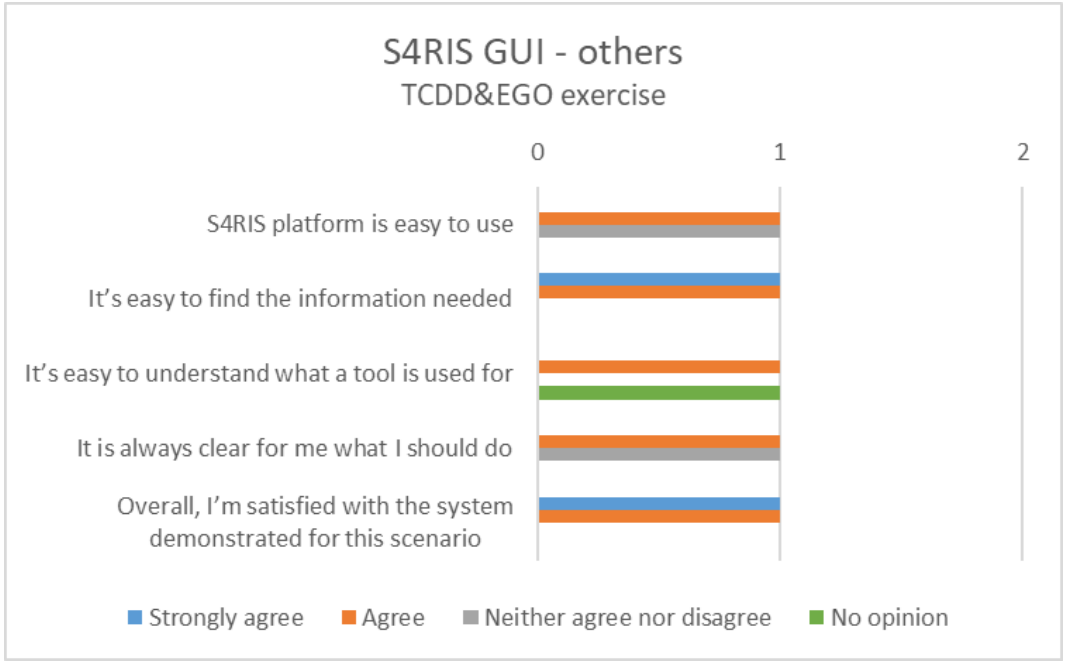
- Point to be considered more broadly in terms of what is achievable and useful still in project based on actual knowledge

What could be improved to make the handling more transparent?

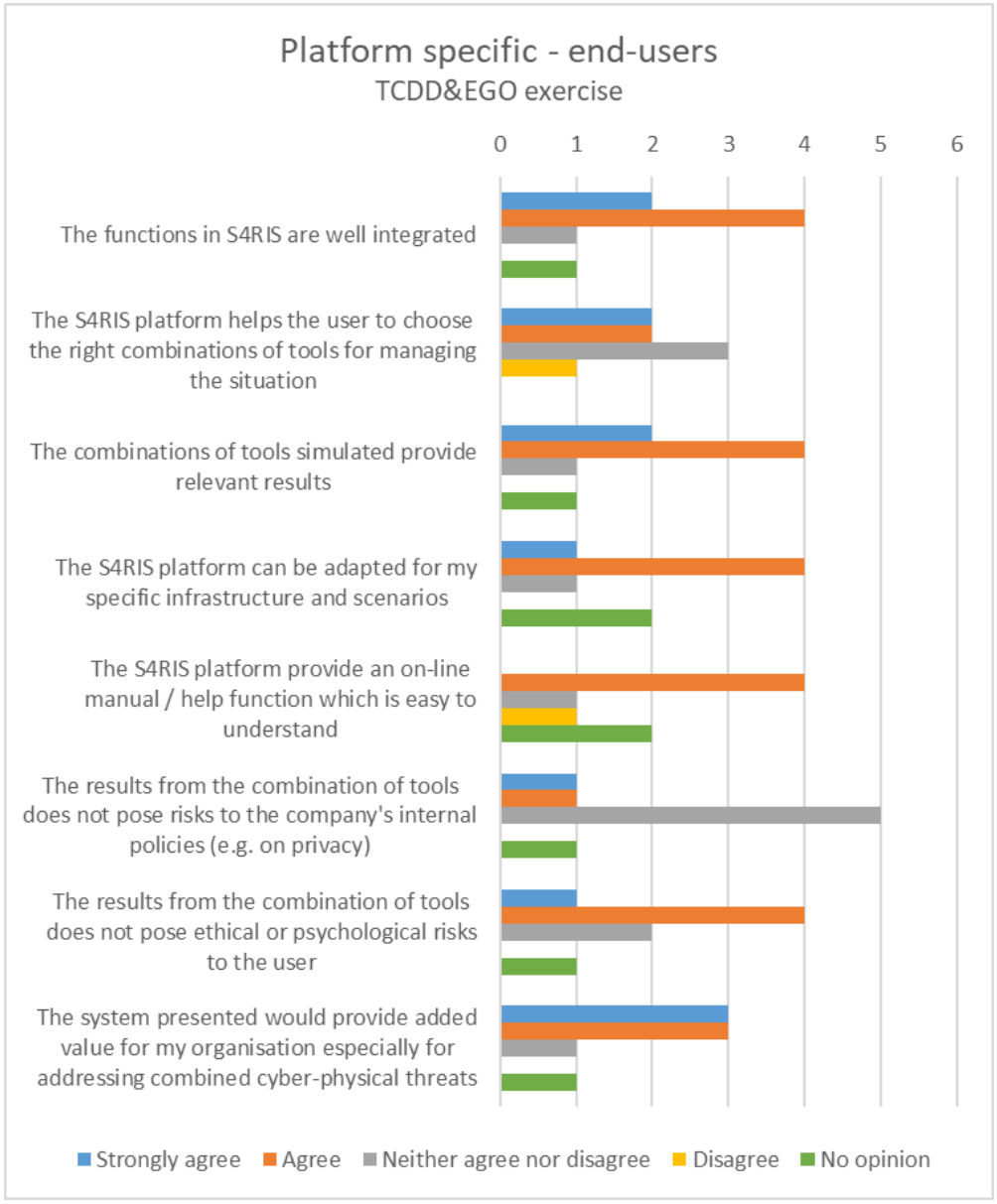
- Full screen option for the inner window
- Point to be considered more broadly in terms of what is achievable and useful still in project based on actual knowledge

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- A wiki-based user guide can be proposed
- Point to be considered more broadly in terms of what is achievable and useful still in project based on actual knowledge


S4RIS GUI - others
TCDD&EGO exercise
0
1
2
S4RIS platform is easy to use
It's easy to find the information needed
It's easy to understand what a tool is used for
It is always clear for me what I should do
Overall, I'm satisfied with the system demonstrated for this scenario
Strongly agree
Agree
Neither agree nor disagree
No opinion

TCDD&EGO PLATFORM SPECIFIC QUESTIONNAIRE 6



Were there situations where you did not understand what the system was doing?

- No
- Without experiencing it for a while, I can't say anything based on what's been told.
- I had trouble in understanding (the progress in) the Tisail tool. Moreover it seems that some of the tools "do the same thing but on another subject". So it would be good to explain the differences and the different user possibilities of the different tools
- no
- No it was so clear
- No, but it didn't show the tools when I initiated them in the system.

Would you recommend the system presented to your colleagues and why?

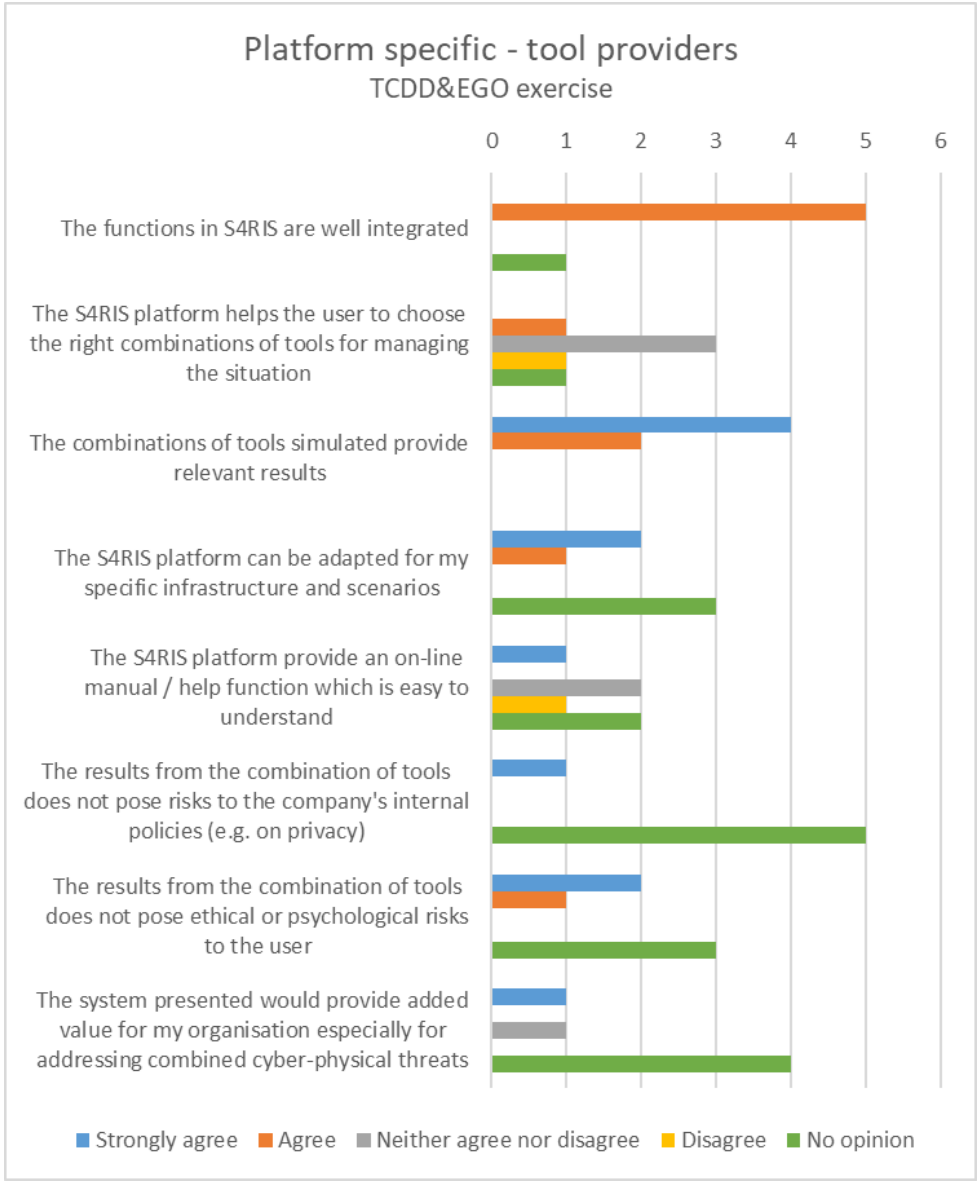
- Yes
- Yes
- At this moment within our organization we agreed I would be the representative to join the simulation and after that decide for which colleagues this could be interesting. So i'm still thinking about that and what would be the best way to introduce them to the system.
- yes
- Yes. It is so helpful for decision making, take actions and improve strength

What could be improved in the context of this scenario?

- Without experiencing it for a while, I can't say anything based on what's been told.
- more tools integrated

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- Without experiencing it for a while, I can't say anything based on what's been told.



Were there situations where you did not understand what the system was doing?

- The scenarios and main goals of the tools can be presented in a more user-friendly way.

Would you recommend the system presented to your colleagues and why?

- Not yet.

What could be improved in the context of this scenario?

- Demonstrations covering the time-critical scenarios and scalability (big data etc.)
- There was a mismatch between what was presented in the joint simulation and the questions in the questionnaires. There was also some mismatch between the scenario objectives in the questionnaire compared to what was actually presented and/or demonstrated.

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- More self-triggering scenarios dealing with instant messaging, and integration of more recovery tools in joint exercises.
- Based on present status, it may be that req/spec defined for S4RIS UI / GUI should be reviewed.

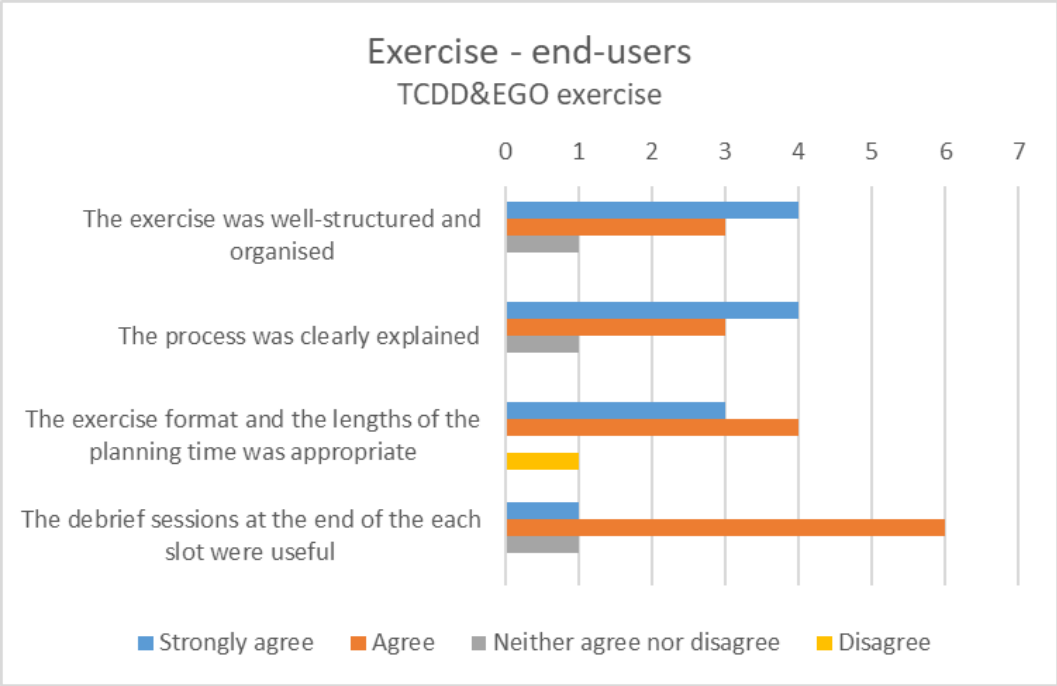
Were there situations where you did not understand what the system was doing?

- Yes. I only attend one of the 2 days - maybe that is the reason.

Would you recommend the system presented to your colleagues and why?

- Yes - to inspire them

TCDD&EGO EXERCISE QUESTIONNAIRE 6



Which part of the exercise did you find the most useful and why?

- It was a whole. All of them had some useful points.
- the Joint exercise
- It should be face to face. Because exrrcise time way longer than a standart meeting. It iş hard to keep concentrate
- Some tool presentations were very useful to understand the outputs of the tool.

Were there any parties missing whose participation would have given added value for the exercise?

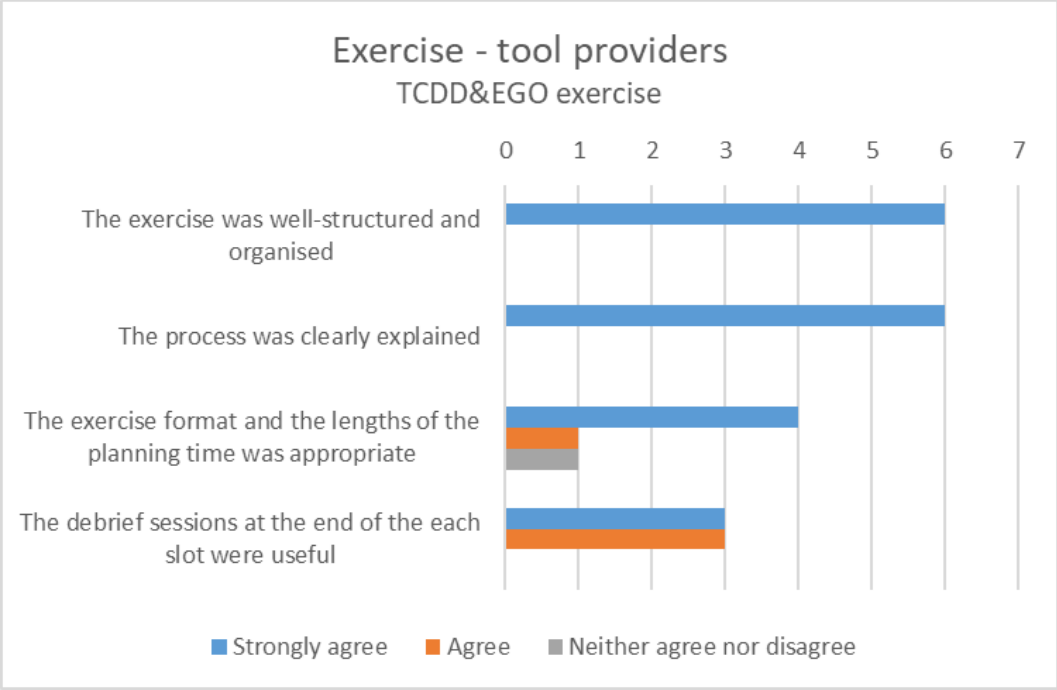
- I cannot answer this question without detailed study.
- more feedback from the end-users

What can be done differently for the next exercises or what improvement need to be made?

- I cannot answer this question without detailed study.
- in person simulation exericse
- It should be face to face
- I would shorten the technical explanations of the tools and focus more on the scenario and the information that would be useful for the end-user. It may be hard to follow so many tools in a short period of time. This time I watched the recording of the Day 2 because I couldn't attend the virtual meeting and it was certainly helpful to scroll around the video to rewatch some parts that I did not understand, but of course it took more time than expected.

What are the main lessons learnt for you and why?

- There were some very important teachings in this work. Data were evaluated from many perspectives. It was useful work.
- Databased decision making with regard to (security)measures is an option. The use of deep learning/algoritms is developing
- the solutions demonstrated and especially their combinaition are very promising



Which part of the exercise did you find the most useful and why?

- joint exercise itself.
- Joint simulation - how tools work together
- demonstration of capabilities

Were there any parties missing whose participation would have given added value for the exercise?

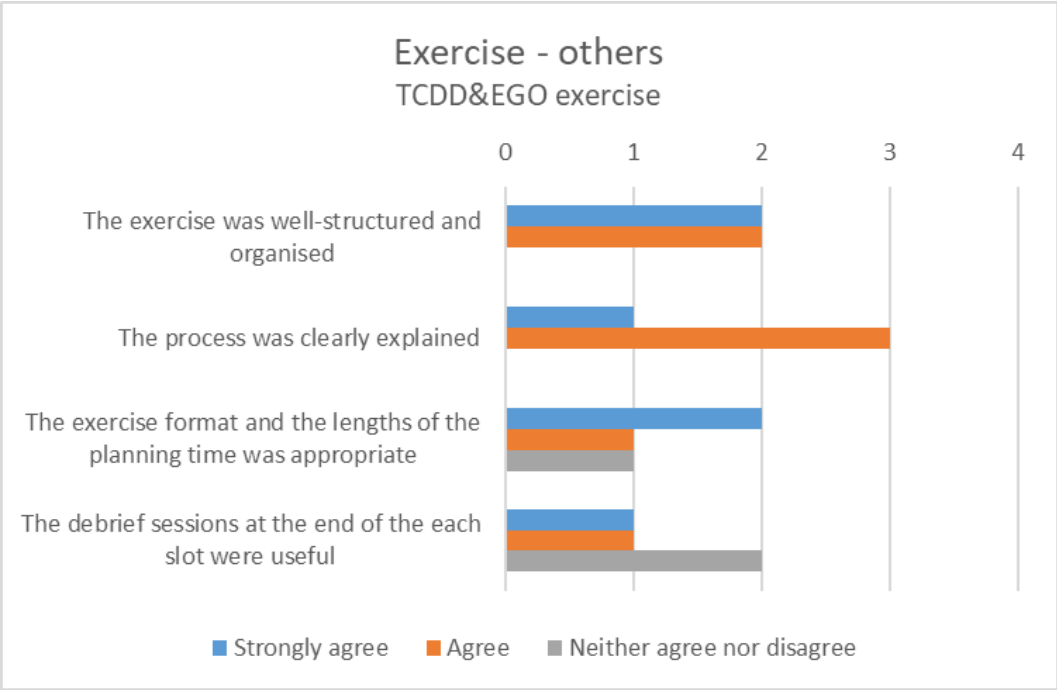
- other tools....
- Critical questions from advisory board

What can be done differently for the next exercises or what improvement need to be made?

- End-users need to be promoted at beforehand as they are asked to prepare questions and comments.
- Detection / response individual presentations before or combined with the joint simulation could have helped viewer

What are the main lessons learnt for you and why?

- It could be more proactive. Maybe because of its virtual characteristics
- Closer preparation/checking between tool presentation / demos and questionnaires



Which part of the exercise did you find the most useful and why?

- I found the full joint scenario exercice the most useful as it showed the interaction between all individual tools. It was clearly explained and gave depth to the individual exercices.
- The simulation process
- The demonstration of the S4RIS platform and how it would look when all tools are integrated. It offered an overview of how the system will look at the end of the project and how all the demonstrated tools will work together in a threat scenario.

Were there any parties missing whose participation would have given added value for the exercise?

- More end-users representatives.
- rescue services, gard services, police authorities

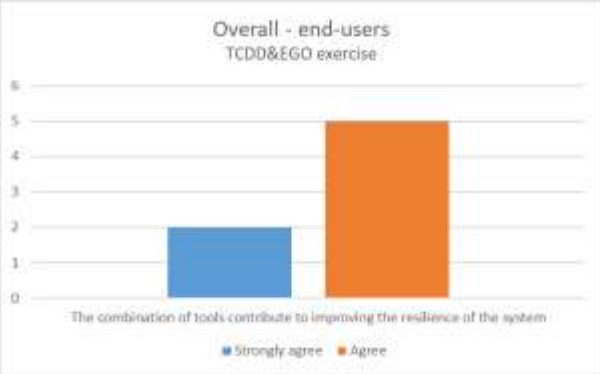
What can be done differently for the next exercises or what improvement need to be made?

- I believe the exercice was well organised and the different Powerpoints were quite interactive. Maybe the individual exercices presentations could be made a bit shorter.
- create a broad panel that can comment on the exercice and tool. Broad meaning : stakeholders from consortium together with stakeholders not belonging to the consortium and railways sector. The OT part is not really analysed -

What are the main lessons learnt for you and why?

- How the individual tools can work together to provide efficient detection and response to an incident from different data points.
- A integrated solution should be possible

TCDD&EGO OVERALL QUESTIONNAIRE 6



Which capabilities are the most important/useful for this scenario?

- Tümetmenleriveetkileridetaylıolarakelealınmasıönemli.
- Detection of abandoned luggage. And in general the fact that it is possible to have a data driven decision making process
- integration,
- Threat detection

What are the current obstacles for adopting such a system?

- Habits and having a new system.
- Financial (cost)/security
- data availability for training the tools based on machine learning
- Data privacy
- The complexity of changing the current operational schemes for crisis communication and the added complexity of integrating so many tools into one system.

What could be improved in the context of this scenario?

- Can be detailed
- I would propose to do questionnaires after each tool. Not sure if this would be efficient, but it may help to get more clear answers from the end-users if the questionnaire is done right after each tool is used. Just floating an idea.

Has any limitation of tools been discovered during the exercise? If so, please specify.

- Data would be more realistic. But beqcıuse of privacy it iş hard to maintain

What is the overall added value as may be assessed from your own experience in your current daily work?

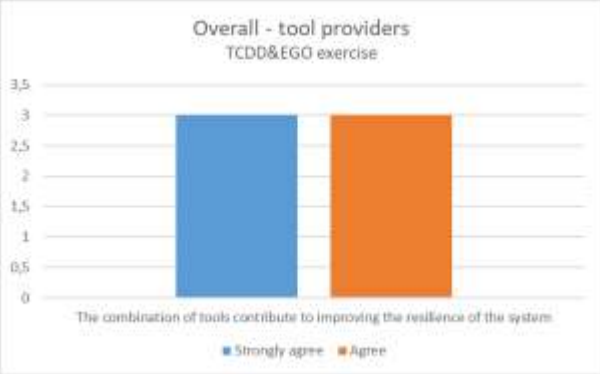
- Positive
- See earlier answer: data based decision making
- combining lalerts from different tools and provide mitigation measures in real time
- They help mainly on basit tasks so we can focus more sophisticated tasks

What were the main lessons learnt by you and why?

- In such studies, all data and details must be carefully evaluated and processed appropriately.
- See earlier answer
- combination of tool is very powerful - data provision is a challenge - standards are needed for data and communication

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- Can be detailed



Which capabilities are the most important/useful for this scenario?

- IoT-enabled live demos show that system is getting more responsive to instant messaging.
- Seemed detection capailities

What are the current obstacles for adopting such a system?

- Explainability of the tools. Scalability and responsiveness (especially for time-critical missions.)
- integration of tools with end-user infrastructure to get data is a challenge;

What could be improved in the context of this scenario?

- More evidence-based and multimodal cases can be incorporated (e.g. other modes of transportatin)

Has any limitation of tools been discovered during the exercise? If so, please specify.

- Prediction models can be improved. More quantitative measures cost of countermeasures, reliabiltiy scoring, etc. needed. No evidence about the scalability of the tools.
- Demonstration of reliability (but OK not products yet), more evidence based on quantitative data should be provided.
- 1)Not clear how tools would behave in normal mode, would we have some false alarms and wrong decision support?; 2) Th partners have elaborate alarms/messages for specific scenarios where a lot of knowledge about the scenario go into, would the the alarms/messages be precise enough for scenarios which were not yet covered or are unknown? Perhaps introducing parts of scenario/data which is unknown tools and partners similar to a blinded experiment could be helpful.

What is the overall added value as may be assessed from your own experience in your current daily work?

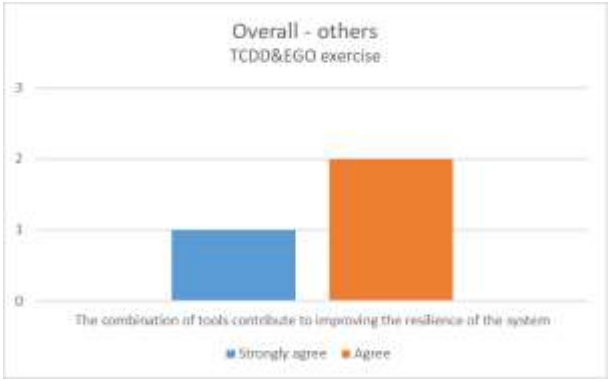
- Interoperability of tools is getting better.
- Increase resilience

What were the main lessons learnt by you and why?

- There is more work needed to elaborate the scenarios by addig LEAs and practitioners, like fire brigades, ambulances, etc.
- See earlier responses

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- See earlier responses

	Which capabilities are the most important/useful for this scenario? • Detection and response • the end to end integration What are the current obstacles for adopting such a system? • Possibly the interaction between the tools and well as large scale implementation. • the integration to the existing IT landscape What could be improved in the context of this scenario? • IT - OT interactions & emphasize the cyber attack Has any limitation of tools been discovered during the exercise? If so, please specify. • No. • OT specific for the railways What is the overall added value as may be assessed from your own experience in your current daily work? • cooperation between different tools to fulfill end-user expectations. What were the main lessons learnt by you and why? • As I did not attend the MDM exercice, I discovered the interaction between the tools for the first time (in the context of a physical and cyber attack).

ANNEX VII Assessment of how far the TCDD&EGO scenario objectives were met based on evaluation

The correspondence of the evaluation results with the objectives set for the tools in each exercise phase is presented in following tables. In the estimation of the achievement of objectives the following classification has been used:

- Fulfilled according to the majority – more than half of the respondents have answered “strongly agree” or “agree” to question “The objective was successfully met”
- Partially fulfilled according to the majority – half of more of the respondents have answered “neither agree nor disagree” to question “The objective was successfully met”
- Not fulfilled according to the majority – more than half of the respondents have answered “disagree” or “strongly disagree” to question “The objective was successfully met”

WARNING: The “good faith” evaluation is based on the data provided in the Annex VI which can include only limited responses and was based on what was seen at the simulation exercise.

TCDD&EGO SIMULATION EXERCISE - REQUIREMENTS FOR THE PREVENTION PHASE

Tool	**TCDD&EGO Scenario objectives**	**Integrated in S4RIS (Y/N)**	**Result of evaluation**
CAMS	The individual tool will be used to inform the metro operator to allocate to repair/maintain/ rehabilitate the infrastructure after a set of possible events, therefore providing the necessary input to make a proactive plan and be ready in case of an attack. The metro operator will also be provided with information regarding the asset condition and degradation due to normal ageing, enabling timely response ahead of malfunctioning.		Fulfilled according to the majority
SECURAIL	Allow off-line risk analysis of the metro infrastructure to understand the level of risk for each critical asset during a given hazardous event. Perform a cost benefit analysis of the		Fulfilled according to the majority

Tool	TCDD&EGO Scenario objectives	Integrated in S4RIS (Y/N)	Result of evaluation
	infrastructure to understand which of the solutions analysed to reduce the risk level is the best, considering both costs and benefits.		
TISAIL	Provide situational awareness about vulnerabilities that could be exploited by attackers: e.g. CCTV, Power Grid, Windows 10.		Fulfilled according to the majority
DATAFAN	DATAFAN will focus on the reliable prediction of passenger load on specific metro stations and provides information about the expected number of passengers to happen in the day of the event. The end-user will be able to run what-if scenarios to analyse how they will affect the number of passengers and delays in the infrastructure (e.g., the closure of a station).		Fulfilled according to the majority
CaESAR	CaESAR will focus on the analysis of weak components, mitigation measures, and the overall resilience of the system. The Operational Centre Supervisor asks the user to implement mitigation measures to test which of them would work better on the infrastructure.		Fulfilled according to the majority
iCrowd	iCrowd will focus on the simulation of infiltration/escape scenarios to better understand the chance of detection for different CCTV cameras and guard configurations. It will provide simulation capabilities to understand the probability of detecting a malicious actor attempting to break into the EER, therefore assessing the effectiveness of CCTV camera location and guards to eventually improve them.		Fulfilled according to the majority

TCDD&EGO SIMULATION EXERCISE - REQUIREMENTS FOR THE DETECTION PHASE

Tool	**Objective for the TCDD&EGO exercise**	**Integrated (Y/N)**	**Result of evaluation**
Ganimede	Ganimede will be focused on the detection of objects and people in each frame and their movement to determine if the object is candidate for being abandoned		Fulfilled according to the majority
CuriX	Crisis Manager will be able to be alerted when deviations from normal behaviour (anomalies) or potentially upcoming disruptions of technical systems (IT and OT) from their monitoring data are detected. The crisis manager can check metrics and which technical devices are responsible for causing the major change in the system behaviour. The crisis manager can monitor the health of the monitored technical system.		Fulfilled according to the majority
PRIGM	Analysis of log data of main security operations (e.g., authentication, encryption, key exchange, etc) to determine anomalies, monitor the authentication flow for misuses/spoofing and help to discriminate between flooding data and normal flow. Furthermore, tracing and detection of cyber anomalies will be enabled, therefore assisting other countermeasure tools for enhanced resilience.		Fulfilled according to the majority
SENSTATION	Secure Gateway at edge nodes responsible from data protection where data is generated. It allows receive some instant information from the Electronic Equipment room to monitor unauthorised physical access, so that the operator can alert the security guard and the main Command and Control Centre.		Fulfilled according to the majority

Tool	Objective for the TCDD&EGO exercise	Integrated (Y/N)	Result of evaluation
DATAFAN	Data gathered regarding the flow of passengers will be used to detect significantly high passenger volumes in stations and trains, also considering days with really crowded events.		Fulfilled according to the majority
TISAIL	Crisis Manager will be able to correlate the information (e.g., IoCs) provided by TISAIL for detecting threats in their networks using their security tools (e.g., IDS, SIEMs).		Fulfilled according to the majority
RAM2	RAM2 processes cyber physical assets information and events, received from S4RIS monitoring tools, for identification of vulnerabilities and provides risk assessments within the operations context. For example, it will be able to correlate the different attack vector happening in the station.		Fulfilled according to the majority

TCDD&EGO SIMULATION EXERCISE - REQUIREMENTS FOR THE RESPONSE PHASE

Tool	Objective for the TCDD&EGO exercise	Integrated (Y/N)	Result of evaluation
RAM2	Risk-based prioritization of issues, case management for tracking response actions. End-user consumes the data through RAM2 Dashboards display. The user follows the prioritized alerts and Recovery phase		Fulfilled according to the majority
DATAFAN	Prediction of the number of passengers for a specific surrounding station to redistribute the passengers at the affected station mitigation steps for each of the alerts for risk reduction and response to detection of ongoing threats.		Fulfilled according to the majority

CaESAR	Support to end-user to select the appropriate mitigation measure to respond against different event int the Turkish infrastructure.		Fulfilled according to the majority
CuriX	Evaluate how passenger flows correlate to each other, so to enhance/optimise the cascading effects analysis performed by the other S4RIS tools. Identify anomalies in passenger flows of other connected stations.		Fulfilled according to the majority

TCDD&EGO SIMULATION EXERCISE - REQUIREMENTS FOR THE RECOVERY PHASE

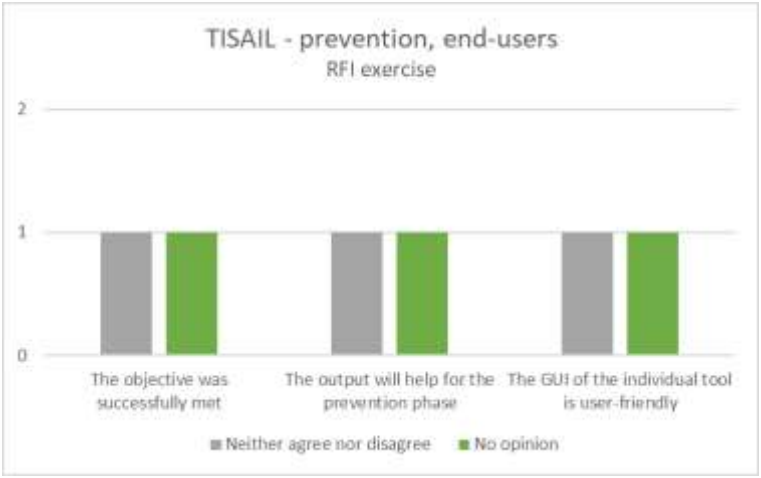
Tool	**Objective for the TCDD&EGO exercise**	**Integrated (Y/N)**	**Result of evaluation**
CAMS	Crisis Manager will be provided with time and cost needed to respond to the crisis and restore normal functioning, so that resource deployment and reaction is based on proactive actions planned. Railway operator will be aware of vulnerability and fragility of the asset after the incident, so to improve resource deployment and control financial loss in the future.		Fulfilled according to the majority

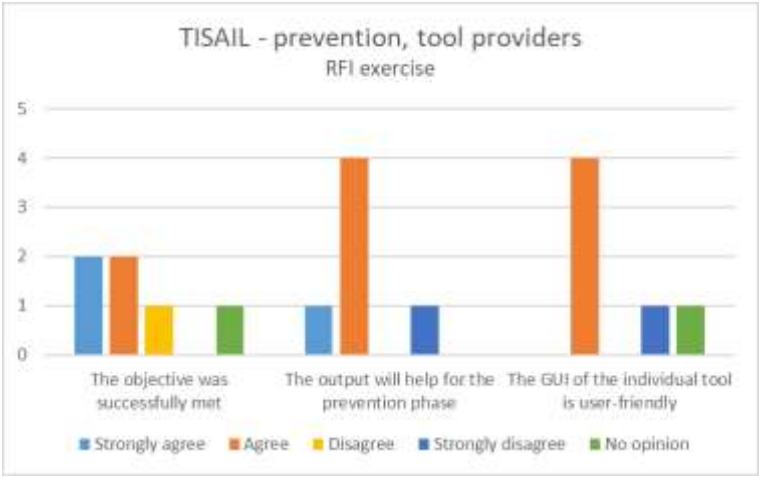
ANNEX VIII Rome (RFI) exercise schedule

DAY 1 – MAY 31 - AFTERNOON – SIMULATION EXERCISE (PART 1)		End-user audiences targeted
OPENING CEREMONY		
14:00 - 14:30	Welcome Speech by RFI Project Presentation by Coordinator (FHG) Presentation about the implementation of the Exercise (LDO)	
INDIVIDUAL TOOL DEMONSTRATIONS - FIRST SESSION		
14.30-15.30	CaESAR (Prevention + Response) DATAFAN (Prevention + Response) TSAIL (Prevention)	e.g. Maintenance planners, security managers, risk managers
15.30-15.45	**Online survey/questionnaire for the debriefing of Tools demonstrations –1st session**	All taking part in this session
15.45-16.00	Coffee break	
INDIVIDUAL TOOL DEMONSTRATIONS - SECOND SESSION		
16.00-17.00	CuriX (Detection) GANIMEDE (Detection) SC2 (Detection –Response)	e.g. Maintenance planners, security managers, risk managers
17.00-17.30	**Online survey/questionnaire for the debriefing of Tools demonstrations – 2nd session**	All taking part in this session
	End of Day #2	

DAY 2 – JUNE 1 – MORNING – SIMULATION EXERCISE (PART 2)		End-user audiences targeted
09.00-09.15	Wrap up of previous day	All taking part in this session
INDIVIDUAL TOOL DEMONSTRATIONS - THIRD SESSION		
09.15-10.15	WINGSPARK (Detection & Response) CAMS (Recovery) S4RIS Platform User interface	e.g. Maintenance planners, security managers, risk managers
10.15-10.30	**Online survey/questionnaire for the debriefing of Tools demonstrations – 3rd session**	All taking part in this session
10.30-10.45	Coffee Break	
FULL JOIN SCENARIO EXERCISE		
10.45-11.45	Joint tools Simulation Exercise (Detection and Response phases) in RFI scenario	Security managers, Control Centre personnel, Cyber security personnel
11.45-12:00	Online survey/questionnaire for the Joint simulation exercise	All taking part in this session
11.30-12.30	Open session	Security managers, risk managers, Cyber security personnel
12.30-13.00	Final remarks and Closure of the event	All taking part in this session
	End of Day #3	

RFI PREVENTION PHASE QUESTIONNAIRE 1

TISAIL	**Objective:** **TISAIL** will focus on providing situational awareness about cyber-threats that might have an undesirable impact on the RFI infrastructure. In particular, the tool will provide intelligence about the following cases: • Vulnerabilities in CCTV and DVRs systems. Video surveillance systems are crucial for physical security teams and it's very important to be up to date of disclosed vulnerabilities that can affect these systems. • Malware variants targeting CCTV Cameras and DVRs systems. There are some malware families such as Mirai or BotenaGo that have been targeting during the last years IoT devices including CCTV cameras. TISAIL will include some IoCs (Indicators of Compromise) as well as some detection mechanism. • Current active malware campaigns that might be a threat for any industry such as active ransomware campaigns.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Of course threat analysis is a relevant and necessary thing and the objectives of TISAIL surely look promising. But I must say that on the basis of the presentation it is very difficult for me to assess the added value of this tool for us as an end-user.

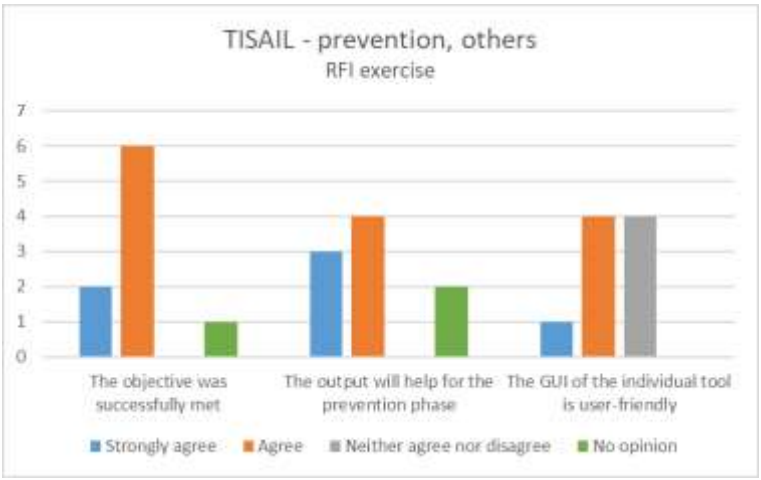


What is the added value of this tool to the prevention phase that you know from your current daily work?

- To detect vulnerabilities in CCTV and DVR systems - but I cannot assess the added value since I am not working with such systems every day and therefore, I do not know what is already there
- This presentation and its study about prior railway incidents does not apply to the S4R proposal project and they are using an internal attack that was released to public media outlets as a professional cyber attack.

How could this tool be improved in the context of this scenario?

- The GUI seems to be very complex for a user who is not using the tool every day. Maybe to reduce the complexity here a bit.
- I believe the project proposal should be reviewed more thoroughly by TISAIL for a better integration of CAESAR and DATAFAN.
- more actively pushing events to the user
- if there was more data available from the end-users, the tool could be more customized to the specific end-user

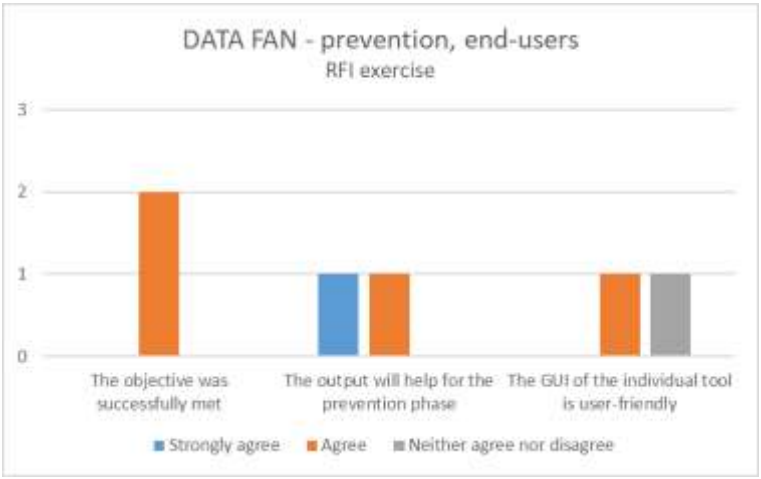


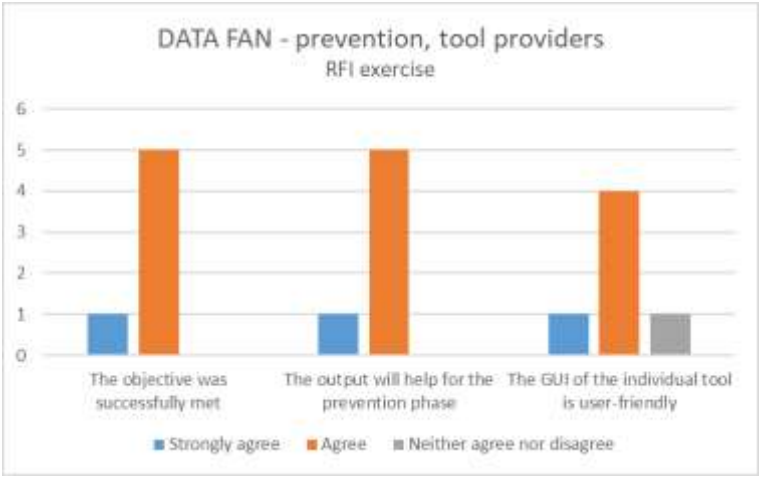
What is the added value of this tool to the prevention phase that you know from your current daily work?

- Any information on potential threats must be of value to metro/rail security decision making.

How could this tool be improved in the context of this scenario?

- By highlighting the rail/metro systems at risk from the identified threats and the potential risks to commercial and operational safety. safety

DATAFAN	**Objective:** **Providing information on the expected number of passengers** for a target station (here: Roma Termini), a set of surrounding stations, and for a specific time or event (e.g. during Christmas festivity, rush hour or a soccer game). This can be used as a basis for what-if scenarios (i.e. prevention) where the target station's operability is compromised (e.g. closure of a station) or for an informed responds to an event in progress. Ultimately, the tool supports the end-user in redirecting passenger flows.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Data based decision making which will lead to more accurate action and measures and wil make the acceptability much higher.

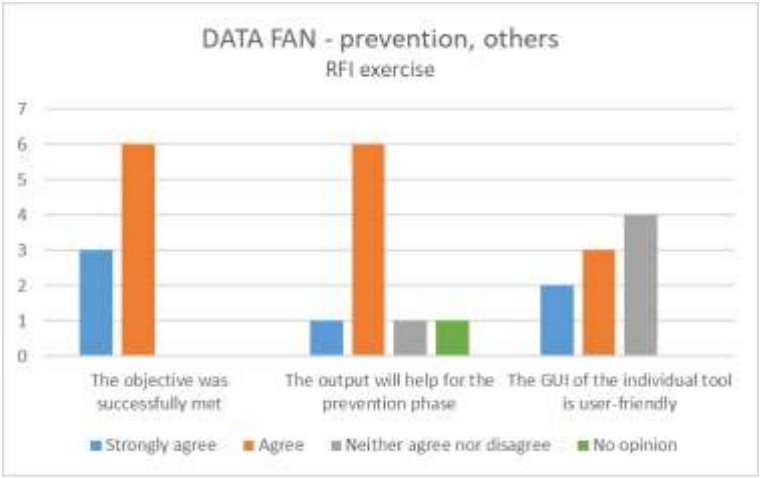


What is the added value of this tool to the prevention phase that you know from your current daily work?

- To get information on the expected passengers, the capacities and the free capacities of the surrounding stations and also information on the interconnected infrastructures
- There is the possibility of highlighting the out of service stations either in simulation or in real life situations.

How could this tool be improved in the context of this scenario?

- To insert more data and options for the what-if-scenarios, to design the GUI in a more intuitive way
- By utilizing a historical database of similar incidents to produce accurate time history data rather than using general data such as Google maps, the time history data is made more accurate.
- validation of expected results with the current scenario
- make it more integrated into the end-user system, and more automatic

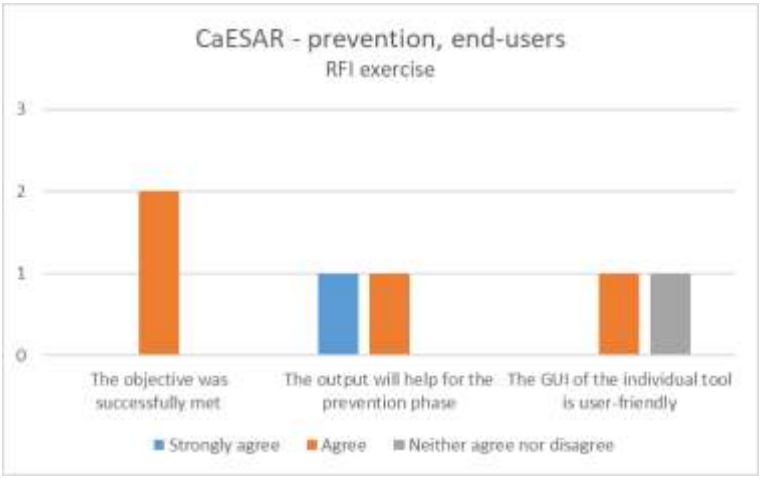


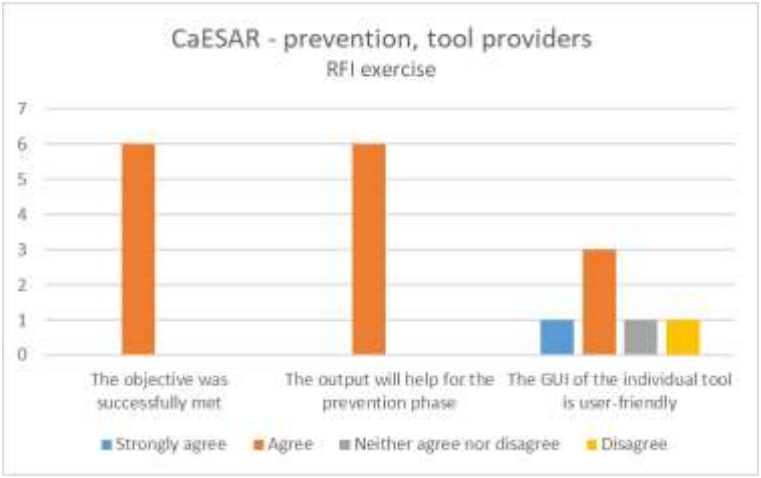
What is the added value of this tool to the prevention phase that you know from your current daily work?

- The ability to study different simulations can be used to prepare for action.
- Of help both to incident response plan preparers when considering potential resource needs/also to real time incident commanders in evaluation of optimum response to an incident. Potential use for overall rail/metro system designers. scenario.assess

How could this tool be improved in the context of this scenario?

- It was not clear whether the input data was for crowded events or "just" times series in general? If in general, then not reflecting scenario (crowded event). How to deal with? User must be clear whether data inputted for crowded / not crowded event? Or both types of data can be inputted and GUI must provide option for "normal" or "crowded" event. More time to look at in detail (but accept not suitable/possible for SE demo considering timeframe of SE demo) - booth at future event?
- Identification of the optimum solution at a given point in time?

CaESAR	**Objective:** • Identification of critical stations/components based on a grid representation of the metro network • Stochastic simulation of various what-if scenarios to identify critical combinations of threats and impacted stations/components
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Data based decision making which will make acceptability much higher

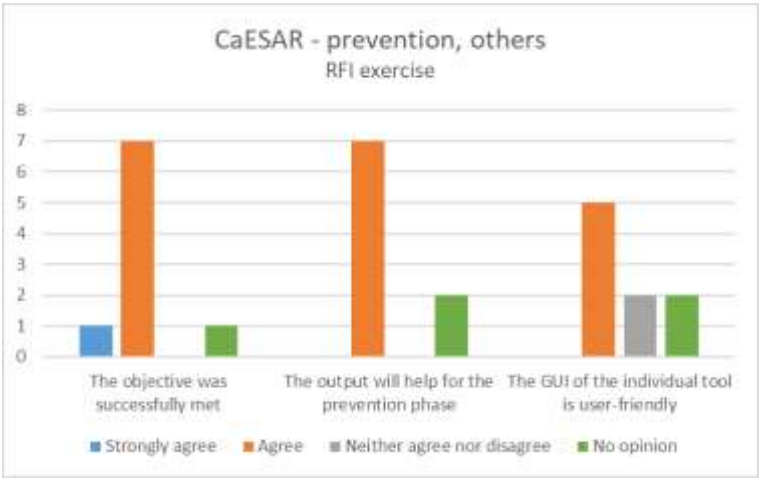


What is the added value of this tool to the prevention phase that you know from your current daily work?

- To identify critical nodes in a network
- Having the ability to gather node data as specific input is extremely helpful.

How could this tool be improved in the context of this scenario?

- To insert more options and grids - not only those for the prepared networks
- The integration of results and data from the timeline, along with a justification, with the other tools.
- Detects anomalies and create relevant alerts
- Interconnection with other tools could be increased



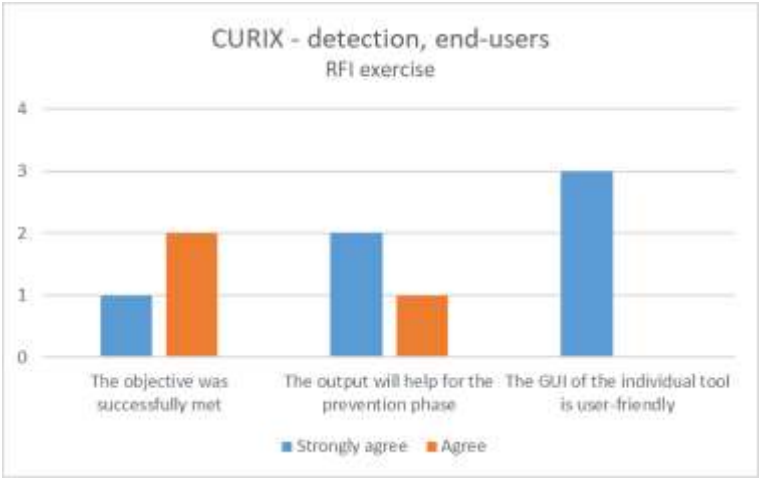
What is the added value of this tool to the prevention phase that you know from your current daily work?

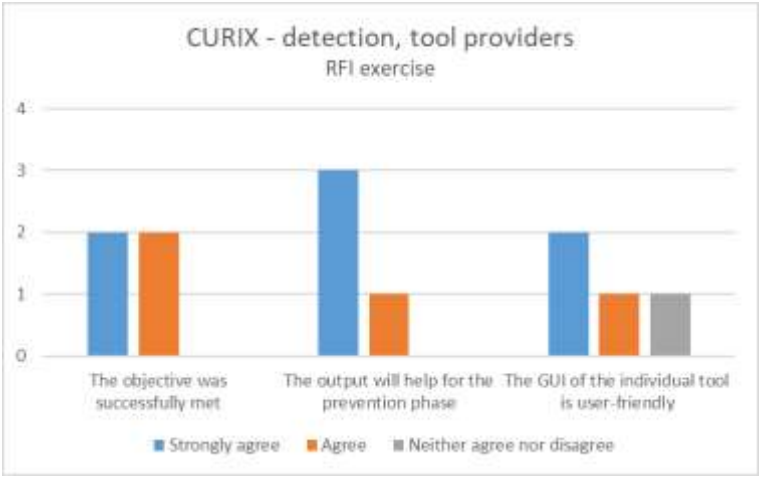
- Provides incident response planners with useful information preparing response plans.

How could this tool be improved in the context of this scenario?

- Not sure that it could be without comparing the outputs with those of a real event involving the same location.

RFI DETECTION PHASE QUESTIONNAIRES 2, 3 AND 4

CURIX	**Objective:** Crisis Manager will be alerted when deviations from normal behaviour (anomalies) or potentially upcoming disruptions of technical systems (IT and OT) from their monitoring data are detected. The crisis manager can check metrics and which technical devices are responsible for causing the major change in the system behaviour.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • help to detect anomalies • Automated and real time check of the health of the system and its components How could this tool be improved in the context of this scenario? • I might have to take a closer look but is it visible in the GUI which component in the system "fails"?

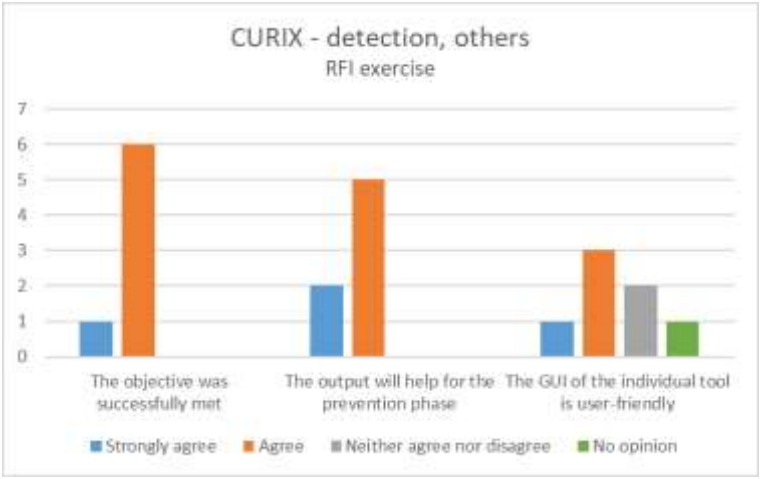


What is the added value of this tool to the prevention phase that you know from your current daily work?

- The detection of abnormal behavior - but since I did not use such tool every day I am not aware of what is already there
- Enhance the resilience of the end-user requirements by detecting unknown threats early on.
- Cyber risk assessment

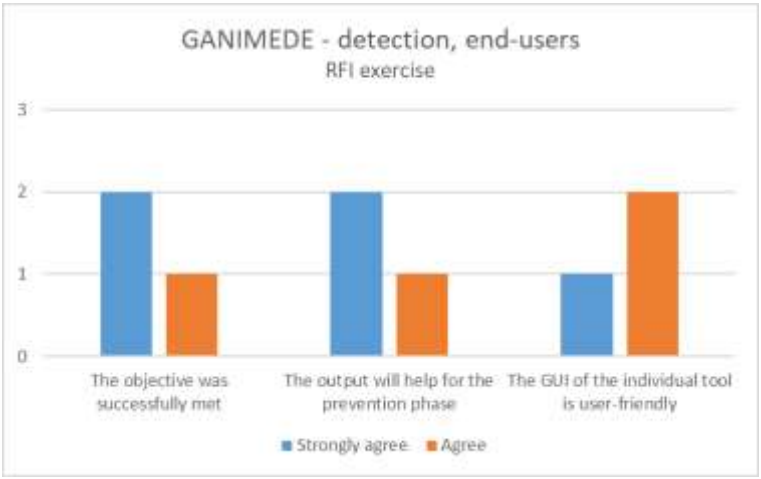
How could this tool be improved in the context of this scenario?

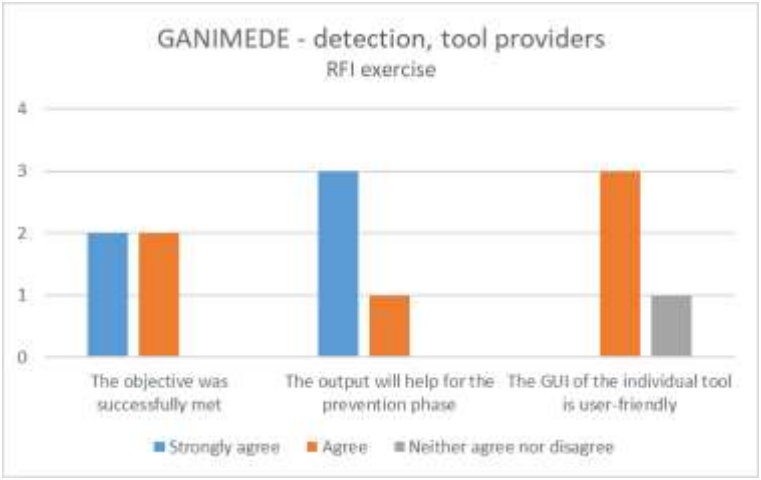
- The GUI seems to be very complex, especially for users who are not using the tool every day. Maybe the complexity can be reduced



What is the added value of this tool to the prevention phase that you know from your current daily work?

- Overview and control of systems and/or sensors.

GANIMEDE	**Objective:** The objectives will be: 1) the analysis of an audio stream searching for relevant pattern in the context of safety and security (a shot in this case); 2) the detection of objects and people in each frame and their movement to determine if the object is candidate for abandon; 3) the ability of recognizing people based on the clothes they are wearing.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • early detection • Real time detection and information about the incident and the location in the station where it occurred. So it is clear what immediate action (and where) has to be taken. How could this tool be improved in the context of this scenario? • ok for this scenario

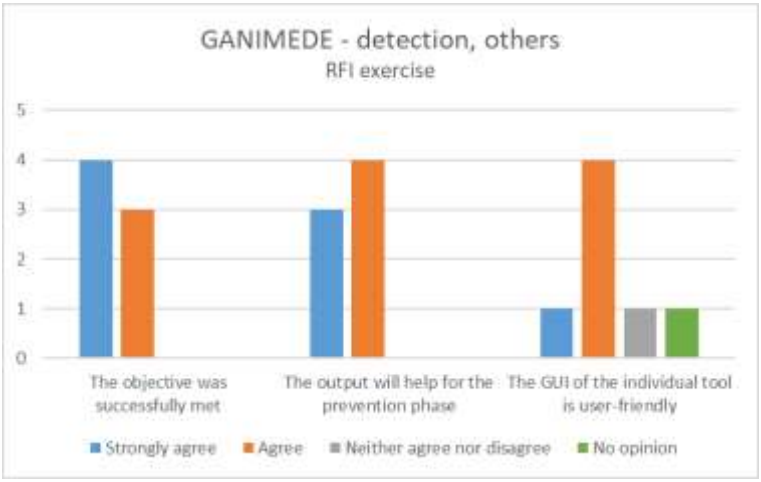


What is the added value of this tool to the prevention phase that you know from your current daily work?

- The detection e.g. of suspicious people - but since I am not using the tools in my daily work I am not aware ot what is already there.
- Improved features include audio detection and abandoned items, as well as powerful prices.
- visual anomalies detection

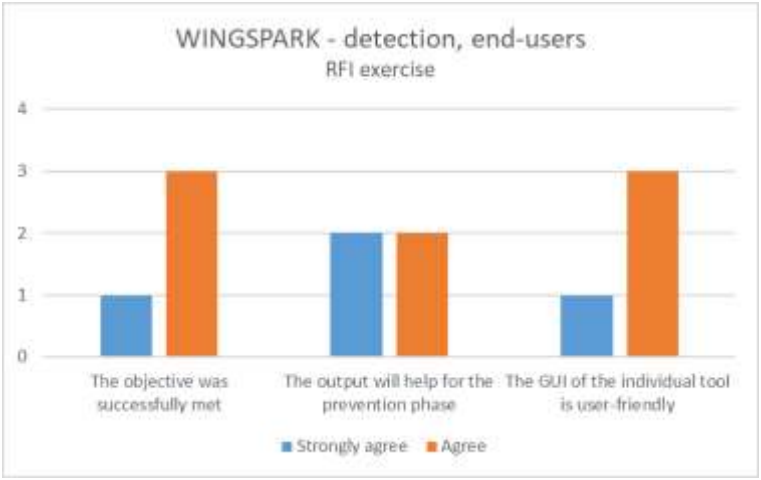
How could this tool be improved in the context of this scenario?

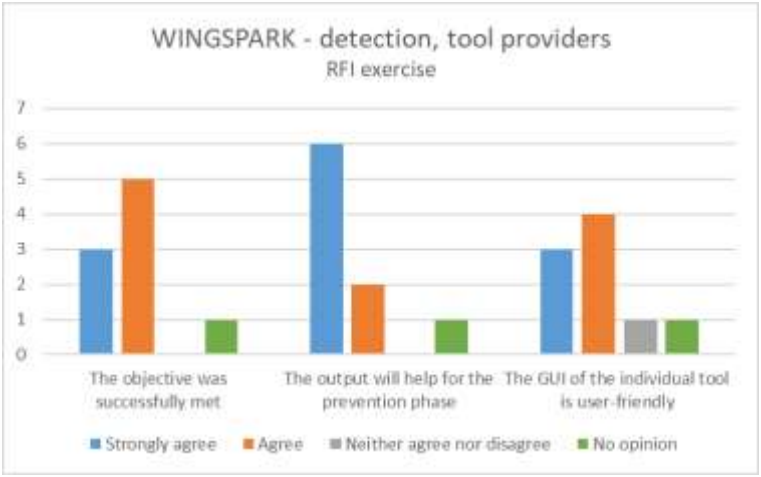
- It seems that the complexity of the GUI of the tools is quite high, especially for user who are not using the tools every day. Maybe the complexity can be reduced a bit..
- Using historical data from end-user companies and organizations, rather than using public sources such as Google Maps, they will be able to obtain a more accurate result.
- connection of SC2 to mobile responders



What is the added value of this tool to the prevention phase that you know from your current daily work?

- Detection of suspicious things and behavior and making guards or similar aware of it.

WINGSPARK	**Objective:** The objective of WINGSPARK is to forward the alerts to RAM2 in case the specified thresholds have been exceeded and provide evacuation guidelines to ease the situation.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • early detection • The added value of the tools lies mainly in the crowd concentration detection part. The fact that this process is automated is a step up from our current practice in which this is being done by "people behind a tv screen" • Getting the alarms immediately and being able to check and dismiss if necessary How could this tool be improved in the context of this scenario? • I'm curious how the evacuation application works. It looks like it is being done by an app which can be used by people who are in the station. I wonder if any research has been done on the use of such an app when people are panicking • More attractive output for operator even if already improved

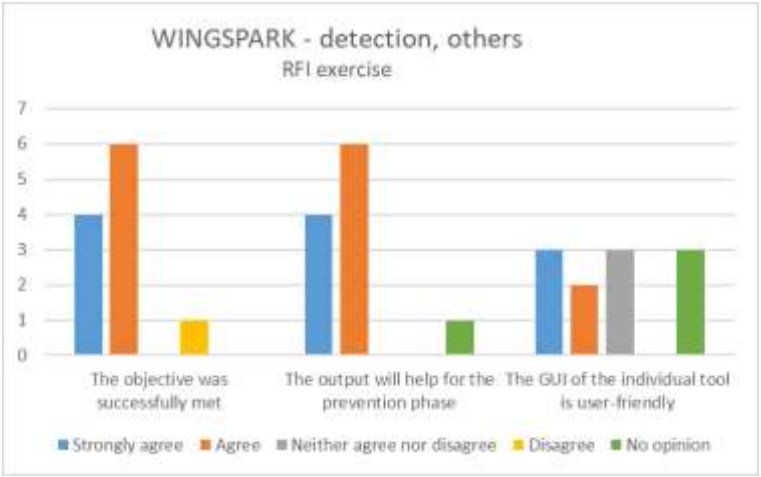


What is the added value of this tool to the prevention phase that you know from your current daily work?

- Flexibility in Anomaly Detection
- Crowd estimation, anomalies
- Mixing local data with incident data gets better WINGSPARK results than previous simulations.
- To provide early identification of an event and give useful metadata and insights regarding the event
- Scalability, interpretability and early detection
- Alerts will be sent and forwarded to S4RIS if specific thresholds are exceeded.

How could this tool be improved in the context of this scenario?

- More automatization
- An important monitoring tool to get insight from
- Apply to more exercises.
- In order for the tool to be more accurate, I think it should be integrated with other tools in the detection phase.
- enrich the statistics provided, e.g. motion flows of the people
- Additional stations or train based on realistic data
- The GUI seems to be very complex especially for users who are not using the tool every day. Maybe the complexity can be reduced a bit.



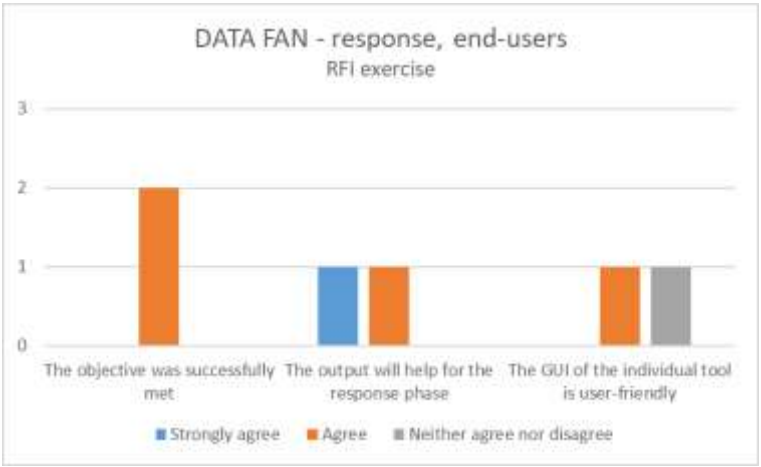
What is the added value of this tool to the prevention phase that you know from your current daily work?

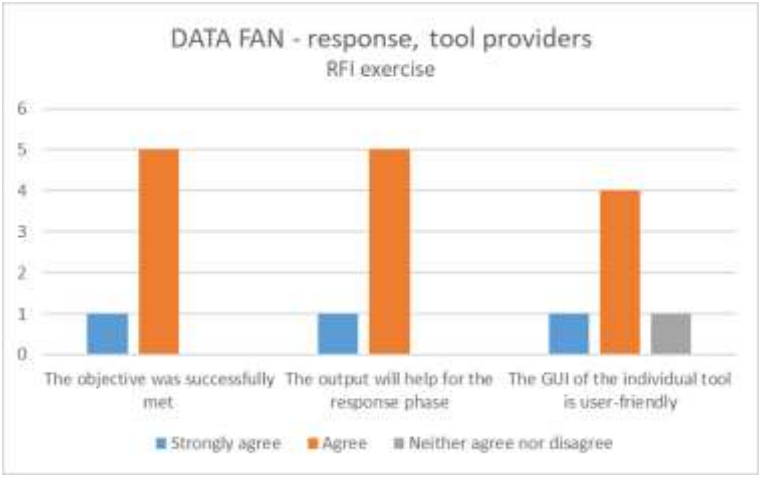
- The end-user is notified live for events anomalies in the speed of the train or overcrowded situations from cameras
- Alarms if people are crowding in a cctv area and also if train speeds are too low.
- Early detection is the most important

How could this tool be improved in the context of this scenario?

- Should adapt better to physical attacks
- Disagree under objective as for the specific scenario, did not see evacuation guidelines presented. As with some other tools, it would be good to have more time to look at the tool and ask more details questions / play with it (with WINGS support) (e.g. with use of booth) at a future SE or event? In the GUI/presentation it was not so clear what the smaller red dots (smaller anomalies...?) meant compared to the main blue line

RFI RESPONSE PHASE
QUESTIONNAIRES 1, 3 AND 4

DATAFAN	**Objective:** **Providing information on the expected number of passengers** for a target station (here: Roma Termini), a set of surrounding stations, and for a specific time or event (e.g. during Christmas festivity, rush hour or a soccer game). This can be used as a basis for what-if scenarios (i.e. prevention) where the target station's operability is compromised (e.g. closure of a station) or for an informed responds to an event in progress. Ultimately, the tool supports the end-user in redirecting passenger flows.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Data based decision making which will lead to more accurate action and measures and will make the acceptability much higher. How could this tool be improved in the context of this scenario?

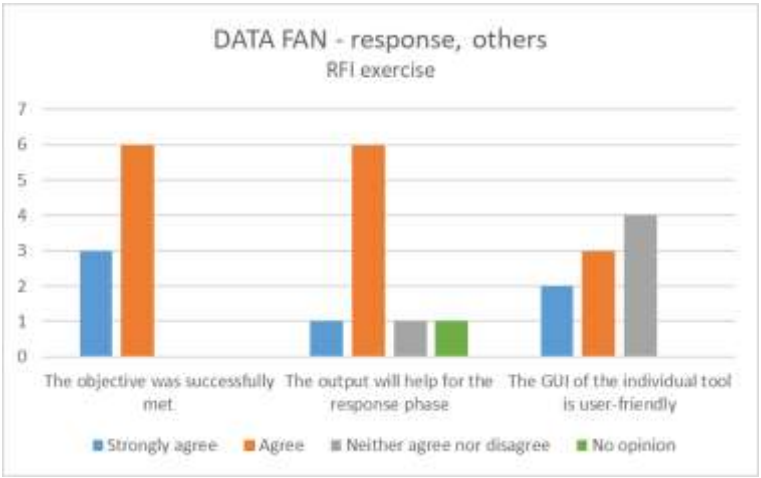


What is the added value of this tool to the prevention phase that you know from your current daily work?

- To get information on the expected passengers, the capacities and the free capacities of the surrounding stations and also information on the interconnected infrastructures
- There is the possibility of highlighting the out of service stations either in simulation or in real life situations.

How could this tool be improved in the context of this scenario?

- To insert more data and options for the what-if-scenarios, to design the GUI in a more intuitive way
- By utilizing a historical database of similar incidents to produce accurate time history data rather than using general data such as Google maps, the time history data is made more accurate.
- validation of expected results with the current scenario
- make it more integrated into the end-user system, and more automatic

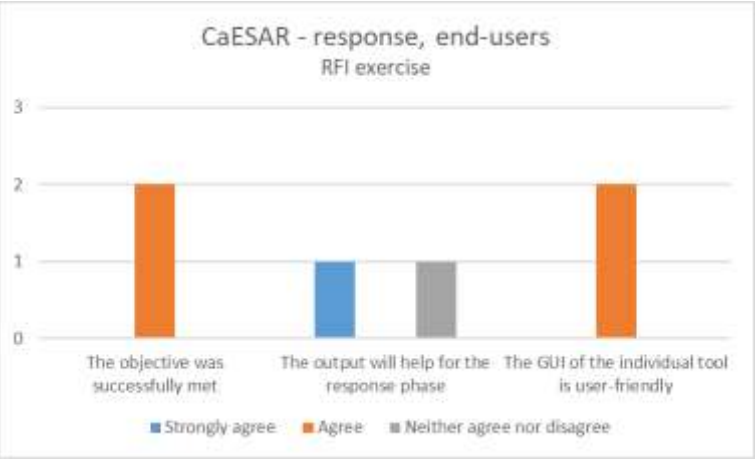


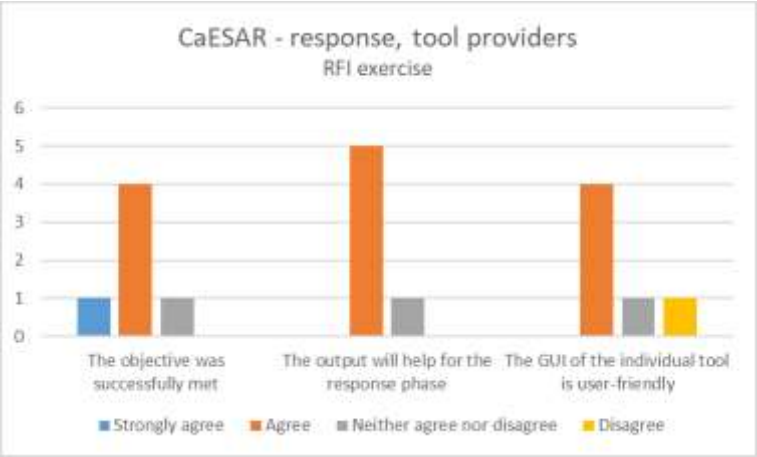
What is the added value of this tool to the prevention phase that you know from your current daily work?

- The ability to study different simulations can be used to prepare for action.
- Of help both to incident response plan preparers when considering potential resource needs/also to real time incident commanders in evaluation of optimum response to an incident. Potential use for overall rail/metro system designers. scenario.assess

How could this tool be improved in the context of this scenario?

- It was not clear whether the input data was for crowded events or "just" times series in general? If in general, then not reflecting scenario (crowded event). How to deal with? User must be clear whether data inputted for crowded / not crowded event? Or both types of data can be inputted and GUI must provide option for "normal" or "crowded" event. More time to look at in detail (but accept not suitable/possible for SE demo considering timeframe of SE demo) - booth at future event?
- Identification of the optimum solution at a given point in time?

CaESAR	**Objective:** • Quantified resilience assessment based on performance-time curves for the threats of the exercise and estimation of resilience indicators • Comparison of certain mitigation measures (as defined in the exercise) to reduce the impact of the threats of the exercise • Visualization of the model, the impact propagation based on different concepts (connectivity based, agent-based) and the resilience assessment
	What is the added value of this tool to the prevention phase that you know from your current daily work? • Data based decision making which will make acceptability of measures to be taken much higher. Expected objective impact of measures is an important factor. Currently this is done by expert judgement. How could this tool be improved in the context of this scenario? • I'm not certain yet of the added value of a gif which represents the impact on the system. Although it looks very good, in the end decisions are made on the basis of numbers and data.

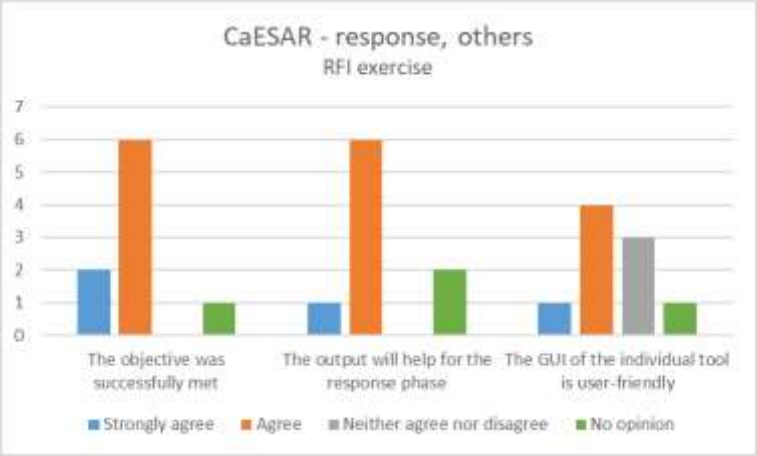


What is the added value of this tool to the prevention phase that you know from your current daily work?

- To identify critical nodes in a network
- The ability to mix Node files with Arc files and configuration files in unique input fields.

How could this tool be improved in the context of this scenario?

- To insert more options and grids - not only those for the prepared networks; information on former scenarios and the resilience actions then
- This would necessitate adding up two similar historical data sets, each with a similar set of end-users in order to achieve more accuracy.
- Detects anomalies and create relevant alerts
- reduce abstraction level --> being more concrete in actions and results

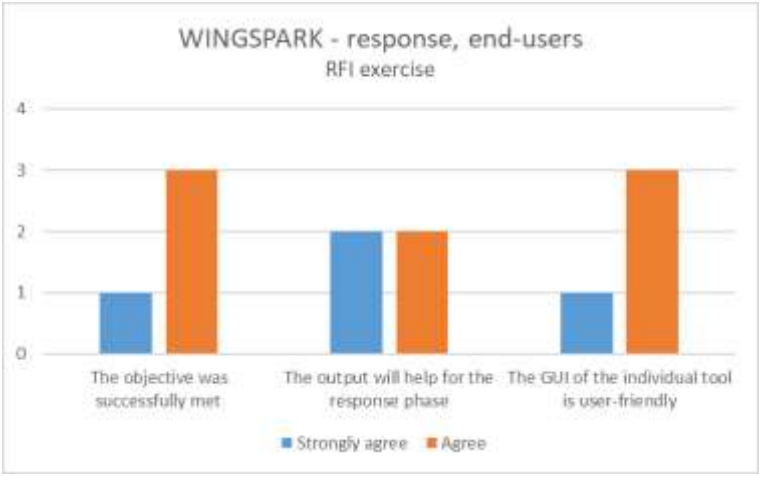


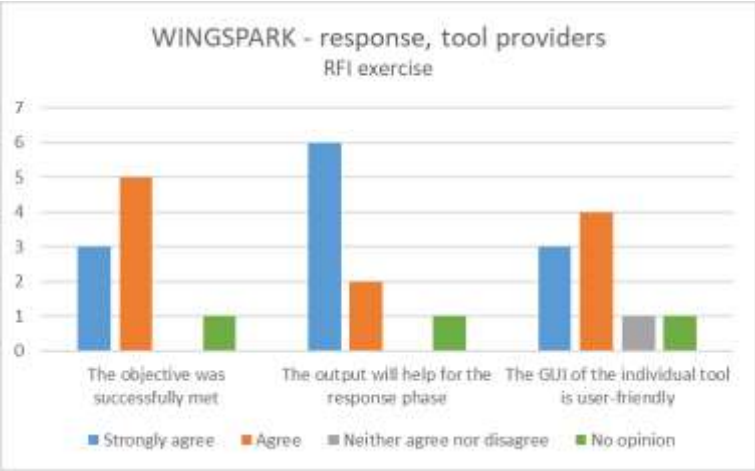
What is the added value of this tool to the prevention phase that you know from your current daily work?

- Would help the overall incident commander's response decision making when evaluating all of the potential response options.

How could this tool be improved in the context of this scenario?

- More time to look at in detail (but accept not suitable/possible for SE demo considering timeframe of SE demo) - booth at future event?

WINGSPARK	**Objective:** The objective of WINGSPARK is to forward the alerts to RAM2 in case the specified thresholds have been exceeded and provide evacuation guidelines to ease the situation.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • early detection • The added value of the tools lies mainly in the crowd concentration detection part. The fact that this process is automated is a step up from our current practice in which this is being done by "people behind a tv screen" • Getting the alarms immediately and being able to check and dismiss if necessary How could this tool be improved in the context of this scenario? • I'm curious how the evacuation application works. It looks like it is being done by an app which can be used by people who are in the station. I wonder if any research has been done on the use of such an app when people are panicking • More attractive output for operator even if already improved

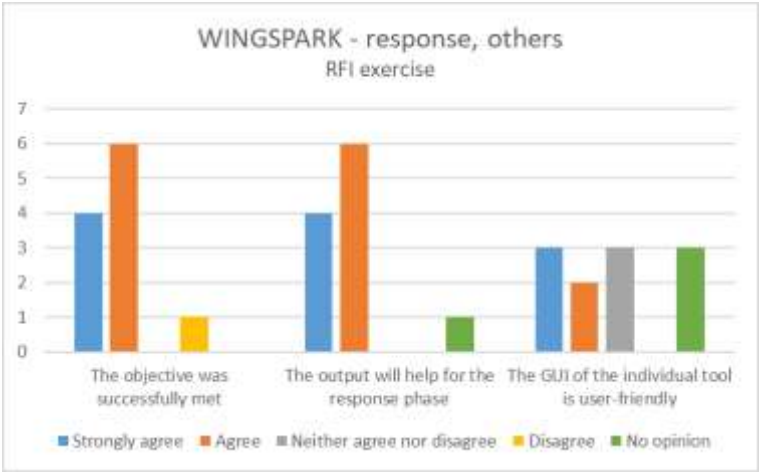


What is the added value of this tool to the prevention phase that you know from your current daily work?

- Flexibility in Anomaly Detection
- Crowd estimation, anomalies
- Mixing local data with incident data gets better WINGSPARK results than previous simulations.
- To provide early identification of an event and give useful metadata and insights regarding the event
- Scalability, interpretability and early detection
- Alerts will be sent and forwarded to S4RIS if specific thresholds are exceeded.

How could this tool be improved in the context of this scenario?

- More automatization
- An important monitoring tool to get insight from
- Apply to more exercises.
- In order for the tool to be more accurate, I think it should be integrated with other tools in the detection phase.
- enrich the statistics provided, e.g. motion flows of the people
- Additional stations or train based on realistic data
- The GUI seems to be very complex especially for users who are not using the tool every day. Maybe the complexity can be reduced a bit.



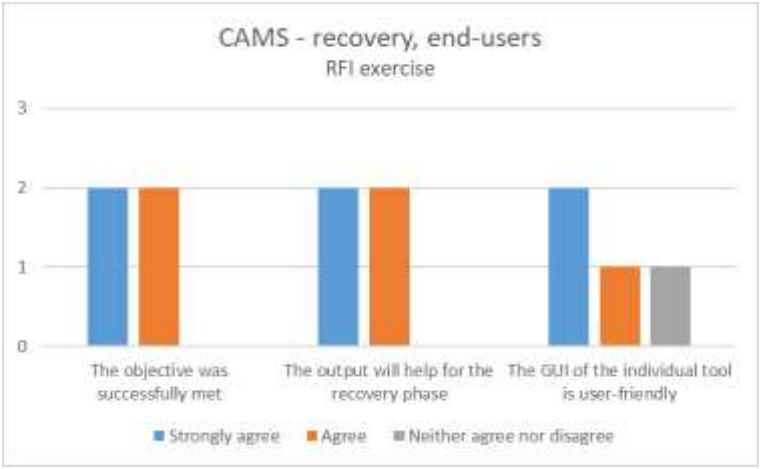
What is the added value of this tool to the prevention phase that you know from your current daily work?

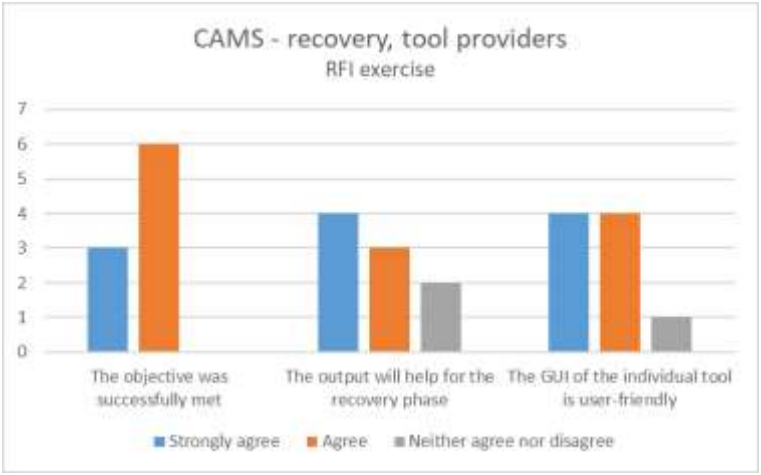
- The end-user is notified live for events anomalies in the speed of the train or overcrowded situations from cameras
- Alarms if people are crowding in a cctv area and also if train speeds are too low.
- Early detection is the most important

How could this tool be improved in the context of this scenario?

- Should adapt better to physical attacks
- Disagree under objective as for the specific scenario, did not see evacuation guidelines presented. As with some other tools, it would be good to have more time to look at the tool and ask more details questions / play with it (with WINGS support) (e.g. with use of booth) at a future SE or event? In the GUI/presentation it was not so clear what the smaller red dots (smaller anomalies...?) meant compared to the main blue line

RFI RECOVERY PHASE QUESTIONNAIRE 3

CAMS	**Objective:** CAMS will provide accurate recovery cost for assets involved in a sudden event through the assessment of final assets damage. The final damage is assessed using the initial condition (before incident) and the impact measure of the specific incident on the asset. The end-user is then provided with a budget needed to restore the service.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • prediction of recovery costs and normal deterioration on the basis of data is very useful. At this moment this is mainly being done by expert judgement (for instance: "the average lifespan of an bridge is 80-90 years") • All the economic study provided to allow a Quick decision How could this tool be improved in the context of this scenario? • Already a big improvement. Maybe more creative in the output with pictures of the affected equipment

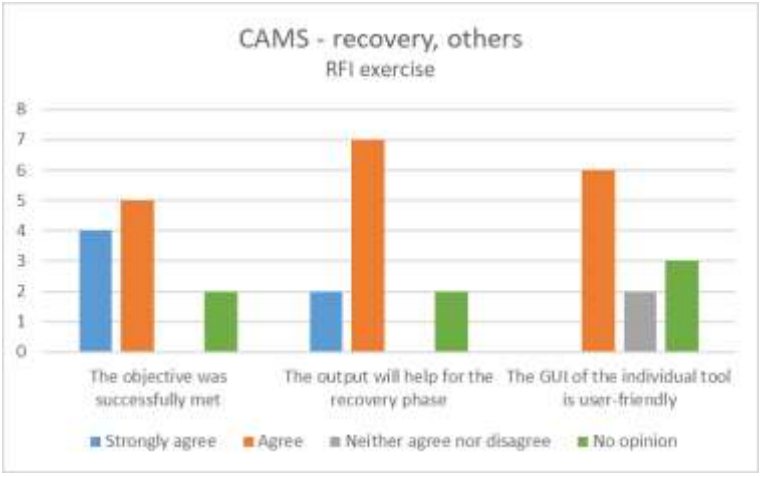


What is the added value of this tool to the prevention phase that you know from your current daily work?

- total cost and time for recovery can be estimated and decision makers can make the best decision for recovery. it also can help to evaluate what-if scenarios.
- All degradation models included, no need to calculate those things manually
- Cost estimates.
- Adding more features and accuracy to CAMS output for ROME SE based on simulations of Ankara and Madrid experiences.
- Manipulation of several sources
- A recovery cost estimation in the case of a sudden event

How could this tool be improved in the context of this scenario?

- integration to other tools so the data automatically entered to CAMS can be a big improvement
- more graphs to be shown in the demo / gui
- Post crisis analysis
- Provide more results.
- Integration of recovery results from other participants along with historical data of similar incidents focusing on the cost of damaged assets and recovery time for each component.
- The GUI seems to be a bit complex especially for users who are not using the tool every day. Maybe the complexity can be reduced a bit.



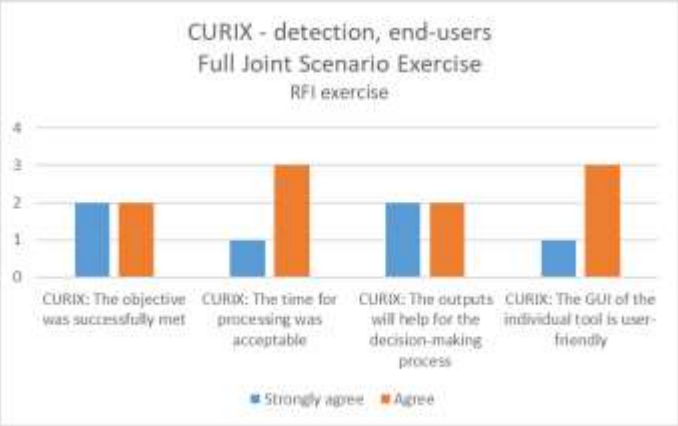
What is the added value of this tool to the prevention phase that you know from your current daily work?

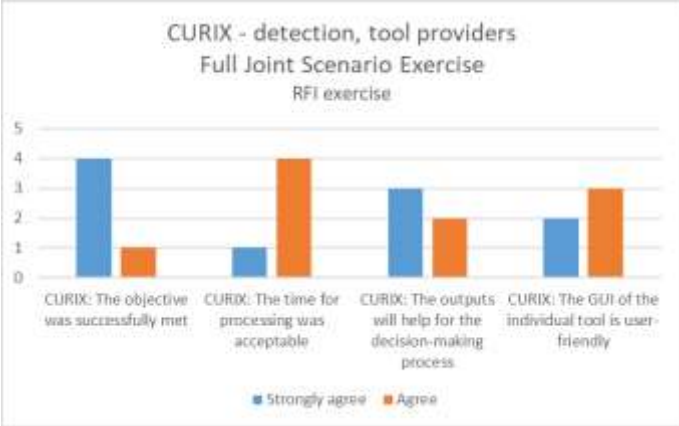
- Estimate time scale and cost for repairing facilities after an accident or incident.
- Quantification and high disaggregation

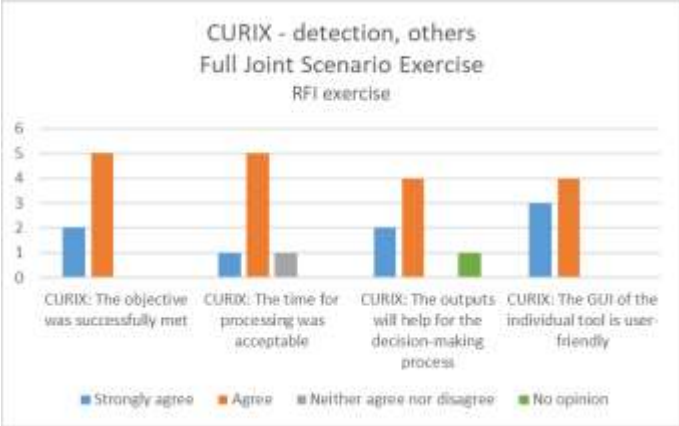
How could this tool be improved in the context of this scenario?

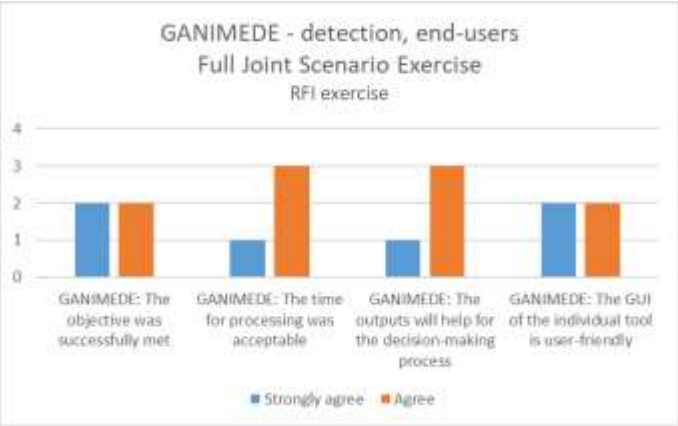
- More details about the damaged assets

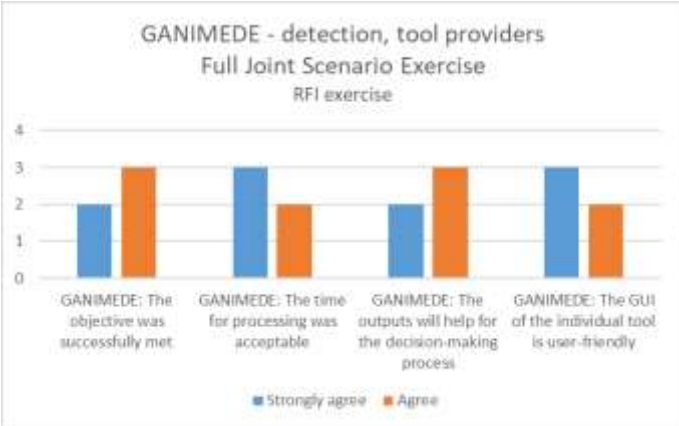
RFI FULL JOINT SCENARIO EXERCISE QUESTIONNAIRE 4

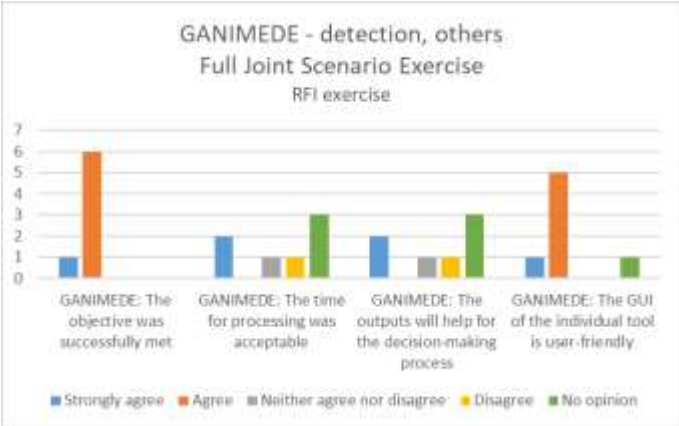

CURIX - detection, end-users
Full Joint Scenario Exercise
RFI exercise
CURIX: The objective was successfully met
CURIX: The time for processing was acceptable
CURIX: The outputs will help for the decision-making process
CURIX: The GUI of the individual tool is user-friendly
Strongly agree
Agree

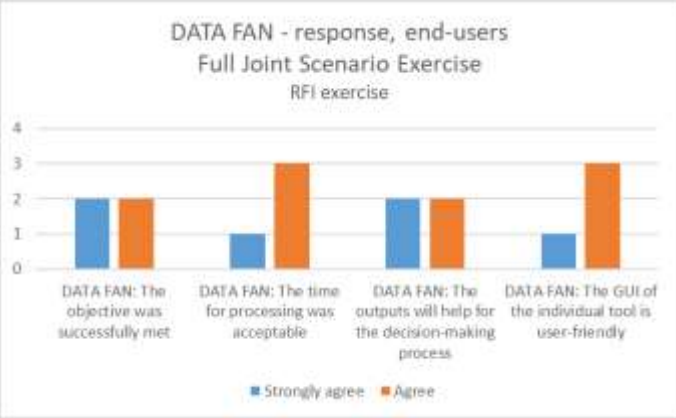

CURIX - detection, tool providers
Full Joint Scenario Exercise
RFI exercise
CURIX: The objective was successfully met
CURIX: The time for processing was acceptable
CURIX: The outputs will help for the decision-making process
CURIX: The GUI of the individual tool is user-friendly
Strongly agree
Agree

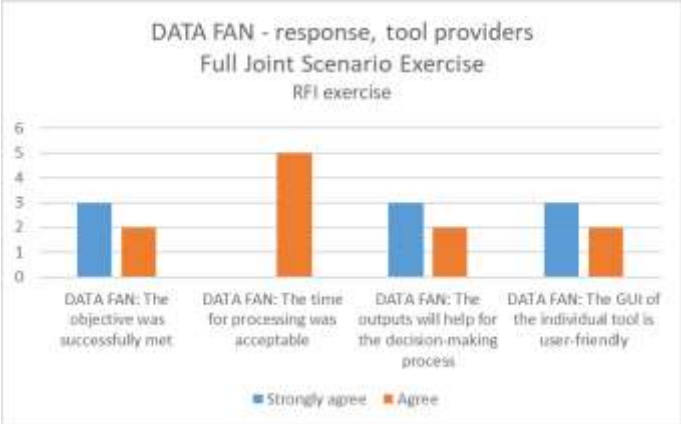

CURIX - detection, others
Full Joint Scenario Exercise
RFI exercise
CURIX: The objective was successfully met
CURIX: The time for processing was acceptable
CURIX: The outputs will help for the decision-making process
CURIX: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

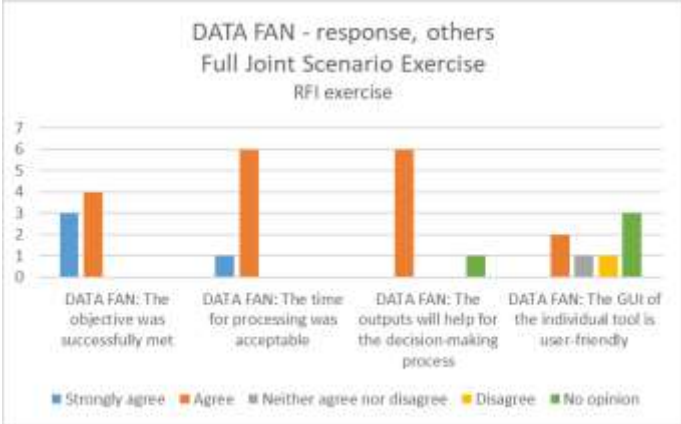

GANIMEDE - detection, end-users
Full Joint Scenario Exercise
RFI exercise
GANIMEDE: The objective was successfully met
GANIMEDE: The time for processing was acceptable
GANIMEDE: The outputs will help for the decision-making process
GANIMEDE: The GUI of the individual tool is user-friendly
Strongly agree
Agree

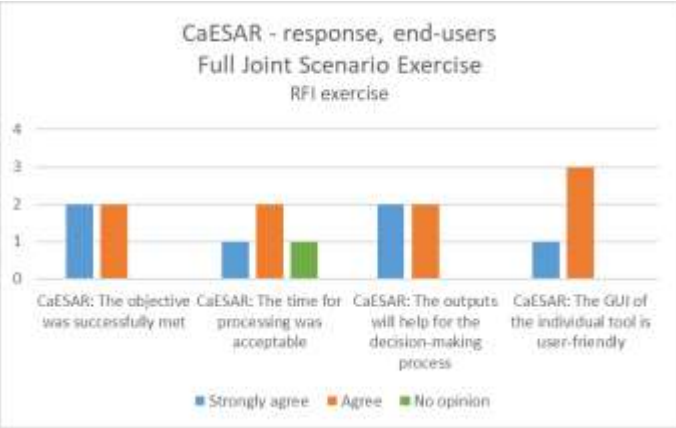

GANIMEDE - detection, tool providers
Full Joint Scenario Exercise
RFI exercise
GANIMEDE: The objective was successfully met
GANIMEDE: The time for processing was acceptable
GANIMEDE: The outputs will help for the decision-making process
GANIMEDE: The GUI of the individual tool is user-friendly
Strongly agree
Agree

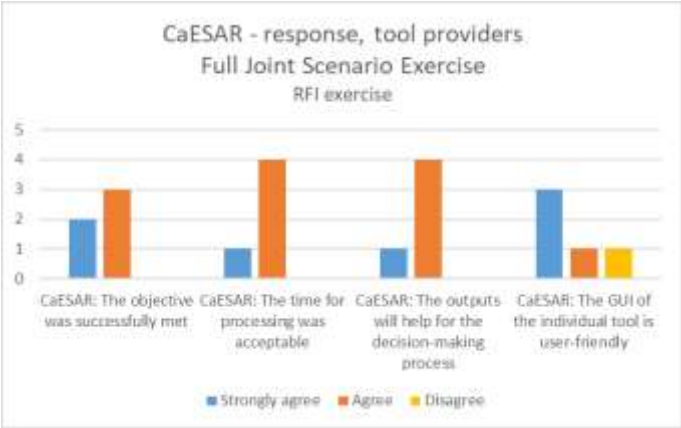

GANIMEDE - detection, others
Full Joint Scenario Exercise
RFI exercise
GANIMEDE: The objective was successfully met
GANIMEDE: The time for processing was acceptable
GANIMEDE: The outputs will help for the decision-making process
GANIMEDE: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
Disagree
No opinion

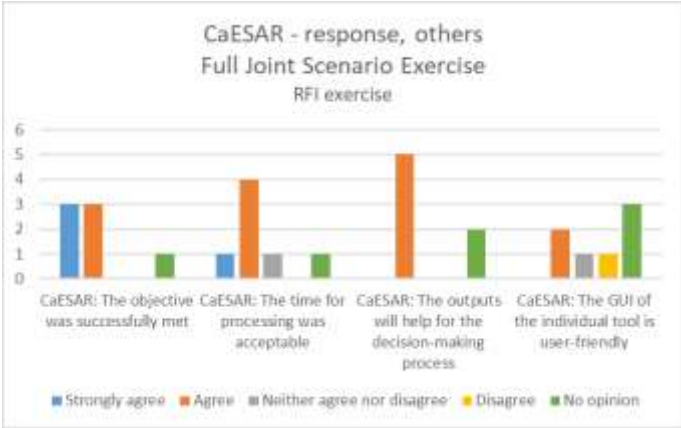

DATA FAN - response, end-users
Full Joint Scenario Exercise
RFI exercise
DATA FAN: The objective was successfully met
DATA FAN: The time for processing was acceptable
DATA FAN: The outputs will help for the decision-making process
DATA FAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree

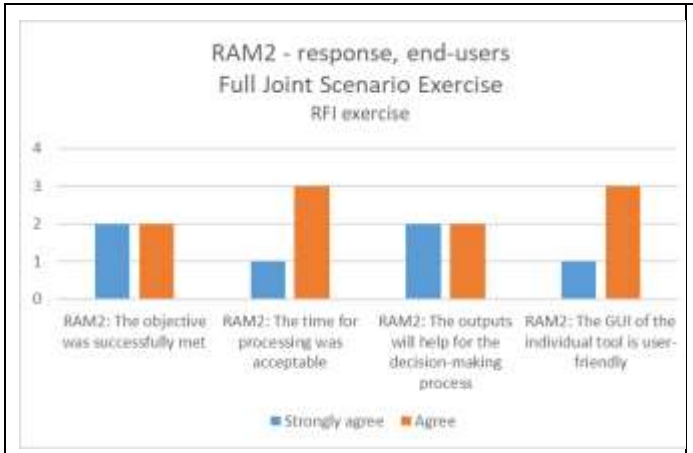

DATA FAN - response, tool providers
Full Joint Scenario Exercise
RFI exercise
DATA FAN: The objective was successfully met
DATA FAN: The time for processing was acceptable
DATA FAN: The outputs will help for the decision-making process
DATA FAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree

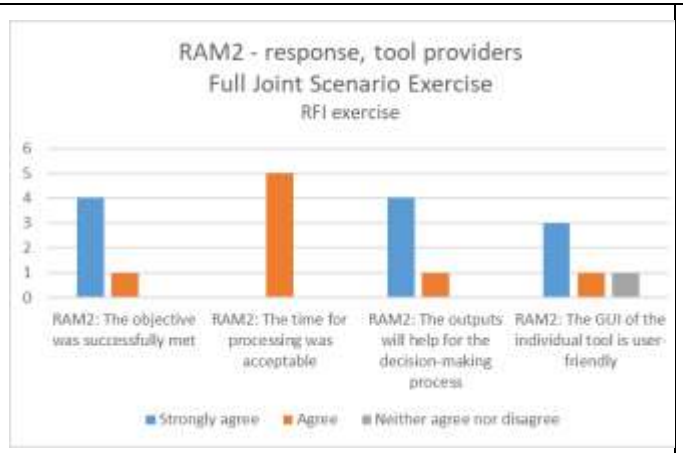

DATA FAN - response, others
Full Joint Scenario Exercise
RFI exercise
DATA FAN: The objective was successfully met
DATA FAN: The time for processing was acceptable
DATA FAN: The outputs will help for the decision-making process
DATA FAN: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
Disagree
No opinion

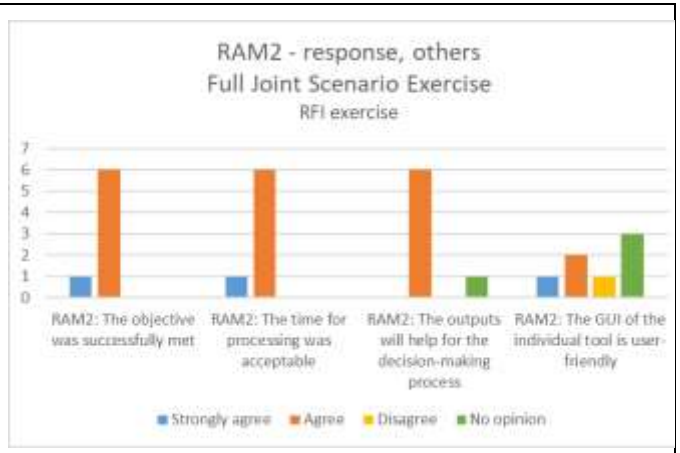

CaESAR - response, end-users
Full Joint Scenario Exercise
RFI exercise
CaESAR: The objective was successfully met
CaESAR: The time for processing was acceptable
CaESAR: The outputs will help for the decision-making process
CaESAR: The GUI of the individual tool is user-friendly
Strongly agree
Agree
No opinion

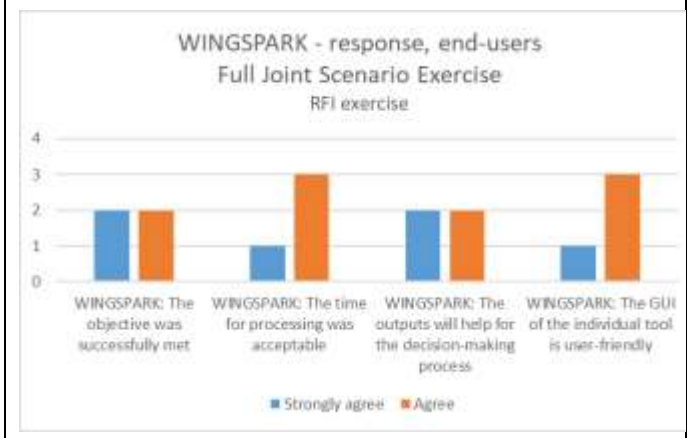

CaESAR - response, tool providers
Full Joint Scenario Exercise
RFI exercise
CaESAR: The objective was successfully met
CaESAR: The time for processing was acceptable
CaESAR: The outputs will help for the decision-making process
CaESAR: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Disagree

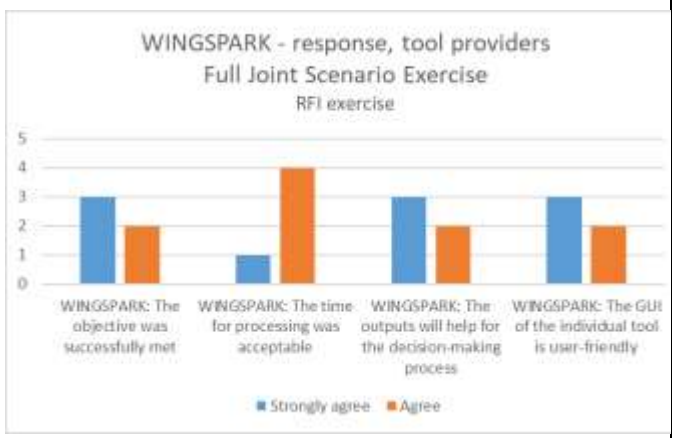

CaESAR - response, others
Full Joint Scenario Exercise
RFI exercise
CaESAR: The objective was successfully met
CaESAR: The time for processing was acceptable
CaESAR: The outputs will help for the decision-making process
CaESAR: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
Disagree
No opinion

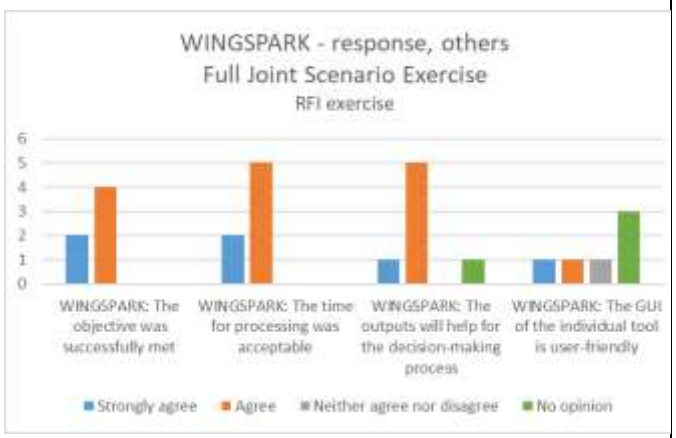

RAM2 - response, end-users
Full Joint Scenario Exercise
RFI exercise
RAM2: The objective was successfully met
RAM2: The time for processing was acceptable
RAM2: The outputs will help for the decision-making process
RAM2: The GUI of the individual tool is user-friendly
Strongly agree
Agree


RAM2 - response, tool providers
Full Joint Scenario Exercise
RFI exercise
RAM2: The objective was successfully met
RAM2: The time for processing was acceptable
RAM2: The outputs will help for the decision-making process
RAM2: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree

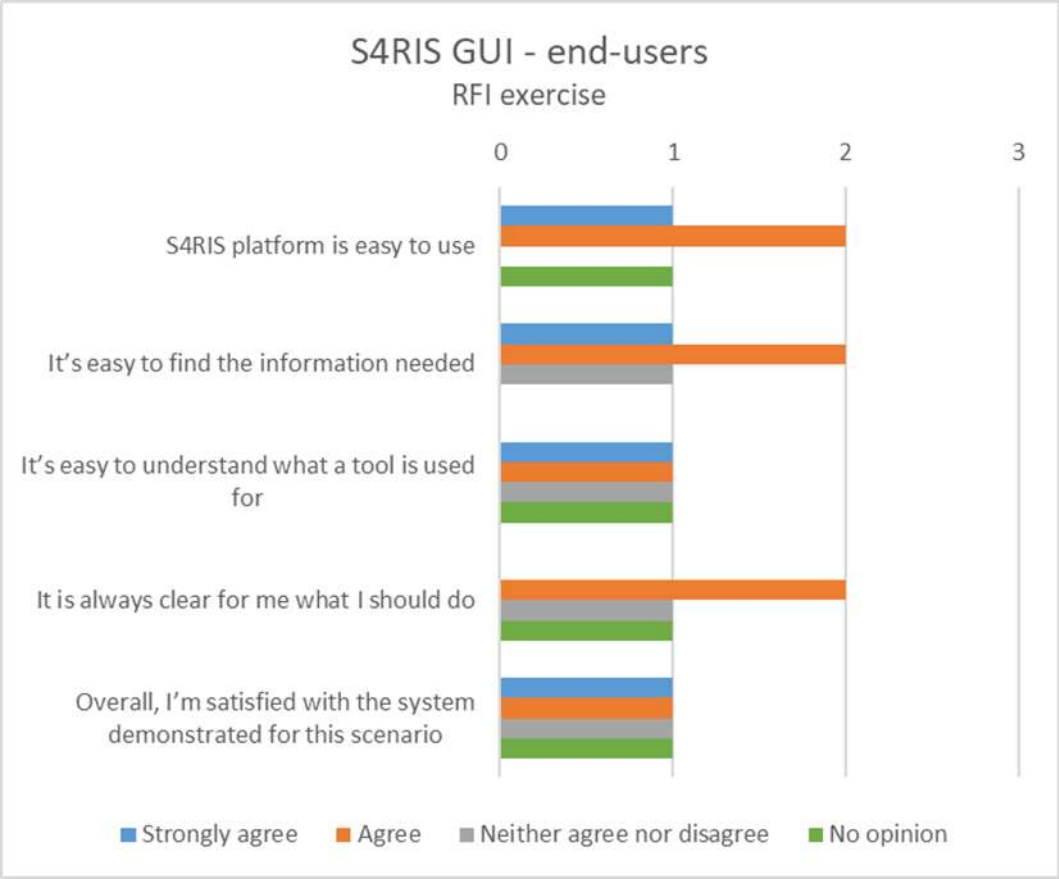

RAM2 - response, others
Full Joint Scenario Exercise
RFI exercise
RAM2: The objective was successfully met
RAM2: The time for processing was acceptable
RAM2: The outputs will help for the decision-making process
RAM2: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Disagree
No opinion


WINGSPARK - response, end-users
Full Joint Scenario Exercise
RFI exercise
WINGSPARK: The objective was successfully met
WINGSPARK: The time for processing was acceptable
WINGSPARK: The outputs will help for the decision-making process
WINGSPARK: The GUI of the individual tool is user-friendly
Strongly agree
Agree


WINGSPARK - response, tool providers
Full Joint Scenario Exercise
RFI exercise
WINGSPARK: The objective was successfully met
WINGSPARK: The time for processing was acceptable
WINGSPARK: The outputs will help for the decision-making process
WINGSPARK: The GUI of the individual tool is user-friendly
Strongly agree
Agree


WINGSPARK - response, others
Full Joint Scenario Exercise
RFI exercise
WINGSPARK: The objective was successfully met
WINGSPARK: The time for processing was acceptable
WINGSPARK: The outputs will help for the decision-making process
WINGSPARK: The GUI of the individual tool is user-friendly
Strongly agree
Agree
Neither agree nor disagree
No opinion

RFI S4RIS GUI QUESTIONNAIRE 3



What could be improved in the GUI?

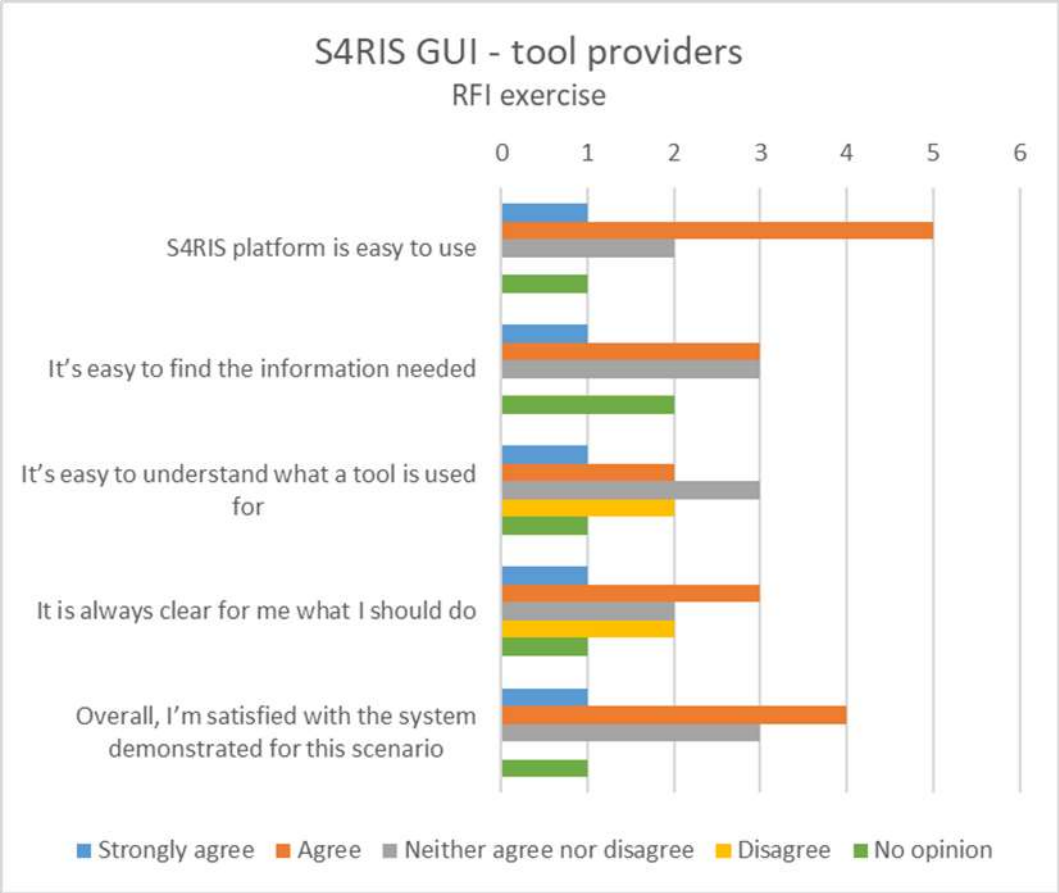
- more explanation for each tool , design of the GUI, guide for the user ,
- This is probably one of the most important parts of the system; I think when the time is right (end)users need the opportunity to "play with the system" so they can get an actual feel of the system and what it can do.
- Huge improvement. Thank you

What complexity / functions are not necessary and can be deleted or reduced?

- not clear at this moment
- For the moment everything is needed.

What could be improved to make the handling more transparent?

- RAM2 which integrate all the alerts could be highlighted as the integrated tool
- not clear at this moment
- We need more time to see it.



What could be improved in the GUI?

- Advices when to use what tool
- Information flows
- More UX efforts can create a better accessible portal
- Consult some graphics designer
- Add a technical criterion to the category, and then briefly describe the general items.
- The responsiveness could be improved. Also the content is spread among many tabs. It could be more concentrated
- Access mode
- I am not sure if the users of S4RIs - especially those who are not involved in the project, are aware of what the tools are doing and what they should do next. Therefore, I suggest to insert additional information like tooltips that explain what the tools or functionalities are doing when the user is hovering with the mouse over buttons...

What complexity / functions are not necessary and can be deleted or reduced?

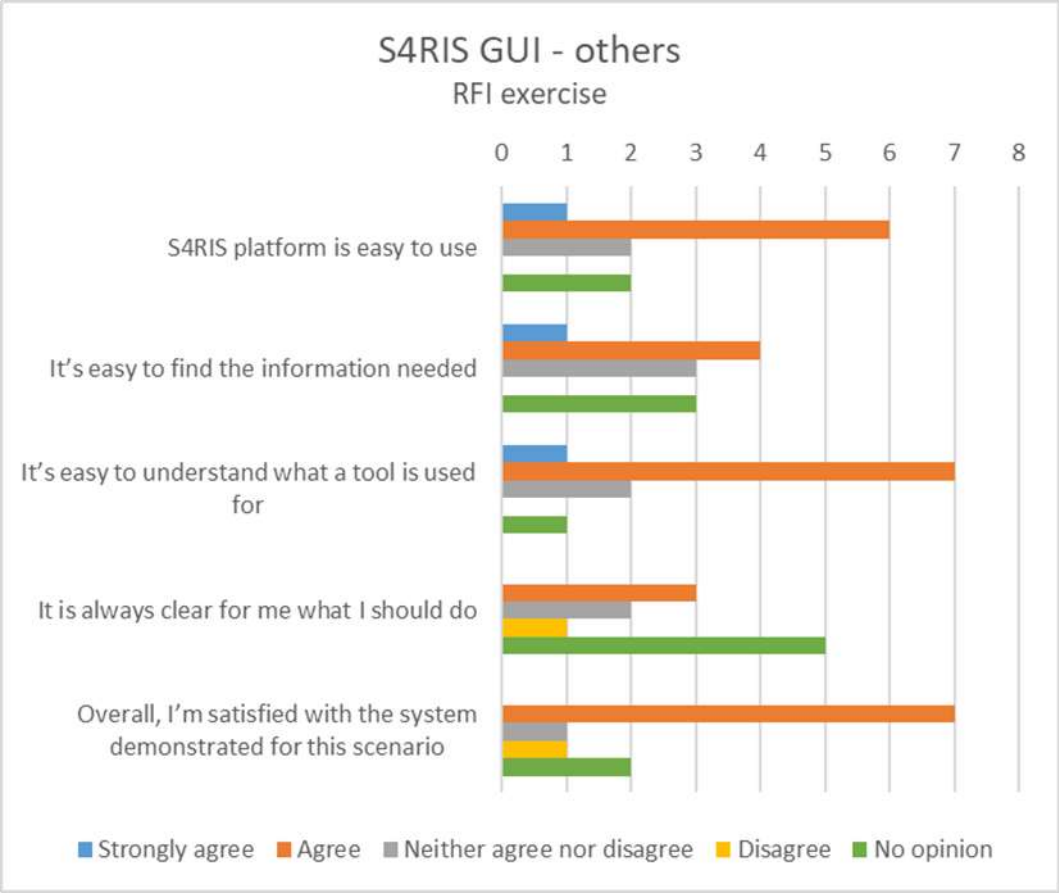
- nothing to be removed.
- Menu for accessing the tools per category
- Only relevant tools for the scenario should appear
- General items can make up a brief summary for the purposes of a project proposal.
- To reduce the complexity, maybe logical next steps can be combined and appear if one option / functionality is checked to guide the user better trough the process

What could be improved to make the handling more transparent?

- Highlight graphically those tool links that are advised to be used next.
- More short, clear and intuitive information to explain what the tools and functionalities are doing

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- I think, The project should have a database that provides detail historical data about similar incidents, focusing on the cost of damaged assets and the time for recovery.
- More short illustrations for the tool results in the joint exercise like for CaESAR



What could be improved in the GUI?

- drop down lists to each city
- Clarity of the options for different end users
- Disagree as S4RIS GUI not directly used in scenario. It would be used if e.g. it was part of the joint exercise as the entry point and results form individual tools would be accessed over the S4RIS GUI.

What complexity / functions are not necessary and can be deleted or reduced?

- Some tools are not needed in a certain time span, I think.
- Minimize options, to only necessary ones
- (Internally there are notes from 12/05 (meeting UNEW/IC/Fraunhofer) on this topic (with connected actions to implement)

What could be improved to make the handling more transparent?

- I don't know.
- Nothing at the moment
- (Internally there are notes from 12/05 (meeting UNEW/IC/Fraunhofer) on this topic (with connected actions to implement)

RFI PLATFORM SPECIFIC QUESTIONNAIRE 4

Were there situations where you did not understand what the system was doing?

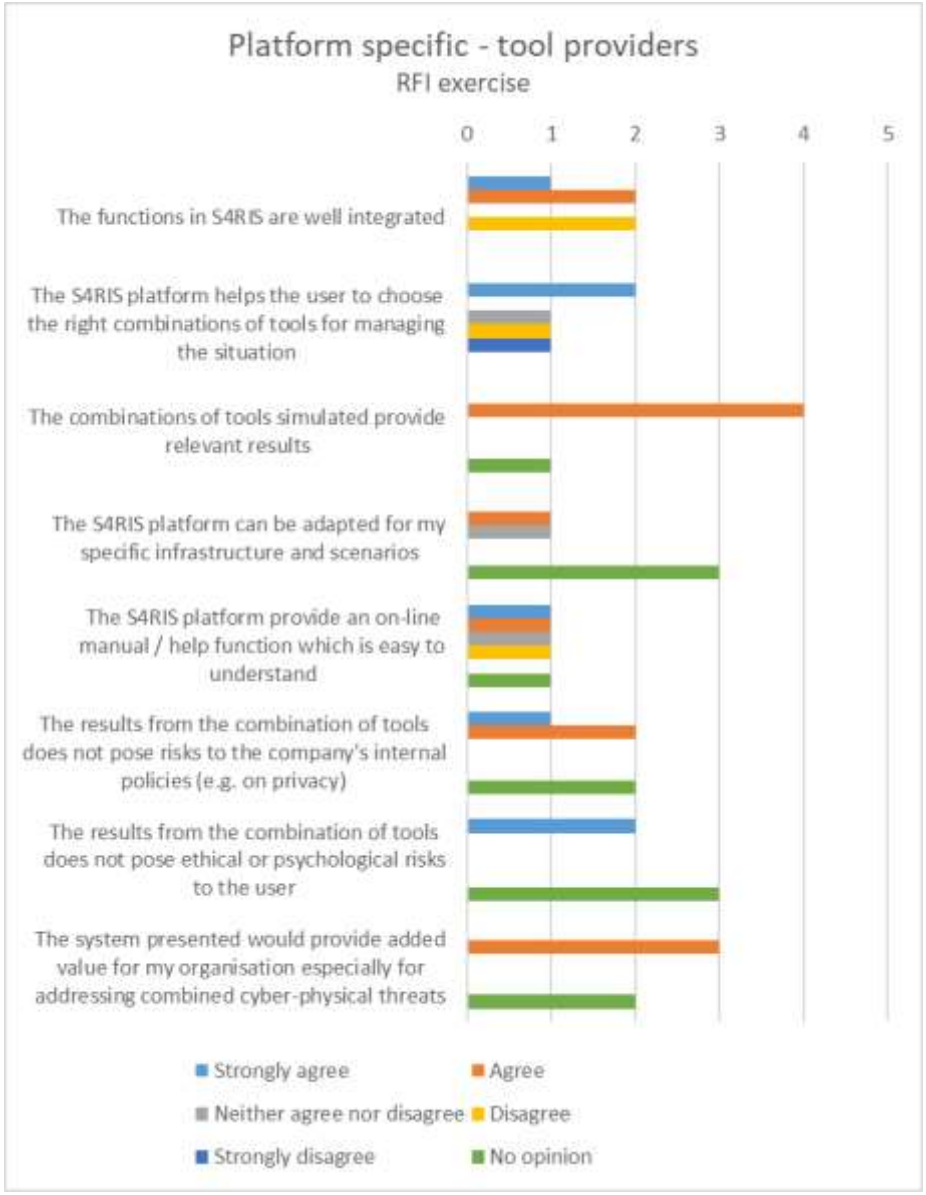
- Although I have quite a good picture about what the tools can do, the time for explanation and demonstration still is relatively short. I expect that the end-user will have a better understanding of the system once they are able to "play" with the system. In the future, helping the end-user to implement te system and a good help desk, will be very important.
- it was clear

Would you recommend the system presented to your colleagues and why?

- There are certain tools which are very relevant for us and which I would certainly like te be presented to some of my colleagues (from the stations department). Then we can have a more interactive session which will benefit the project (feedback) and us as an end-user (better understanding of what the system can do for us).
- yes , the capabilities of the tools and their combination can help to better mange the attack
- Yes, to improve the decision flow in case of an attack

What could be improved in the context of this scenario?

- how to manage the communication to the public,
- An attractive output. But we need to check more in depth using it



Were there situations where you did not understand what the system was doing?

- Yes, specifically about the prevention phase and the role of TISAIL according to the project proposal.
- No, since it was well described. But I am not sure if oit is also clear, when the situation is not described.

Would you recommend the system presented to your colleagues and why?

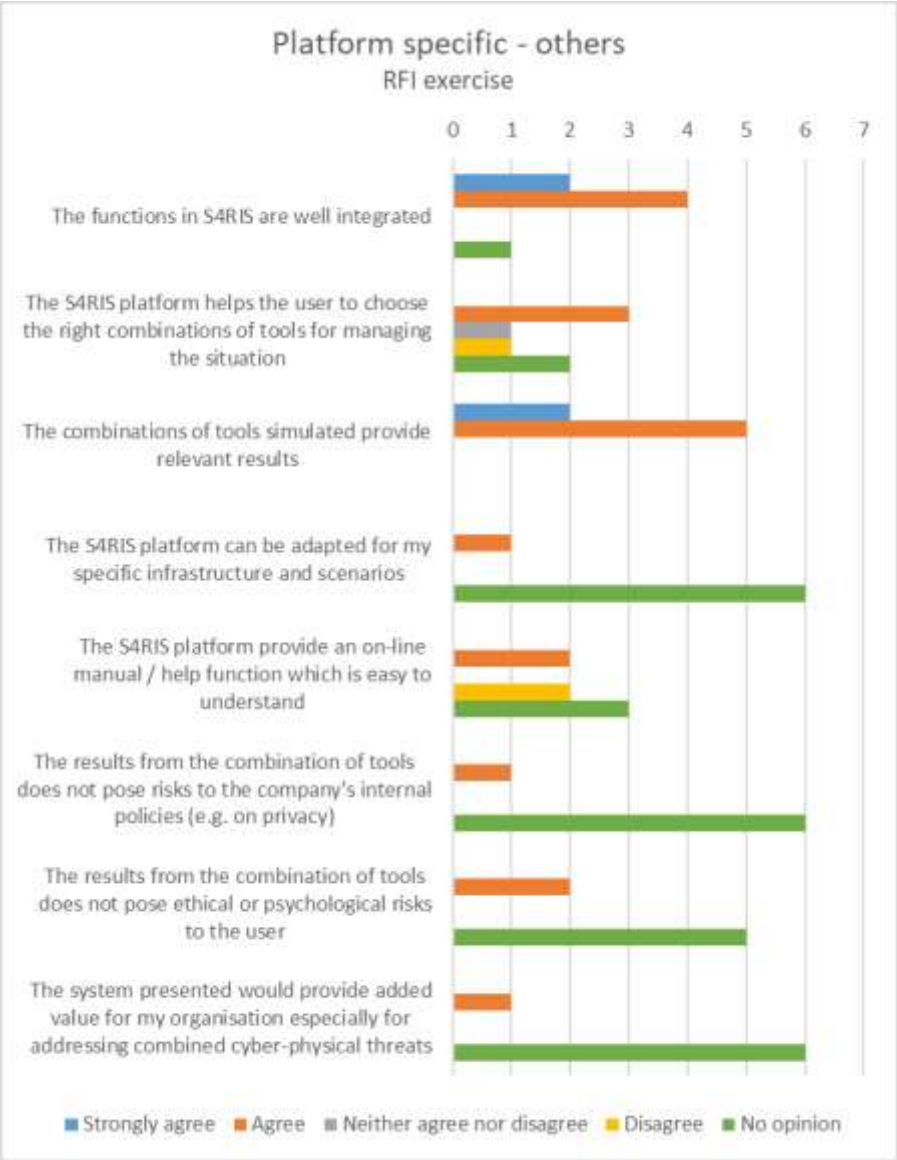
- Yes, as it provides a solution for overall monitoring of various threats for transportation infrastructure
- Not yet, since I think at the moment it is too complex. But if we insert more information on the various functionalities, to make the system more clear, then I would recommend it.

What could be improved in the context of this scenario?

- Some tools provide overlapping functionality. Maybe the organizations could cooperate to provide a unique tool which accomplishes a specific task
- A physical attack and a cyber attack cannot coexist harmoniously . The cyber attack is very simplified in the scenario.
- More (short and intuitive) explanations of the tools and functionalities, more intuitive GUI
- The GUI and the tools presentation within the tool

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- Adapting the scenario based on historical local incidents and RFI internal regulations.
- The system should be as simple as possible and as intuitive as possible to be efficient for the end-user. We should check critically, if this is really fulfilled.



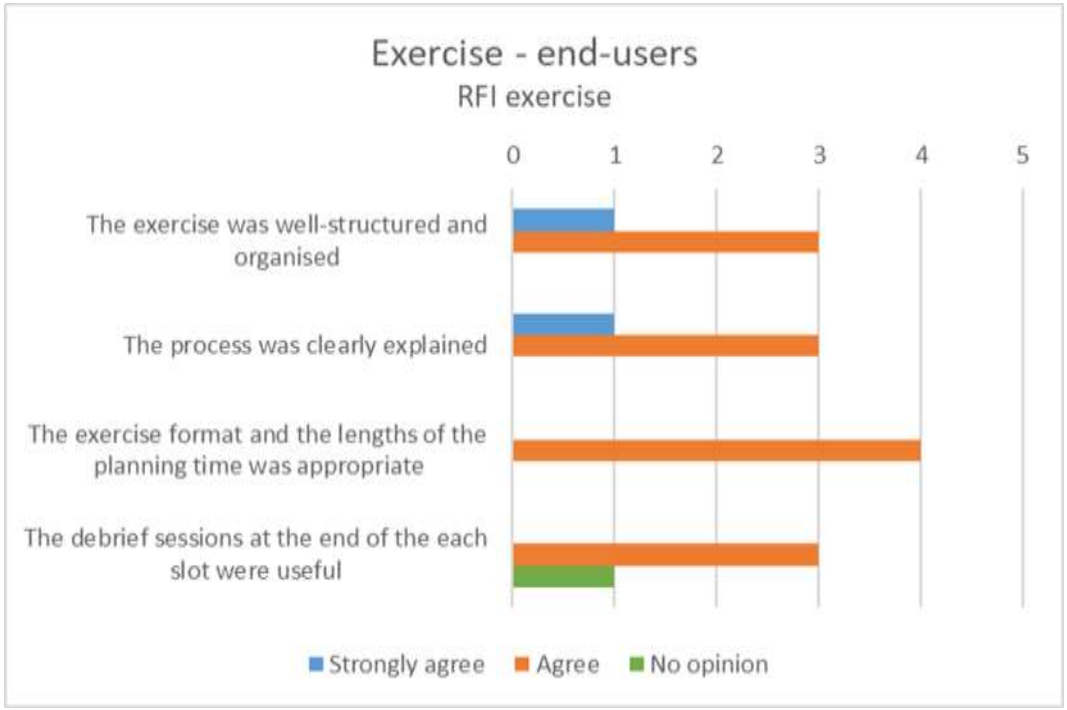
Were there situations where you did not understand what the system was doing?

- Yes, to some degree. I was able to follow the scenario and the reporting though.

What could be improved in the context of this scenario?

- all tools should be shown individually to emphasize the collaborative characteristics of S4RIS
- Where disagree included under S4RIS platform specific it was because this function was not presented/available (manual). More time presenting the mitigation strategies included in RAM2.

RFI EXERCISE EVALUATION QUESTIONNAIRE4



Which part of the exercise did you find the most useful and why?

- I like to explain my comment on the exercise format: within the possibilities (time and space) the format of this exercise is appropriate. I could imagine that a more interactive session (1 on 1) could provide additional feedback
- the joint exercise which shows the integration of the tools
- The joint simulation exercise itself. Because we finally see all tools interacting

Were there any parties missing whose participation would have given added value for the exercise?

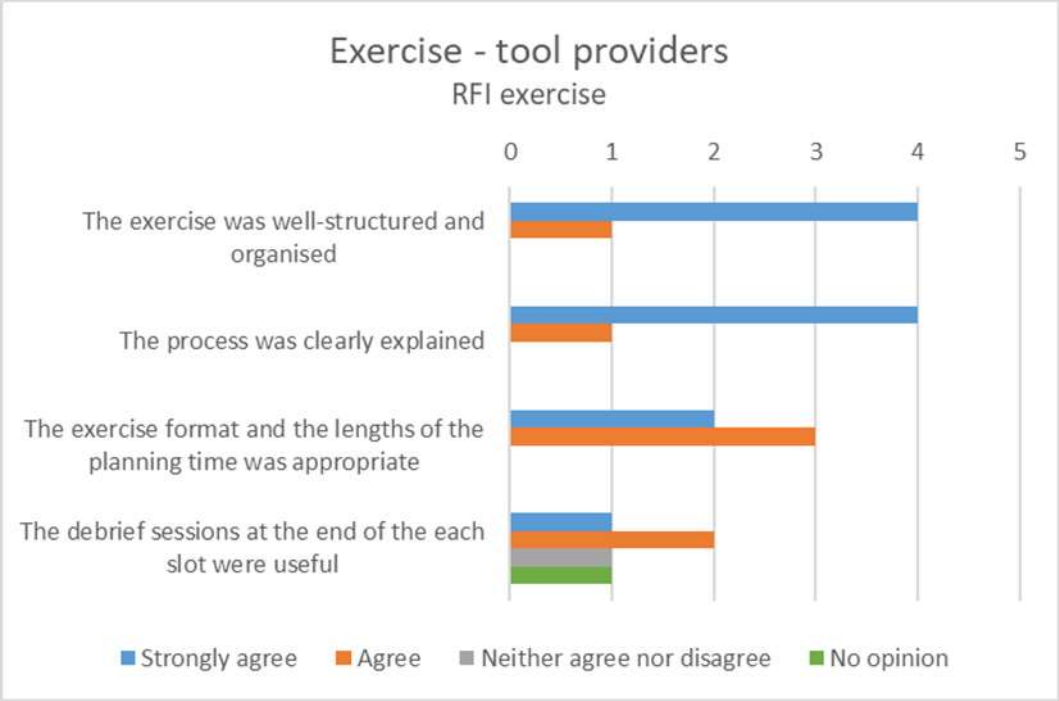
- more representatives from RFI

What can be done differently for the next exercises or what improvement need to be made?

- see earlier comment
- More focus on the joint exercise : with the mitigation measures, the possibility to look at the details in the individual tool that has provided the alert
- Always focusing on the attractiveness of the output. More live simulations of each tool

What are the main lessons learnt for you and why?

- Better understanding of the system
- The huge improvement done by all the tools and the platform



Which part of the exercise did you find the most useful and why?

- Both the prevention phase and detection phase were well done , by DATAFAN and WINGSPARK. During the recovery phase by CAMS, the features were being updated based on previous simulations.
- The joint exercise and the discussion - but this was very short. We should try to get a more intense discussion in the next exercise - because this is the strong benefit that we meet in person.

Were there any parties missing whose participation would have given added value for the exercise

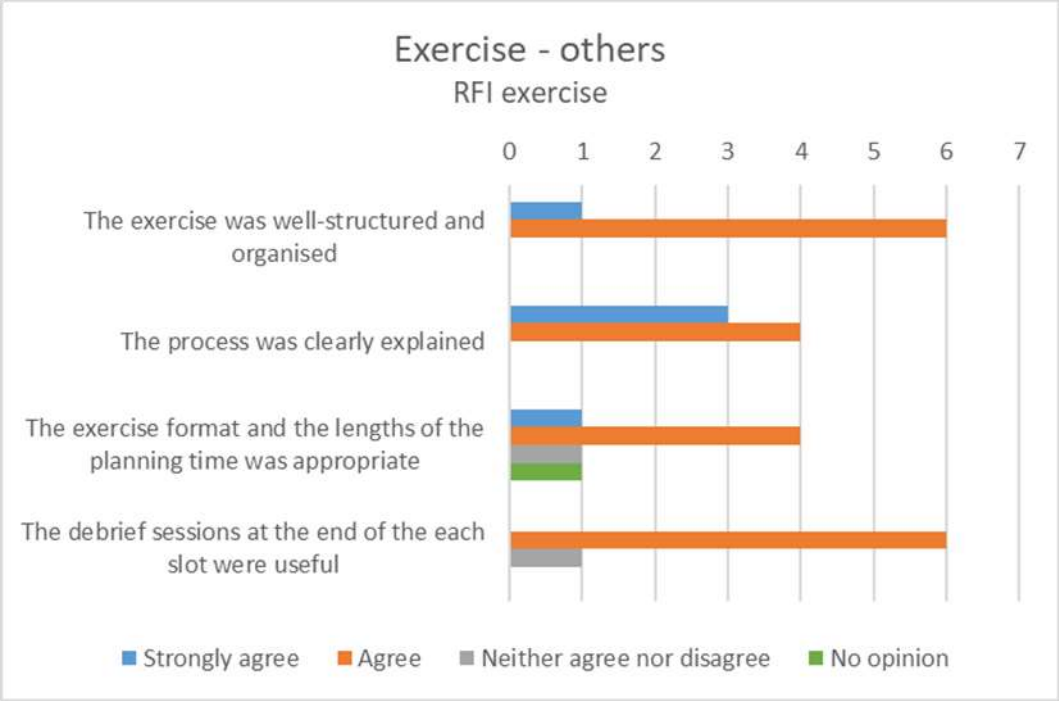
- There are no End-Users from real previous incidents such as RENFE and ADIF, although in the project proposal they are clearly mentioned as related historical incidents in 11 March 2004.
- To involve more end-users and practitioners, more person from the Advisory Board

What can be done differently for the next exercises or what improvement need to be made?

- The provision of more complete set of real data and the deployment of at least some parts/tools of the solution at an actual environment (e.g. on a metro station), in order to showcase better the usefulness of the platform
- Adding historical real data to the scenario.
- The next time, we have to discuss the S4RIS in more detail because we now should focus on the improvement of the GUI and the S4RIS platform to make it as efficient as possible.

What are the main lessons learnt for you and why?

- Separately, the tools are perfect. However, their integration is a challenge.
- Many of the tools and functionalities are still too complex and it is not clear what they are doing in the context of the use case.



Which part of the exercise did you find the most useful and why?

- The possibility to see the combined use of different tools.
- The joint exercise - demonstrates actual integration and results (but the individual tools need also to be presented (as they were) in order to understand the exercise. For the future, maybe it can be considered to have 1 exercise, with all tools (available) accessed over the S4RIS GUI (Tabs) and the tools' providers explain their tools / results / (incl. messages to RAM2 where relevant) as part of the joint exercise; effectively combining what was done in Rome but through 1 joint exercise and the tools trigger the alarms rather than them being mimicked.

Were there any parties missing whose participation would have given added value for the exercise?

- the DMS provider that explains better the behavior of the messaging system
- It would have been nice to have further tools involved in joint exercise

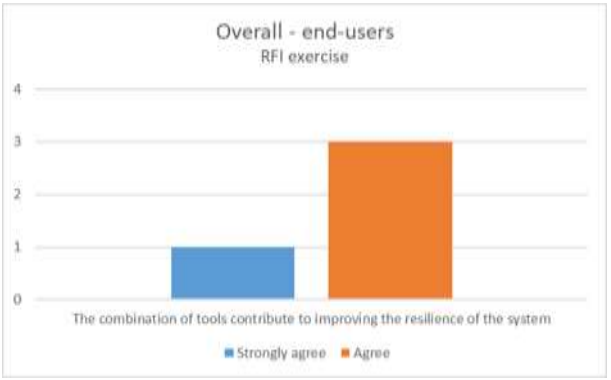
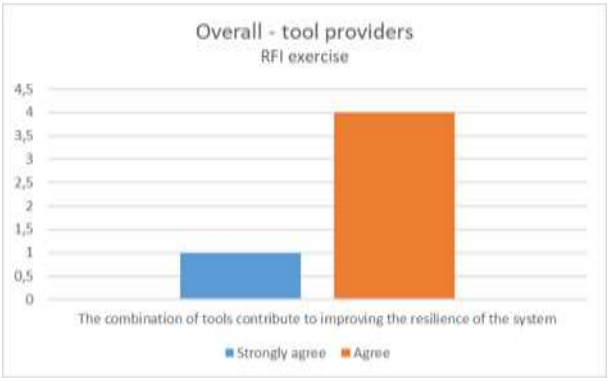
What can be done differently for the next exercises or what improvement need to be made?

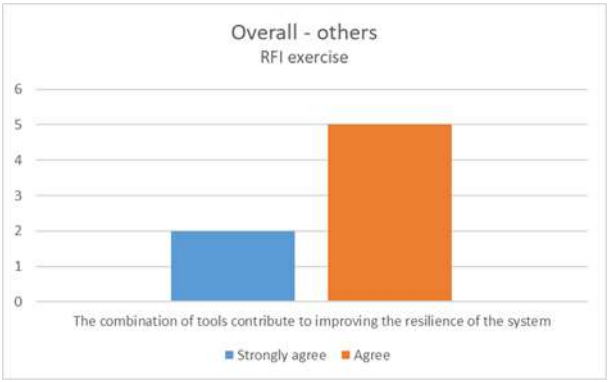
- show each individual tool during the live demo, not a "one-tool show"
- I would have appreciated if I would be able to see a “chart” of how the communication was going for each step and how the different tools are connected to each other.

What are the main lessons learnt for you and why?

- end-users should be more involved, we received not much feedback, don't know how this could be done.
- I now have a more concrete understanding of how the system is going to work.
- It was known before but it still must be clarified what will be now the end status of DMS + S4RIS GUI integration for all contributory tools to SAFETY4RAILS. Also further functionalities in S4RIS GUI itself are still in the process of implementation (notes from 12/05 UNEW/IC/Fraunhofer very relevant here)

RFI OVERALL QUESTIONS QUESTIONNAIRE 4

<table>
<tr>
<td> 
</td>
<td>Which capabilities are the most important/useful for this scenario?
• integration
• The coordination of all the tools
What are the current obstacles for adopting such a system?
• Provision of data
• Huge change for operators that have already tools
What could be improved in the context of this scenario?
• Outputs. Include images. More attractive
Has any limitation of tools been discovered during the exercise? If so, please specify.
• Attractiveness
What is the overall added value as may be assessed from your own experience in your current daily work?
• data based decision making
• The output coming from a combination of so many tools</td>
</tr>
<tr>
<td> 
</td>
<td>Which capabilities are the most important/useful for this scenario?
• The Decision Support System
• The monitoring of passenger's behavior if well implemented would be of great importance
• End-to-end-user experience and management.
• The real-time monitoring and the innovative and combined information of the tools playing together
What are the current obstacles for adopting such a system?
• Integration with current tools
• It's difficult to simulate an actual terrorist attack to evaluate the usefulness of such a platform. As a result realistic KPIs are difficult to be defined and met
• Comparing data between tools and sharing and integrating data together.
• Too much complexity to get good results
What could be improved in the context of this scenario?
• Analyzing historical data from previous incidents.
• A bit more time for preparation in advance, more time to discuss the S4RIS in detail to make it as efficient as possible
What is the overall added value as may be assessed from your own experience in your current daily work?
• The participants' features are being generated efficiently.
• The combination of the different tools in one exercise. Let us still make this more efficient! :-)</td>
</tr>
</table>

	What were the main lessons learnt by you and why? • The more I understand about the features of other tools, the better. • The system is (still) too complex to be really efficient ... Any proposals for revisions and/or additions to the requirements and specifications defined to date? • Using historical incidents data for more accurate results. • To reduce the complexity of the system, to make the system more intuitive and more simple •
	Which capabilities are the most important/useful for this scenario? • Collaboration of all the tools. Has any limitation of tools been discovered during the exercise? If so, please specify. • Limitations for individual tools was not always covered in presentations

ANNEX X Assessment of how far the RFI scenario objectives were met based on evaluation

The correspondence of the evaluation results with the objectives set for the tools in each exercise phase is presented in following tables. In the estimation of the achievement of objectives the following classification has been used:

- Fulfilled according to the majority – more than half of the respondents have answered “strongly agree” or “agree” to question “The objective was successfully met”
- Partially fulfilled according to the majority – half of more of the respondents have answered “neither agree nor disagree” to question “The objective was successfully met”
- Not fulfilled according to the majority – more than half of the respondents have answered “disagree” or “strongly disagree” to question “The objective was successfully met”

WARNING: The “good faith” evaluation is based on the data provided in the Annex IX which can include only limited responses and was based on what was seen at the simulation exercise.

RFI SIMULATION EXERCISE - REQUIREMENTS FOR THE PREVENTION PHASE

Tool	**Objective for the RFI exercise**	**Integrated in S4RIS (Y/N)**	**Result of evaluation**
TISAIL	TISAIL will focus on providing situational awareness about cyber-threats that might have an undesirable impact on the RFI infrastructure. In particular, the tool will provide intelligence about the following cases: • Vulnerabilities in CCTV and DVRs systems. Video surveillance systems are crucial for physical security teams and it’s very important to be up to date of disclosed vulnerabilities that can affect these systems. • Malware variants targeting CCTV Cameras and DVRs systems. There are some malware families such as Mirai or BotenaGo that have been targeting during the last		Fulfilled according to the majority

Tool	**Objective for the RFI exercise**	**Integrated in S4RIS (Y/N)**	**Result of evaluation**
	years IoT devices including CCTV cameras. TISAIL will include some IoCs (Indicators of Compromise) as well as some detection mechanism. • Current active malware campaigns that might be a threat for any industry such as active ransomware campaigns.		
DATAFAN	Providing information on the expected number of passengers for a target station (here: Roma Termini), a set of surrounding stations, and for a specific time or event (e.g. during Christmas festivity, rush hour or a soccer game). This can be used as a basis for what-if scenarios (i.e. prevention) where the target station's operability is compromised (e.g. closure of a station) or for an informed responds to an event in progress. Ultimately, the tool supports the end-user in redirecting passenger flows.		Fulfilled according to the majority
CaESAR	• Identification of critical stations/components based on a grid representation of the metro network • Stochastic simulation of various what-if scenarios to identify critical combinations of threats and impacted stations/components		Fulfilled according to the majority

RFI SIMULATION EXERCISE - REQUIREMENTS FOR THE DETECTION PHASE

Tool	**Objective for the RFI exercise**	**Integrated (Y/N)**	**Result of evaluation**
Ganimede	• The analysis of an audio stream searching for relevant pattern in the context of safety and security (a shot in this case) • The detection of objects and people in each frame and their movement to determine if the object is candidate for abandon • The ability of recognizing people based on the clothes they are wearing.		Fulfilled according to the majority
CuriX	Crisis Manager will be alerted when deviations from normal behaviour (anomalies) or potentially upcoming disruptions of technical systems (IT and OT) from their monitoring data are detected. The crisis manager can check metrics and which technical devices are responsible for causing the major change in the system behaviour.		Fulfilled according to the majority
WINGSPARK	The objective of WINGSPARK is to forward the alerts to RAM2 in case the specified thresholds have been exceeded and provide evacuation guidelines to ease the situation.		Fulfilled according to the majority

RFI SIMULATION EXERCISE - REQUIREMENTS FOR THE RESPONSE PHASE

Tool	**Objective for the RFI exercise**	**Integrated (Y/N)**	**Result of evaluation**
WINGSPARK	The objective of WINGSPARK is to forward the alerts to RAM2 in case the specified thresholds have been exceeded and provide evacuation guidelines to ease the situation.		Fulfilled according to the majority
DATAFAN	Providing information on the expected number of passengers for a target station (here: Roma Termini), a set of surrounding stations, and for a specific time or event (e.g. during Christmas festivity, rush hour or a soccer game). This can be used as a basis for what-if scenarios (i.e. prevention) where the target station's operability is compromised (e.g. closure of a station) or for an informed responds to an event in progress. Ultimately, the tool supports the end-user in redirecting passenger flows.		Fulfilled according to the majority
CaESAR	• Quantified resilience assessment based on performance-time curves for the threats of the exercise and estimation of resilience indicators • Comparison of certain mitigation measures (as defined in the exercise) to reduce the impact of the threats of the exercise • Visualization of the model, the impact propagation based on different concepts (connectivity based, agent-based) and the resilience assessment		Fulfilled according to the majority
RAM2	• Correlation of data gathered from multiple monitoring sources in order to detect potential threats. For example, it will be able to correlate the different attack vectors happening in the station • Risk-based prioritisation of issues, case management for tracking response actions. End-user consumes the data through RAM2 Dashboards display. The user follows the prioritised alerts and mitigation steps for each of the alerts for risk reduction and response to detection of ongoing threats.		Fulfilled according to the majority

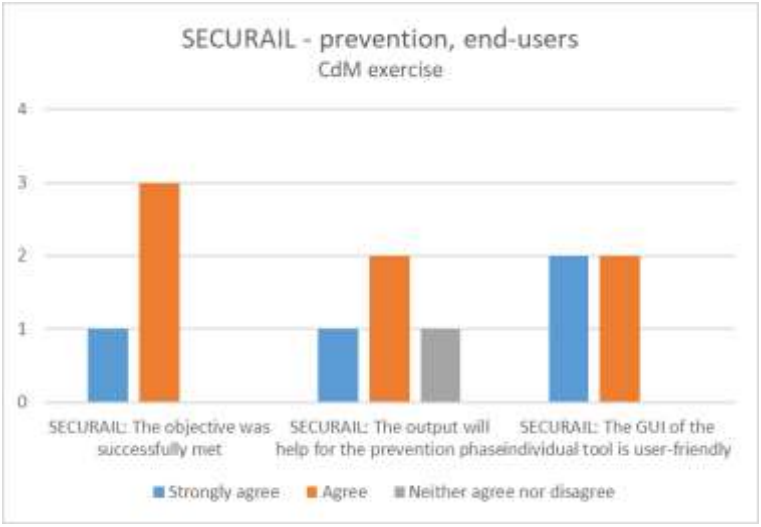
RFI SIMULATION EXERCISE - REQUIREMENTS FOR THE RECOVERY PHASE

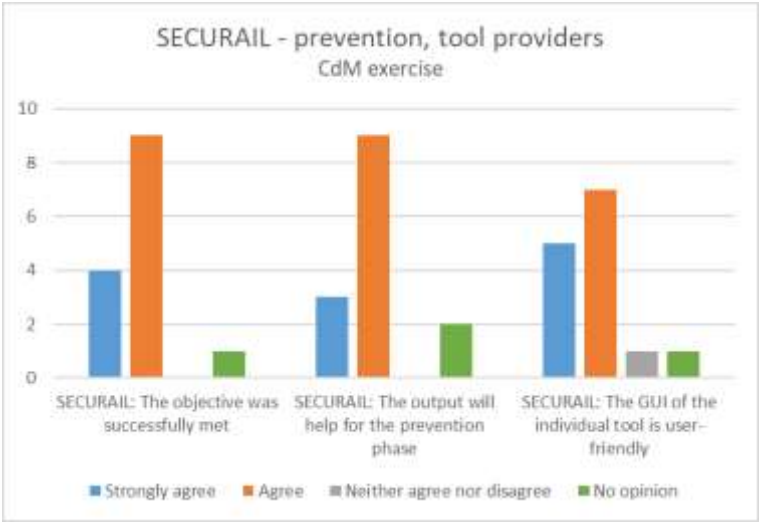
Tool	**Objective for the RFI exercise**	**Integrated (Y/N)**	**Result of evaluation**
CAMS	CAMS will provide accurate recovery cost for assets involved in a sudden event through the assessment of final assets damage. The final damage is assessed using the initial condition (before incident) and the impact measure of the specific incident on the asset. The end-user is then provided with a budget needed to restore the service.		Fulfilled according to the majority

ANNEX XI Milan (CdM) exercise schedule

DAY 2 – JULY 6th – SIMULATION EXERCISE		End-user audiences targeted
OPENING CEREMONY		
09:30 - 10:00	Welcome Speech by CdM Project Presentation by Coordinator (FHG) Presentation about the implementation of the Exercise (LDO)	
PREVENTION PHASE – Individual DEMO		
10:00-11:15	CaESAR (FhG) SECURAIL (STAM) DATAFAN (FhG) SARA (RINA-C)	e.g. Maintenance planners, security managers, risk managers
11:15-11:30	**Online survey/questionnaire for the debriefing of Tools demonstrations for Prevention Phase**	All taking part in this session
11:30-11:45	Coffee break	
FULL JOINT SCENARIO EXERCISE (DETECTION & RESPONSE PHASE)		
11:45-12:45	CuriX (CuriX (IC)) WINGSPARK (WINGS) RAM2 (Elbit) CaESAR (FhG)	Security managers, Control Centre personnel,
12:45-13:00	**Online survey/questionnaire for the Joint simulation exercise**	All taking part in this session
13:00-14:00	Lunch	
RECOVERY PHASE		
14:00-14:30	CAMS (RMIT)	e.g. Maintenance planners, security managers, risk managers
14.30-14:45	**Online survey/questionnaire for the debriefing of Tools demonstrations – Recovery Phase & SARIS UI**	All taking part in this session
14.45-15.00	Coffee break	
OPEN SESSION		
15:00-16:00	Open discussion, final remarks	All taking part in this session
16:00	Closure of the event	
	End of Day #2	

CDM PREVENTION PHASE QUESTIONNAIRE 1

SECURAIL	**Objective:** Allow risk analysis of the metro infrastructure to understand the level of risk for each critical asset for a given hazardous event.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • complete overview on the assett to be protected • The tool can give the municipality an asset for enhancing the mou with the stakeholders • The GUI is very intuitive and easy to use. It is a good tool to list the infrastructure elements and create what-if scenarios. How could this tool be improved in the context of this scenario? • main challenge is the provision of data and their update : is there any automatic process to import and update the data from other information systems? • Better data • Safety and security are the main concerns in railway operation. When an infrastructure element is damaged, if it causes safety or security concerns, it needs to be fixed, no matter the cost. Therefore, perhaps it would be interesting to add a stronger safety-security weight into the tool.

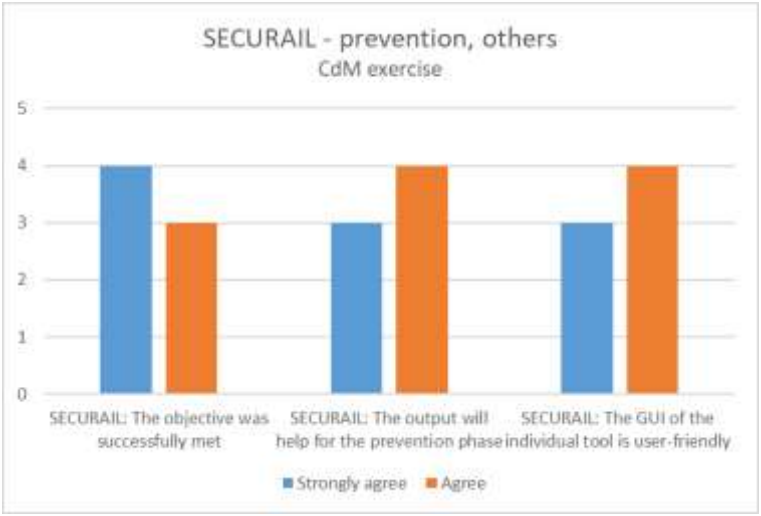


What is the added value of this tool to the prevention phase that you know from your current daily work?

- Quantitative (and mnentary) estimation of risk; risk analysis tailored on specific user railway entwork
- With the tool, it is possible to estimate the prevention of failures caused by disruptive events to interdependent infrastructures, such as railways and metros, and other transportation systems, that may result from disruptions caused by disruptive events.
- May offer some added value in preventing risks, but this needs to be analyzed in more detail.
- performing a risk analysis for the metro infrastructure like CCTS, lights, etc. to identify their functioning and failure

How could this tool be improved in the context of this scenario?

- To simplify and automatize modelling of the network (conenction with BIM models and asset management system?)
- As mentioned above, the tool could be improved by integrating with other tools and adding comparison options between phases to make it more useful.
- No comment at this stage
- To show it more specific to the use case, the presentation was quite top-level

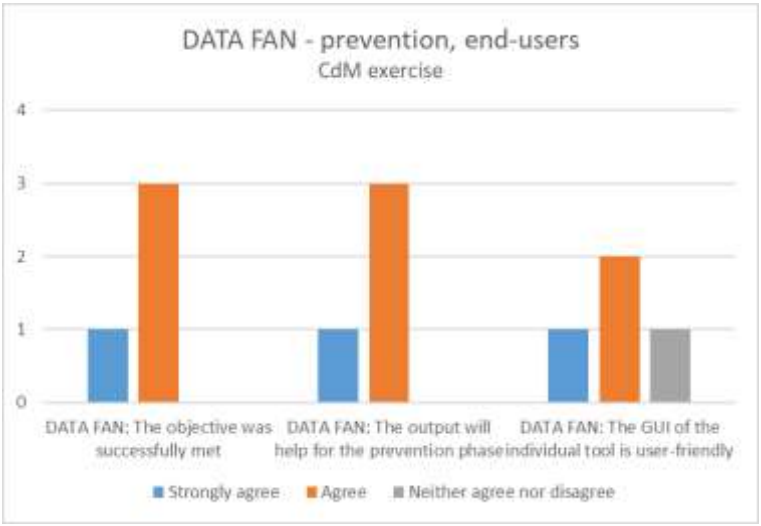


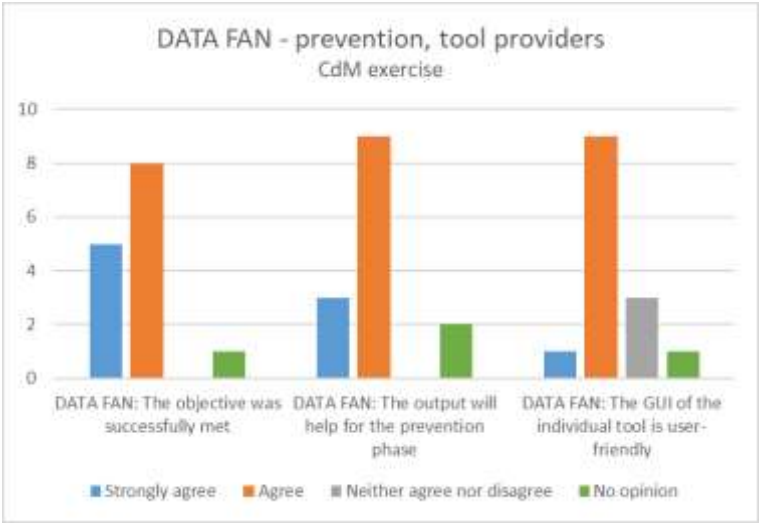
What is the added value of this tool to the prevention phase that you know from your current daily work?

- Flexibilities of the architecture

How could this tool be improved in the context of this scenario?

- Interface for input
- Further improvement of user interaction

DATAFAN	**Objective:** Prediction of the expected number of passengers for a given target station (here: Milan Porta Garibaldi) and its surrounding stations based on historical time-series data. Analysis of events with large crowd concentrations (here: Olympic opening ceremony) using what-if scenarios that affect the free capacity of the target station (e.g. due to the closure of a station).
	What is the added value of this tool to the prevention phase that you know from your current daily work? • provide information to be better prepared and put in place prevention measures • Giving the municipality the opportunity to plan the external stakeholders Activity towards amount of people management • More information when designing redirection procedures when incidents occur. How could this tool be improved in the context of this scenario? • I would personally suggest to make the user experience a little bit easier and facilitated. Additionally I would improve the User interface of the tool: is not very intuitive • Better data • Add redirection recommendations

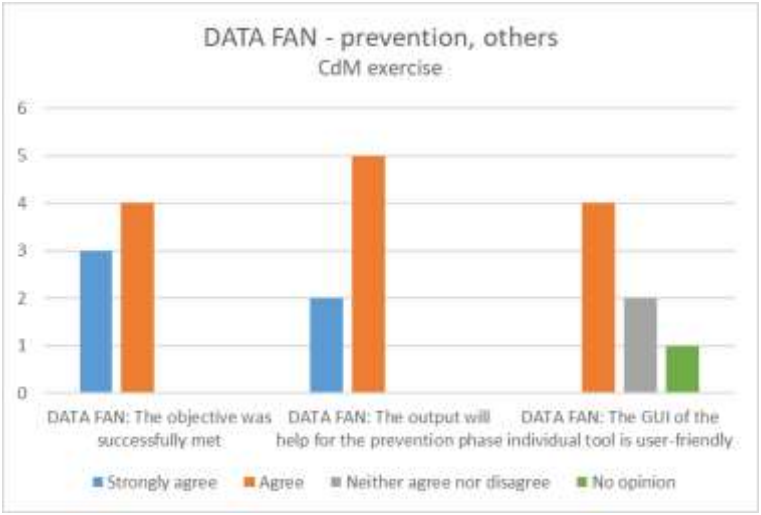


What is the added value of this tool to the prevention phase that you know from your current daily work?

- Quantify the behaviour of the human transportation trends
- Powerful simulation of scenarios
- A tool can estimate the prevention of failures caused by disruptive events to interdependent transportation systems, such as railways and metros.
- Analysis based on profiling might be useful for analyzing demand during repetitive periods,
- To support the end-users in preparing for a hazard event before an incident happens, e.g. before the Opening of the Olympic Games in order to get an idea of the expected number of passenger that has to be additionally dealed with.

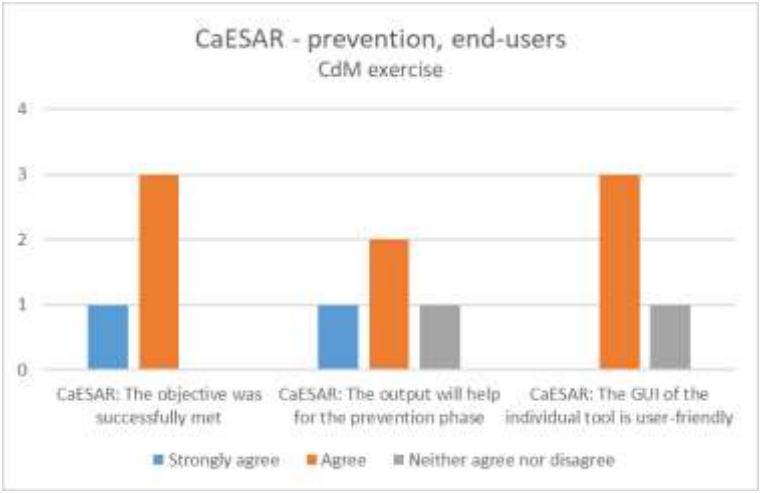
How could this tool be improved in the context of this scenario?

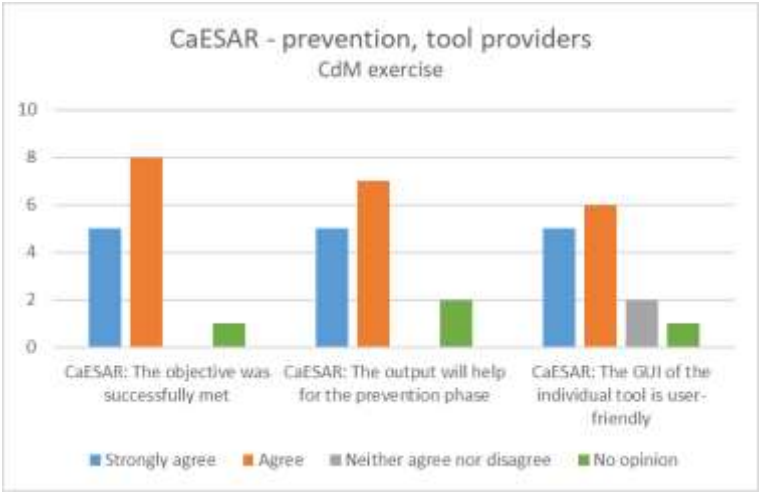
- More accessible and user-friendly GUI; presentation of outputs with advanced charts and views
- In a previous SE, it was suggested that it could be improved by integrating with other tools and adding comparison options between phases..
- This system may fail to provide accurate results when demand changes during exceptional events or unexpected events. This requires adaptation of algorithms with correlation to anticipated changes in case of unexpected events. Has this been considerd?
- To improve the results based on the real data that we got from the end-users.



What is the added value of this tool to the prevention phase that you know from your current daily work?

- Fast calculation

CaESAR	**Objective:** • Identification of critical stations/components based on a grid representation of the metro network • Stochastic simulation of various what-if scenarios to identify critical combinations of threats and impacted stations/components
	What is the added value of this tool to the prevention phase that you know from your current daily work? • supporting the risk assessment phase • The simulation can give us scenarios web can use for bettering out stakeholders' preparation. Web as a municipality could then think about administration support to stakeholders • During prevention, the propagation of impact is already taken into account. Modelling it would be a plus, but sometimes you cannot do anything about the infrastructure you already have. How could this tool be improved in the context of this scenario? • A better User Interface could improve the tool • Bettering the data, the tool could give more precise answers • The tool could be improved by switching the status of the stations (binary --> Functional or not functional) to a more detailed status.

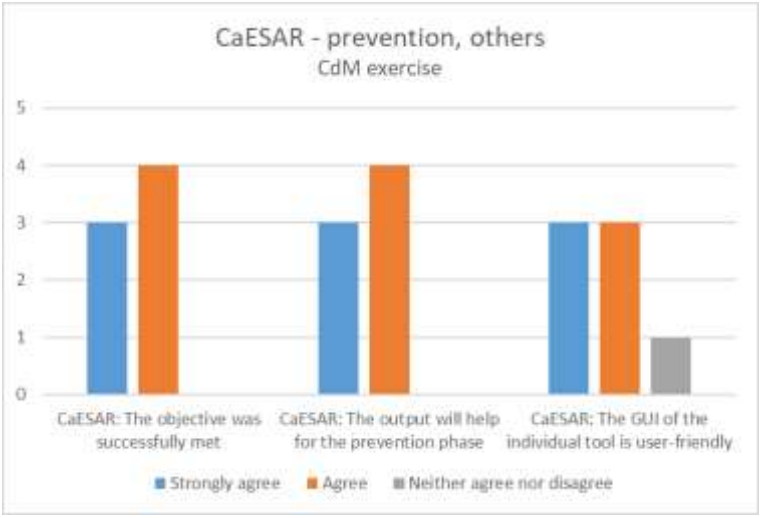


What is the added value of this tool to the prevention phase that you know from your current daily work?

- Prevention
- To model and simulate functionalities of the underlying railway infrastructure
- quickly identify critical nodes of the network under stress
- Using this tool, you could estimate the propagation of failures caused by disruptive events to interdependent infrastructures, such as railways and metros.
- It is similar to tools that we currently market as products.
- To support identifying the critical stations according to an incident
- Easy to use .

How could this tool be improved in the context of this scenario?

- No input
- Improvement of the GUI
- Tool could be more interactive and customisable
- The tool could improve its capability by integrating with other tools and adding comparison options between phases.
- Offer more customization options so it can be better adapted to the operational context of the user.
- Using the real data that we get from the end-users and not only "artificial" data to make the scenario more realistic
- Faster response

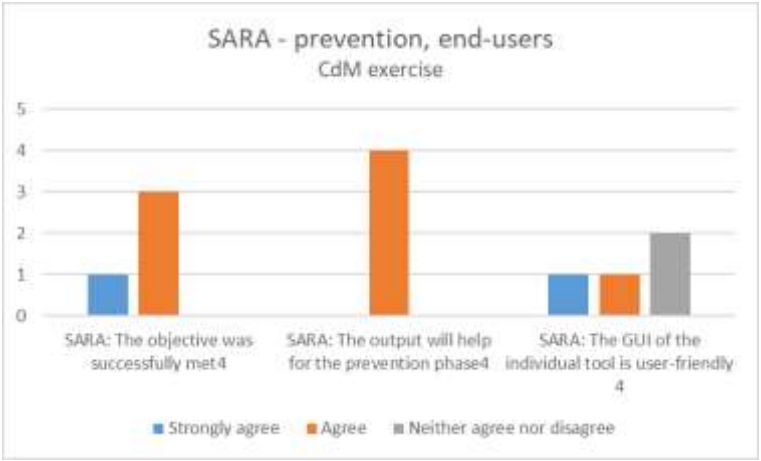


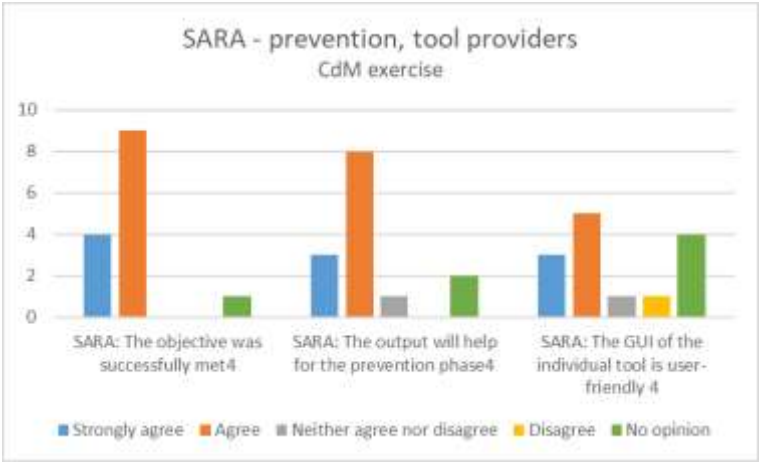
What is the added value of this tool to the prevention phase that you know from your current daily work?

- Integration of different simulators

How could this tool be improved in the context of this scenario?

- More time to explain - but of course time limitations in overall exercise
- More user friendly input
- Improved user experience along with additional functionality

SARA	**Objective:** • Definition of the physical model of the station, for both the structural and equipment part • Description of the people ingress in the station, both for departures and arrivals. • Definition of each scenario, which consist on the definition of the threats and the damage caused on the structural part and on the equipment components. • Definition of different kind of mitigation measure, as hardening, replacing and redundancy of the equipment component. • Evaluation on the economic loss due to direct damage on structure, analysis of the cascading effect on the equipment, computation of the service interruption and/or reduction and its relative economic indirect loss, and at last the evaluation of the affected people and the relative equivalent economic loss.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • better protect assets and increase their resilience in case of an event • Tool to involve other municipal departments • More information to better manage the spending. How could this tool be improved in the context of this scenario? • improve the GUI and the presentation of the mitigation actions • Better and more complete data • Perhaps put more weight on safety and security. When something creates a slight issue with security or safety, the investment to eliminate this needs to be done.

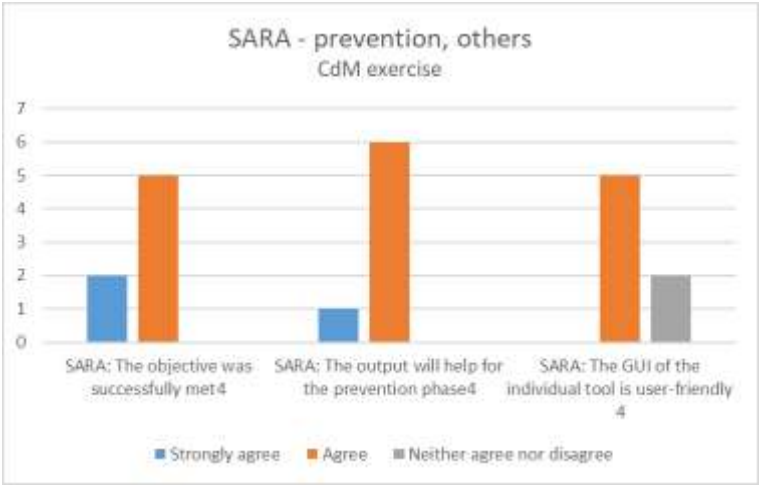


What is the added value of this tool to the prevention phase that you know from your current daily work?

- VEry detailed simulation of the scenario, precious outputs
- The use of a tool can be used to estimate the effectiveness of preventing failures caused by disruptions to interdependent transportation systems, such as railways and metros, as a result of disruptions to these systems.
- Assuming that data is updated to match pertinent changes, this tool offers a value in assessing current demand, as well as physical conditions. Hence preventive measures can be launched to mitigate risks.
- The evaluation of equipment in a threat scenario therms of KPIs

How could this tool be improved in the context of this scenario?

- To be transformed in a more accessible and user-friendly web-app
- As well as integrating with other tools and adding comparison options between phases, this tool could be improved by integrating it with other tools.
- The accuracy can be only as good as the amount and the accuracy of relevant information, hence means of updating information needs to be carefully planned.
- To give more information supporting the end-user in creating a scenario since the tools seems to be very complex



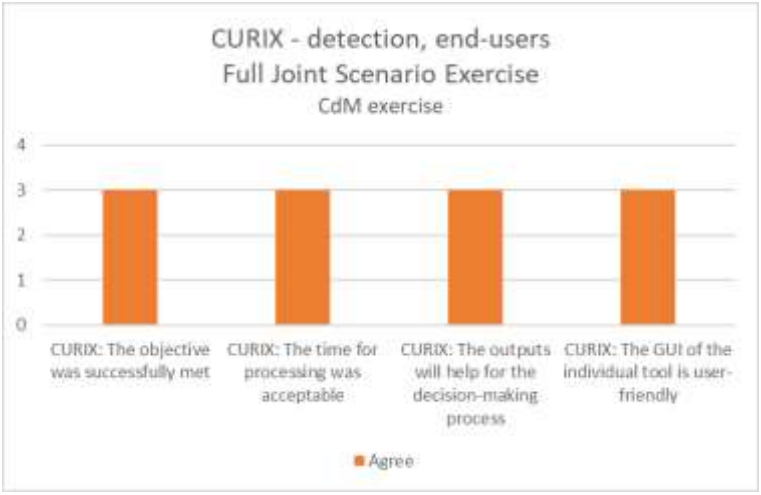
What is the added value of this tool to the prevention phase that you know from your current daily work?

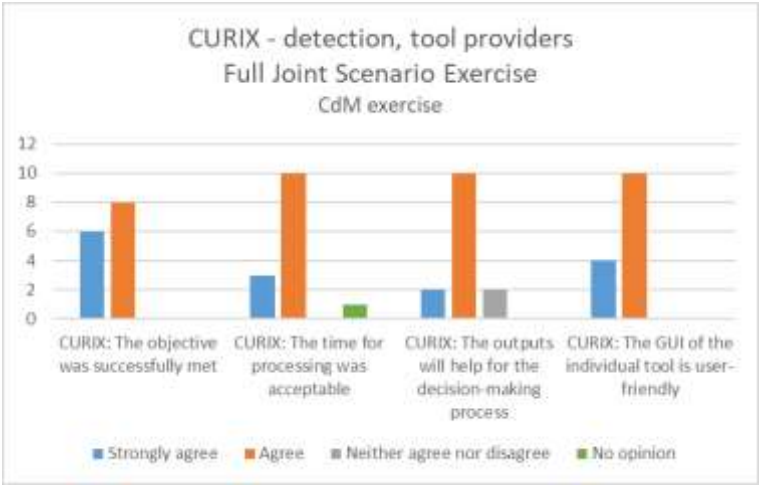
- Robust achitecture

How could this tool be improved in the context of this scenario?

- As a comment: GUI not presented as such - seems expert tool to be used by RINA
- Graphic aspects

CDM DETECTION PHASE
FULL JOINT SCENARIO EXERCISE
QUESTIONNAIRE 2

CURIX	**Objective:** Data regarding the consumption of electric energy and/or voltage levels are monitored, which can be collected from smart meter devices collecting data from the power supply system for the Porta Garibaldi station. Using the anomaly detection capabilities of CuriX on the monitored data, an anomalous behaviour is detected due to the blackout and a corresponding alarm is raised. Additional data from other systems may be monitored, such as the ticketing system and lighting. The latter is also operational during a blackout due to auxiliary power supplies or uninterruptible power supplies.
	What would be your acceptable time to be processed? • I think this was good. The most immediate, the better in case of crisis What is the added value to the detection/response phase that you know from your current daily work? • This can be useful for any enhancement to the power networks and to critical infrastructures refurbishment • early detection to be able to react asap • Having a tool that centralises all the alerts is very convenient. In a railway operator environment there are usually many channels to get information. What could be improved in the context of this scenario? • Always better data (from the stakeholders and the municipality). • sensors for the level of water in the station, tunnel...



What would be your acceptable time to be processed?

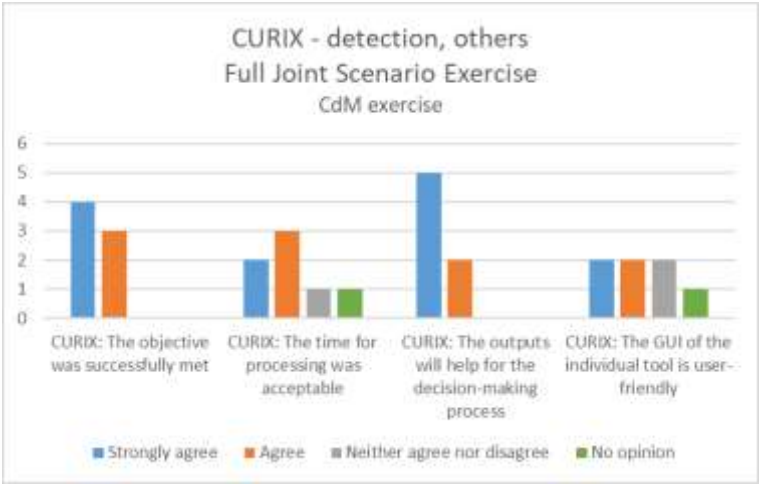
- Demonstration of the tool showed they could monitor data by accessing real-time data bases related to end-users in detection and response phases.
- 1 minute
- Few seconds
- 5min
- 15 - 20 Minutes
- less than 1 minute
- If you mean detection time, this needs to be instant and linked to other cybersecurity tools in case that such incidents are linked with larger scale attacks.

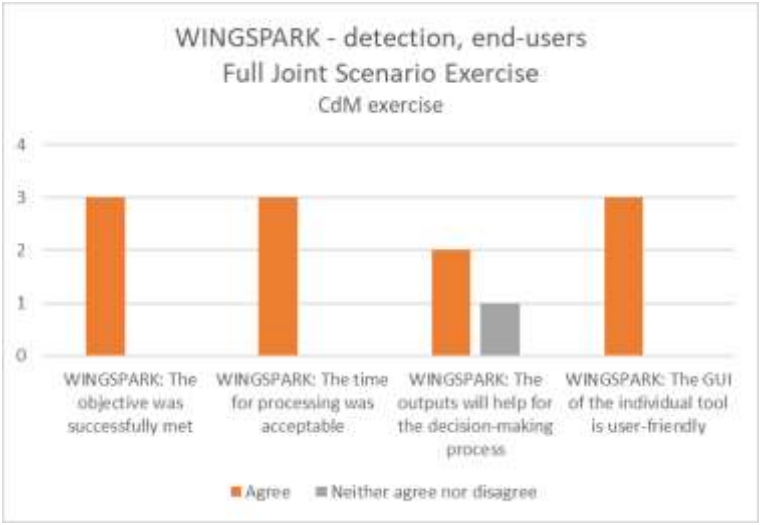
What is the added value to the detection/response phase that you know from your current daily work?

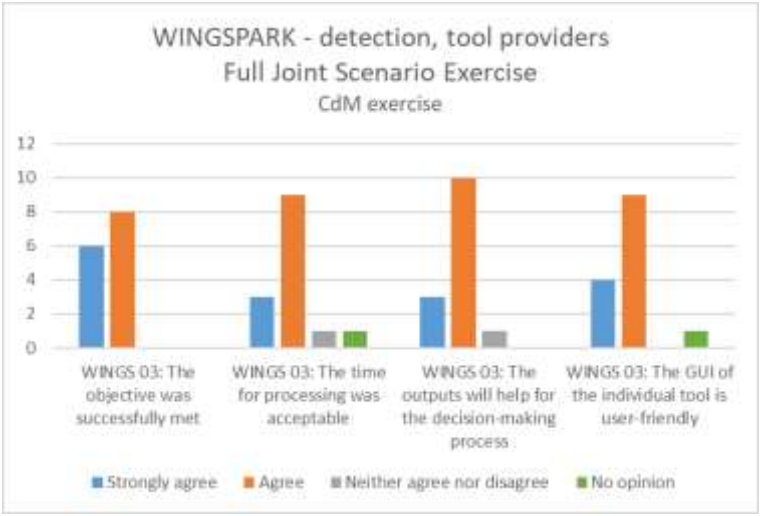
- In detection and response phases, a tool can be used to find incidents caused by disruptions to interdependent transportation systems, such as railways and metros.
- early warning
- Aggregation of avarious alert
- The combination of tools working together and communicating via one platform.
- early warning
- milliseconds
- Apart from detection of faults in energy system, this offers a possible indication of larger scale incident.

What could be improved in the context of this scenario?

- Integration with other tools and adding comparison input data, comparison between phases, and matching up the outputs of those tools can be improved by integrating them.
- Faster responsese and a more clear visualisation of the results
- Anomality detection is linked to blackouts, while excess or under usage and/or discrepancy between demand and supply may indicate cyber threat rather than technical fault.

	What would be your acceptable time to be processed? What is the added value to the detection/response phase that you know from your current daily work? What could be improved in the context of this scenario?

WINGSPARK	**Objective:** Train speed anomaly identification Estimated crowd concentration and alerting when the people density exceeding predefined thresholds Provide evacuation guidelines
	What would be your acceptable time to be processed? • I think this was good. The most immediate, the better in case of crisis What is the added value to the detection/response phase that you know from your current daily work? • Crowd readings could be useful in case of big events, recalling many people to the city, integrating our municipal ability to prevent problems. • early detection and mitigation measures • Estimating crowd concentration in a swift manner. What could be improved in the context of this scenario? • We could enlarge this analysis to other critical nodes in the city, in order to better read the situation • level of water



What would be your acceptable time to be processed?

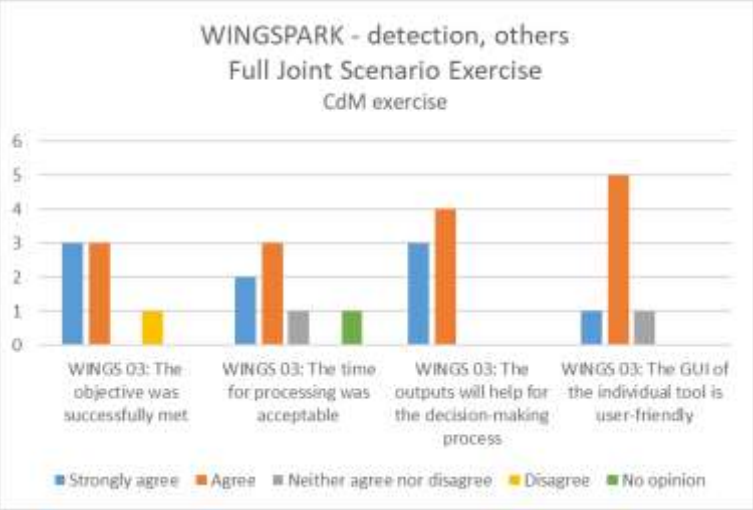
- In detection and response phases, tools should be processed in less than 2 minutes, depending on the type of hazard or physical attack.
- 1 minute
- Few seconds
- 10min
- 2-4 Minutes
- les than 1 minte
- a couple of milliseconds
- In terms of response time, detection of train speed MUST be instant. In terms of passenger density, this is less critical.

What is the added value to the detection/response phase that you know from your current daily work?

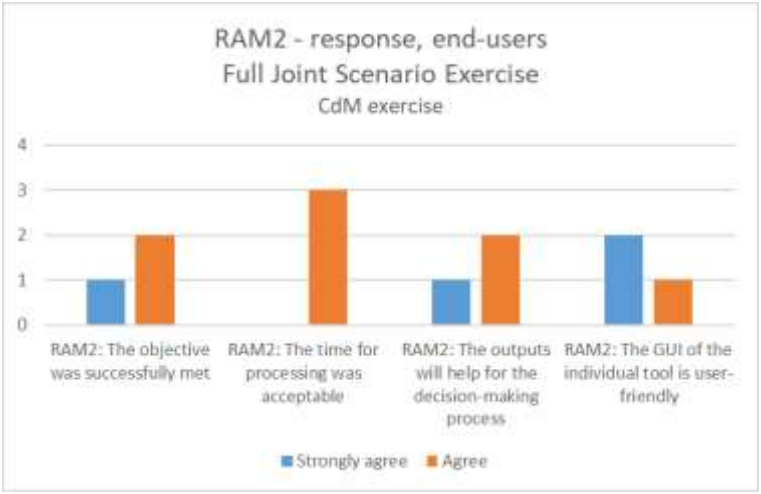
- As part of the preparation, detection, eradication, and recovery activities, it is important to integrate the activities.
- capcaity to raise awareness of occuringthreath
- anomaly detection
- The combination of supporting the train speed anomaly detection and the estimated crowd concentration.
- early warning, dynamic evacuation routes in order to
- Crowd detection and density evaluation would great improve the efficient handling of abnormal incidents
- Speed anomaly is important even in normal system operation. Passenger density is directly required by COVID-like restrictions,

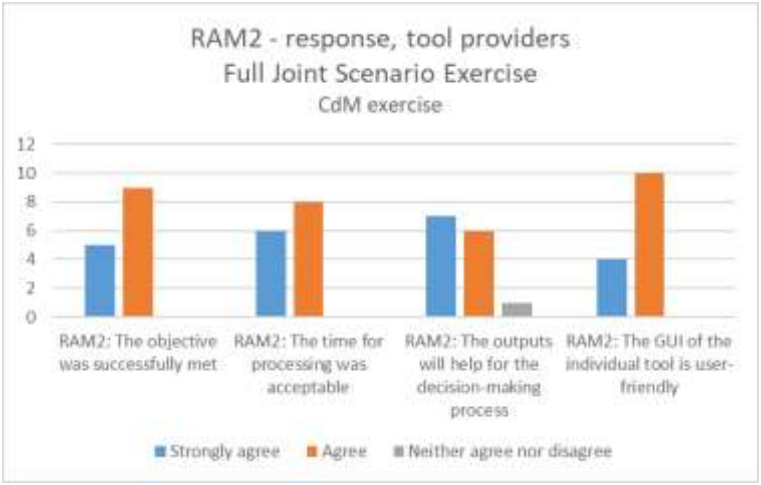
What could be improved in the context of this scenario?

- Through integration of other tools and adding comparison input data, comparing phases, and matching up outputs, the output of those tools could be improved.
- crowd concentrations related to the location of the flooding
- The tool seems to be very complex. Giving small information guiding the user through the process could help here.

	• Integration of entry/exit gates for counting entries and exits from stations, possibly with ML-based count of passengers enterring exiting trains. This would provide the most accurate view of passenger movement across the whole railway network.
	What would be your acceptable time to be processed? What is the added value to the detection/response phase that you know from your current daily work? What could be improved in the context of this scenario? • Disagree stated above under objectives as "Provide evacuation guidelines " not presented

CDM RESPONSE PHASE
FULL JOINT SCENARIO EXERCISE
QUESTIONNAIRE 2

RAM2	**Objective:** Reception via interface with DMS of the alarms provided by the tools, relating to the events of the scenario. Display of alarms with description of possible mitigation actions
	What would be your acceptable time to be processed? • The most immediate, the better in case of crisis What is the added value to the detection/response phase that you know from your current daily work? • stakeholder engagement in mitigation measures and plans description and coordination • all alerts gathered in the same interface What could be improved in the context of this scenario? • Maybe not easy to integrate with different mitigation plans, so it would be good to better understand how to integrate with different plans • how to prioritize the alerts - more focus on the mitigation actions and their status • In order to show the added value in a clearer manner, it could be interesting to show the comparison between conventional alarm displays.



What would be your acceptable time to be processed?

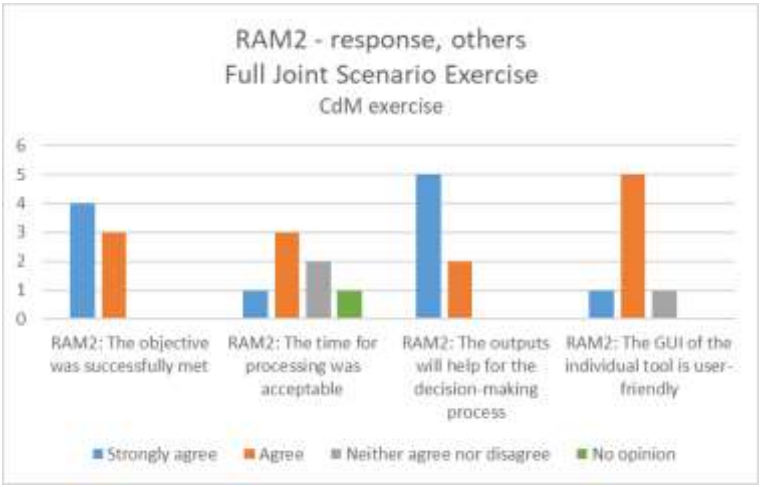
- In the detection and response phases, tools need to be processed within less than two minutes, depending on the type of hazard or physical attack that has occurred, as well as the type of tool that was used.
- 30 seconds
- Few seconds
- 2 Minutes for showing the specific information from the tools
- less than 1 minute
- a couple of milliseconds
- Event detection and notification needs to be immediate, especially if linked with other analytics tools.

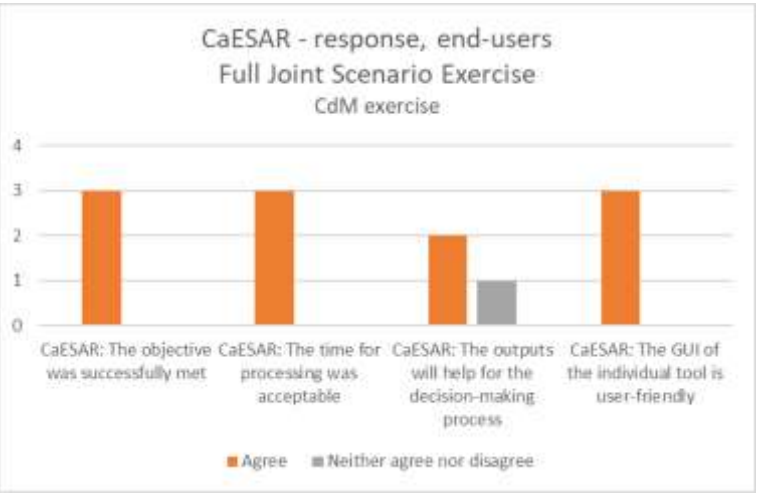
What is the added value to the detection/response phase that you know from your current daily work?

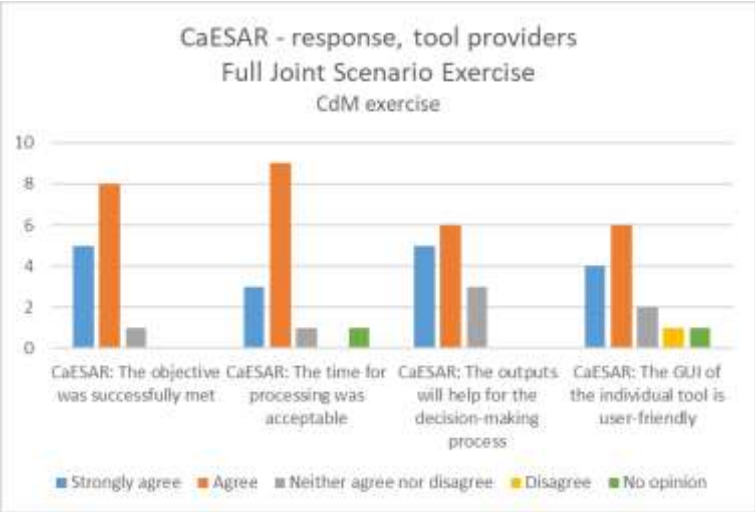
- A tool can be used in the detection and response phases of an incident to make it easier to identify any incidents caused by disruptions to interdependent transportation systems, such as railways and metros, that occur as a result of disruptions to those systems.
- Orchestration of different alerts and messages
- Insights generation
- The aggregation of different alert and the mitigation steps.
- Connected systems and unified platform
- The display of all tool information in one tool
- aggregated info to help the decision making
- Managing alerts and alarms is essential for human operators and may offer added value in automated incident management.

What could be improved in the context of this scenario?

- A better way to utilize these tools would be to integrate them with other tools in order to be able to add comparison data, compare phases, and match outputs more effectively.
- After the alerts happened all together - perhaps taking a step back to revisit and rethink if the alarms display give the whole picture
- Time it takes to reflect messages in RAM2, but could be a Kafka DMS issue as well.

	• The tool seems to be very complex. Giving small information guiding the user through the process could help here.
	What would be your acceptable time to be processed? What is the added value to the detection/response phase that you know from your current daily work? • Strong added value on multiple levels since the tool allows for customized sophisticated decision support What could be improved in the context of this scenario? • More talking through the mitigation measures listed in RAM2.

CaESAR	**Objective:** Quantified resilience assessment based on performance-time curves for the threats of the exercise and estimation of resilience indicators Comparison of certain mitigation measures (as defined in the exercise) to reduce the impact of the threats of the exercise Visualization of the model, the impact propagation based on different concepts (connectivity based, agent-based) and the resilience assessment
	What would be your acceptable time to be processed? • I think this was good. The most immediate, the better in case of crisis What is the added value to the detection/response phase that you know from your current daily work? • Useful for planning the best mitigation measures combination • mitigation measures • The crisis management team usually has experience on picking mitigation measures, but having an added source of information can sometimes help. What could be improved in the context of this scenario? • We could add nodes to scenario and better data from stakeholders and municipality • more details on the mitigation measures : how many guards, where (most affected places), knowledge needed for the guard



What would be your acceptable time to be processed?

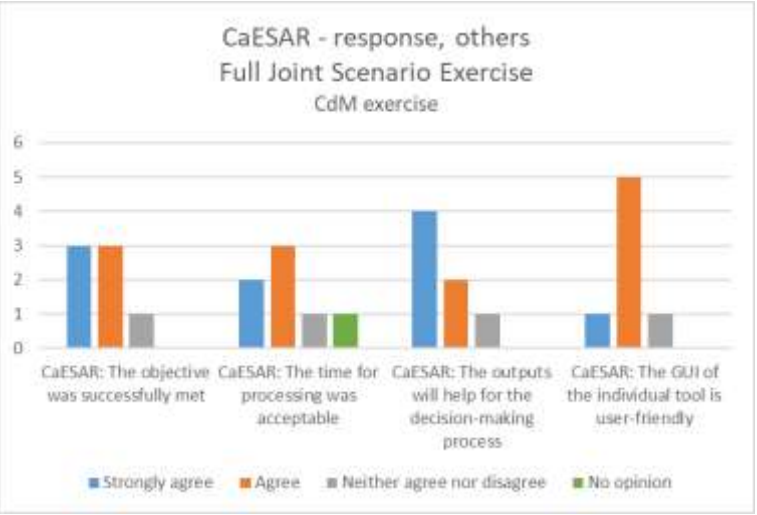
- It is essential for tools to be processed in less than two minutes during the detection and response phases, depending on the type of hazard or physical attack that has occurred.
- 2 minutes
- < 2 minutes
- 2-4 Minutes
- a couple of milliseconds
- Resilience management is not time critical, unless it is directly linked with incident detection, which doe snot seem to apply here.

What is the added value to the detection/response phase that you know from your current daily work?

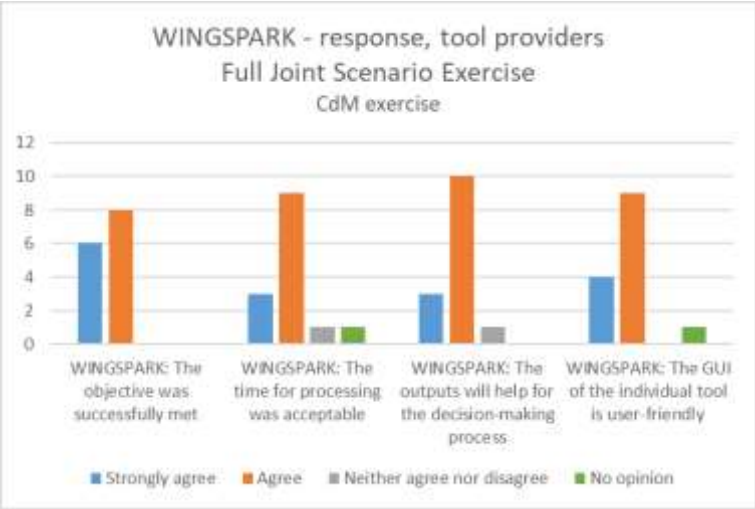
- It is essential for tools to be processed in less than two minutes during the detection and response phases, depending on the type of hazard or physical attack that has occurred.
- fast evaluation of possible consequent scenarios given an occuredthreath
- The identification of critical nodes.
- the reduction of the impact of the threats
- the propagation simulation could enhance identifiying the most vulnerable areas after a specific incident
- Validating resilience and suggesting protection measures is essential in context of raising risks of cyber-physical threats.

What could be improved in the context of this scenario?

- Integrating with other tools, comparing input data, comparing phases, and matching up the output could all be improved through integration.
- presentation of information
- clearer phrasing of the mitigation measures and parameters of the network model. Show perhaps exemplary how the network can be constructed for a rather minimal simple but realistic example
- The tool seems to be very complex. Giving small information guiding the user through the process could help here.
- the UI could be more intuitive

	• More intuitive feedback to end-users might need to be considered.
	What would be your acceptable time to be processed? • Acceptable time depends on the complexity of the models to be analyzed What is the added value to the detection/response phase that you know from your current daily work? What could be improved in the context of this scenario? • Mitigation measure related to the physical presence of guards (or staff) could be problematic: it should be linked to the real time availability of staff and their localisation on the transportation network

WINGSPARK	**Objective:** Train speed anomaly identification Estimated crowd concentration and alerting when the people density exceeding predefined thresholds Provide evacuation guidelines
	What would be your acceptable time to be processed? • I think this was good. The most immediate, the better in case of crisis What is the added value to the detection/response phase that you know from your current daily work? • Crowd readings could be useful in case of big events, recalling many people to the city, integrating our municipal ability to prevent problems. • early detection and mitigation measures • Estimating crowd concentration in a swift manner. What could be improved in the context of this scenario? • We could enlarge this analysis to other critical nodes in the city, in order to better read the situation • level of water



What would be your acceptable time to be processed?

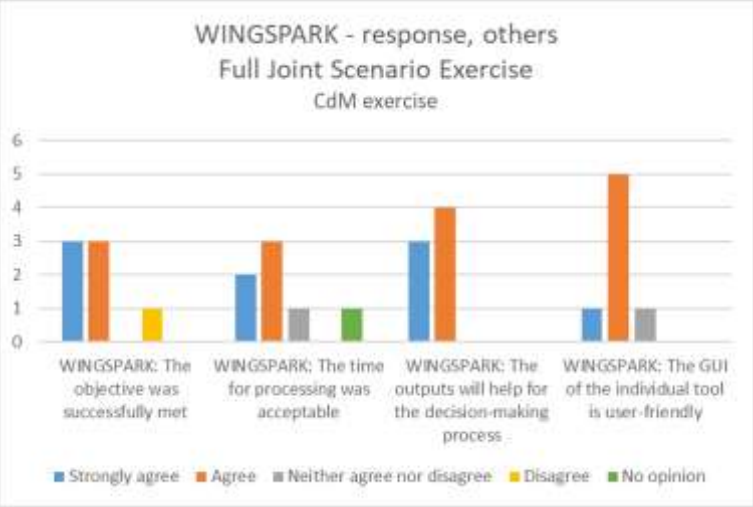
- In detection and response phases, tools should be processed in less than 2 minutes, depending on the type of hazard or physical attack.
- 1 minute
- Few seconds
- 10min
- 2-4 Minutes
- les than 1 minte
- a couple of milliseconds
- In terms of response time, detection of train speed MUST be instant. In terms of passenger density, this is less critical.

What is the added value to the detection/response phase that you know from your current daily work?

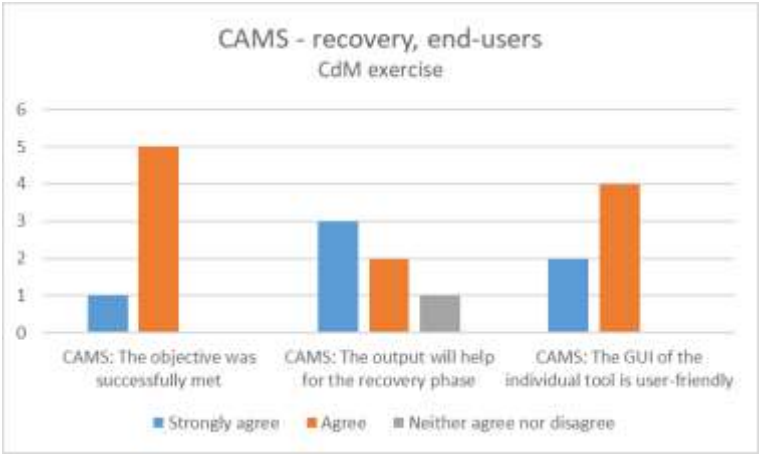
- As part of the preparation, detection, eradication, and recovery activities, it is important to integrate the activities.
- capcaity to raise awareness of occuringthreath
- anomaly detection
- The combination of supporting the train speed anomaly detection and the estimated crowd concentration
- early warning, dynamic evacuation routes in order to
- Crowd detection and density evaluation would great improve the efficient handling of abnormal incidents
- Speed anomaly is important even in normal system operation. Passenger density is directly required by COVID-like restrictions,

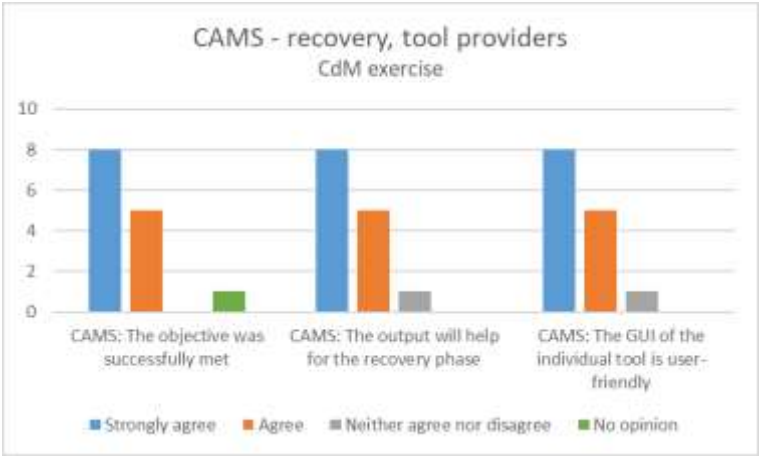
What could be improved in the context of this scenario?

- Through integration of other tools and adding comparison input data, comparing phases, and matching up outputs, the output of those tools could be improved.
- crowd concentrations related to the location of the flooding
- The tool seems to be very complex. Giving small information guiding the user through the process could help here.

	• Integration of entry/exit gates for counting entries and exits from stations, possibly with ML-based count of passengers enterring exiting trains. This would provide the most accurate view of passenger movement across the whole railway network.
	What would be your acceptable time to be processed? What is the added value to the detection/response phase that you know from your current daily work? What could be improved in the context of this scenario? • Disagree stated above under objectives as "Provide evacuation guidelines " not presented

CDM RECOVERY PHASE QUESTIONNAIRE 3

CAMS	**Objective:** Providing accurate recovery cost for assets involved in a sudden event through the assessment of final assets damage. The final damage is assessed using the initial condition (before incident) and the impact measure of the specific incident on the asset. The end-user is then provided with a budget needed to restore the service. As well prediction of normal deterioration due to aging of railway assets in the system considered, Maintenance and repair budget calculation for railway components In this scenario CAMS used to inform the station operator on the budget to allocate to repair, maintain, and rehabilitate the infrastructure after a set of possible events.
	What is the added value of this tool to the prevention phase that you know from your current daily work? • It is useful to have an idea of the recovery costs and therefore to plan eventual recovery options • better management of the budget for asset • FGC already has a an asset replacement procedure which is based on technical and accountable amortization. In case of incidents, the criticality is focused on safety. If any component of the assets is damaged in a way that it can lead to safety issues, it is replaced. The recovery costs are already known. How could this tool be improved in the context of this scenario? • Having better data fromstakeholdefs could give better previsions

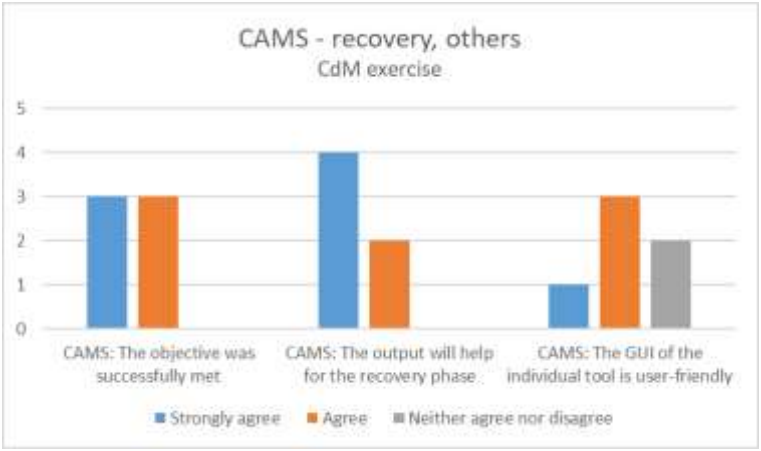


What is the added value of this tool to the prevention phase that you know from your current daily work?

- In recovery phases, a tool's value lies in providing accurate recovery costs for assets involved in a sudden event by assessing final asset damage. An asset's final damage is assessed using its initial condition (before incident) and its impact measure. A budget for restoring the service is then given to the end-user. Calculation of maintenance and repair budgets for railway components as well as prediction of normal deterioration due to aging. As a tool in the recovery phase, CAMS provided the station operator with information regarding the budget needed to repair, maintain, and rehabilitate the infrastructure.
- The tool can help decision makers about cost and time management
- Cost estimation and optimization of financial resource allocation.
- understand cost to be sustained for recovery
- Budget planning
- condition assessment
- The value is both for ageing maintenance and in recovery.
- Supporting the end-user in evaluating the recovery costs

How could this tool be improved in the context of this scenario?

- To improve the context of the scanrarion, we need a dynamic database combining historical data and real-time data from end-users, and we need to integrate all the tools used during the analysis process. In addition, comparing tool outputs of all related phases to incidents in a unique review could be more effective.
- Maybe adding some historical data can increase accuracy of cost and time analysis
- Integrate more sources of information
- showing directly the condition of the assets impacted by the flooding and if it where considering to replace some components because they were old anyway
- Have specific conditions that might affect the recovery conditions (accessibility, supply, transport) been taken into consideration for crisis related scenarios?
- This tool seems to be quite complex. Maybe small information guiding the end-user through the tool could be helpful.

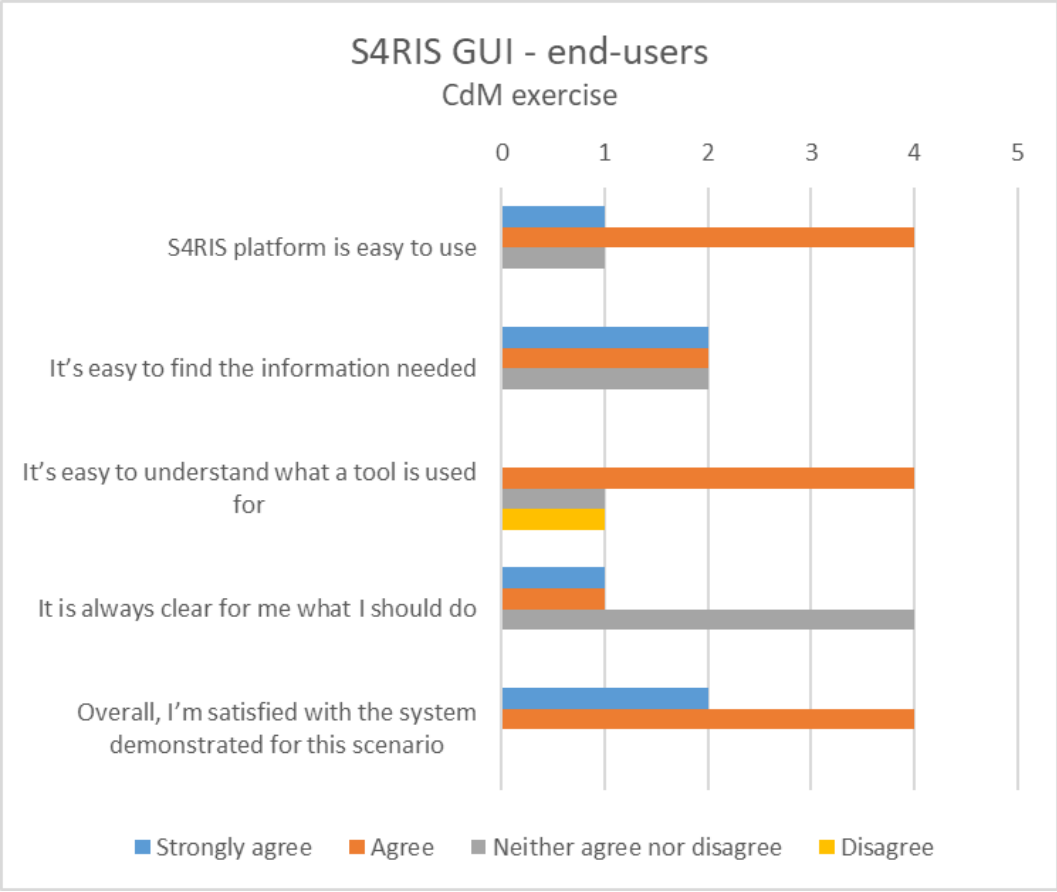


What is the added value of this tool to the prevention phase that you know from your current daily work?

How could this tool be improved in the context of this scenario?

- As mentioned by question raised, it could interest to interconnect the tool with SECURAIL to ensure an accurate update of assets involved and potentiel costs if they are damaged
- Build more advanced use cases so the capabilities of the tool can be further showcased and understood

CDM S4RIS GUI QUESTIONNAIRE 3



What could be improved in the GUI?

- I think the platform would need a clearer homepage with at least one or two sentences that briefly explain the content of tools and their objective. Additionally, the user interface could be redesigned in a more attractive way. Last point: I think it could be great to allign the graphics of all the differente tools in S4RIS platform
- I should use it directly before saying anything about improvements
- to provide a dashboard with main onformation on the situation
- Centralised login. Having to log in to each of the tools creates friction in the usability. Also, a thumbnail of the most visual output of the tool could be added in order to increase the swiftness of the usability.

What complexity / functions are not necessary and can be deleted or reduced?

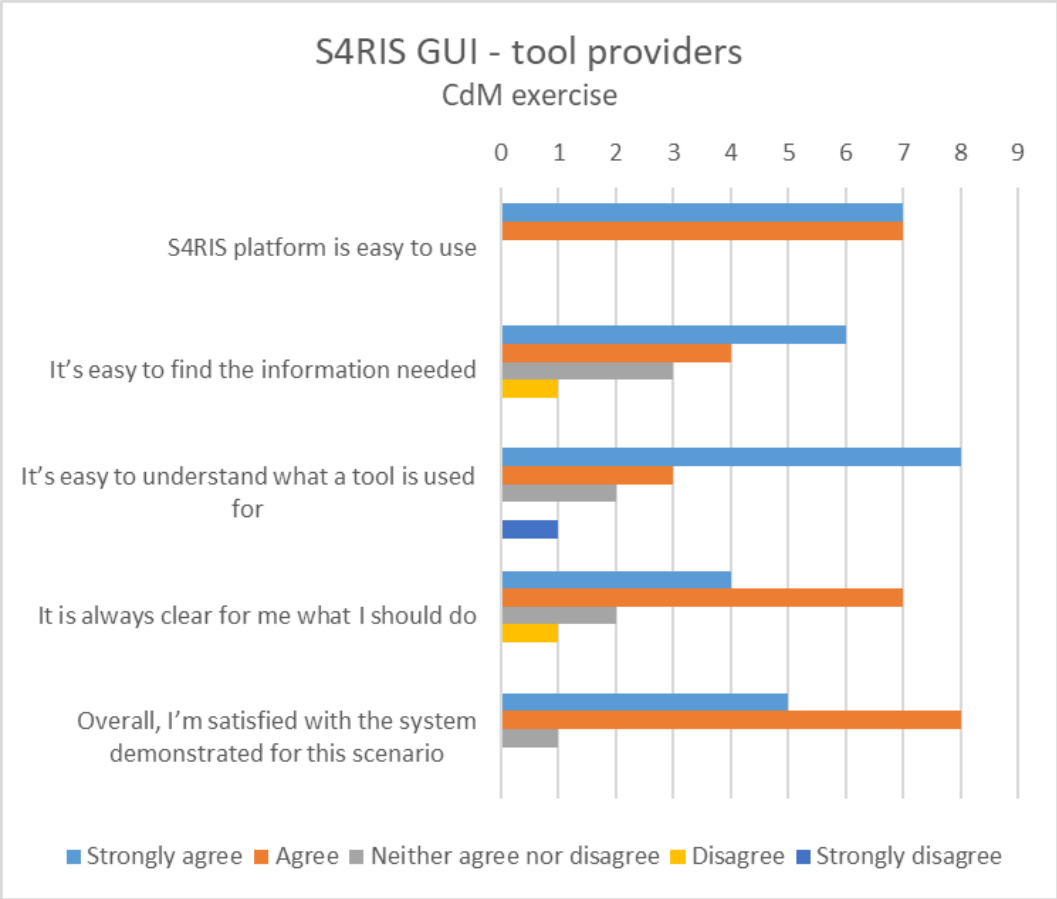
- I think the platform would need a clearer homepage with at least one or two sentences that briefly explain the content of tools and their objective. Additionally, the user interface could be redesigned in a more attractive way. Last point: I think it could be great to allign the graphics of all the differente tools in S4RIS platform
- I should use it directly before saying anything about improvements

What could be improved to make the handling more transparent?

- I think the platform would need a clearer homepage with at least one or two sentences that briefly explain the content of tools and their objective. Additionally, the user interface could be redesigned in a more attractive way. Last point: I think it could be great to allign the graphics of all the differente tools in S4RIS platform
- I should use it directly before saying anything about improvements
- divide the tools according the resilience phase

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- I should use it directly before saying anything about improvements



What could be improved in the GUI?

- This can be accomplished by adding new features and updating them on a regular basis.
- The flow in the screens from UEx perspective
- MOre functionalities (e.g. common dashbaords); single sign-on
- To have all buttons in a window page wuthout the need of scolling
- show clearer in which situations which tools could be used with clearer instructions of the combined use
- First time users might have some difficulty in using some tools. Means of offering extra help might be beneficial, e.g. overlaid comments/suggestions.
- The GUI improved a lot in being user-friendly since the Rome exercise. This should be continued in inserting more information boxes with information for the tools and guiding the end-users what to do next.

What complexity / functions are not necessary and can be deleted or reduced?

- There is a better way to organize the tools than to categorize them according to their functionality, as well as to establish a more productive relationship between related tools by categorizing them according to their phases.
- Some of the provided tools provide overlapping functionality
- No one
- No suggestions
- Nothing is not necessary at the moment...

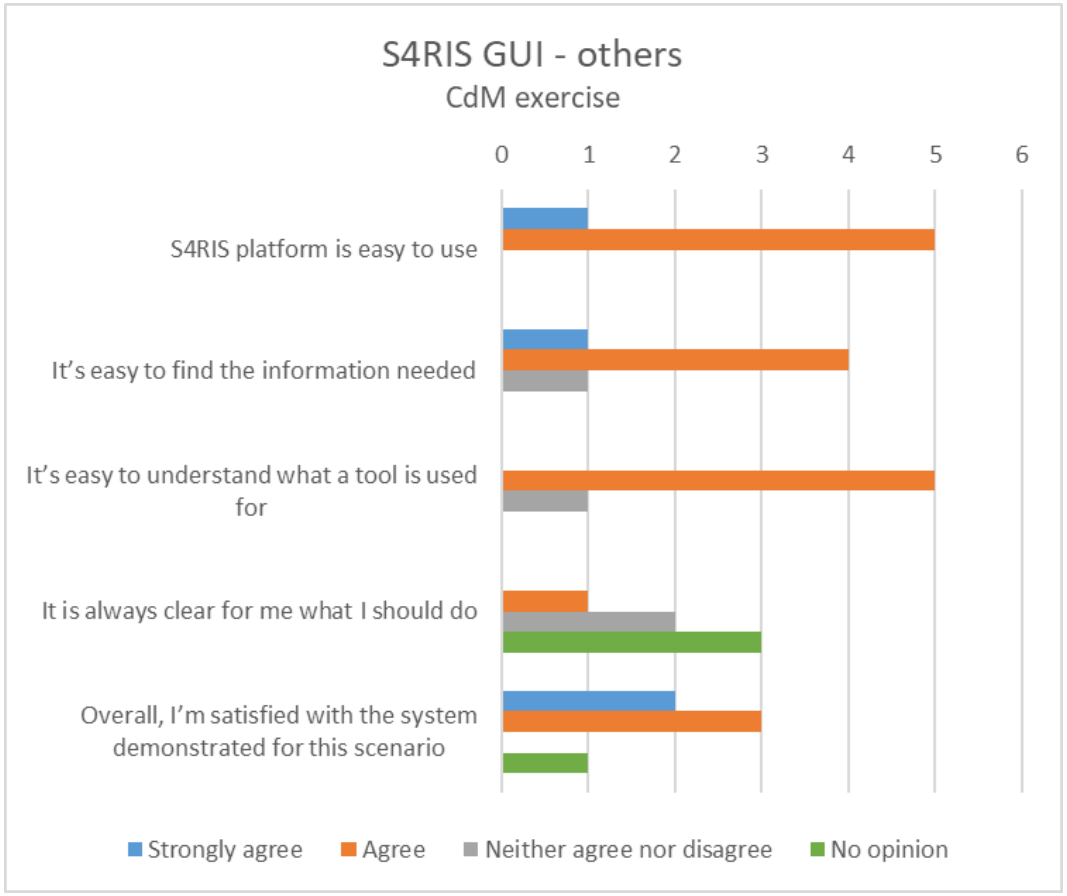
What could be improved to make the handling more transparent?

- user manual and training or tutorials of the end-user. Let the end-users play with the tools
- No suggestions
- Inserting more information boxes with information for the tools and guiding the end-users what to do next - especially on the registration page and on the register page - there should be an information about the requirements of the password.

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- The project can meet the needs of the end-user by updating the features and generating revised versions of the platform in order to satisfy their requirements.
- Developing a digital twin system for automated and intelligent monitoring and maintenance of railway asset
- Single sign-on to facilitate user login (no multiple logins needed)
- make the interface more attractive
- a feature to scheck the synchronisation of the assets list between CAMS and SecuRail

	• No suggestions • To be a bit more user-friendly by inserting more information guiding the end-user - see tipps above.



What could be improved in the GUI?

- Clearer identification of individual tool functionalities
- Did not see in presentation - description of which tools are generally proposed as suitable for which resilience phases?

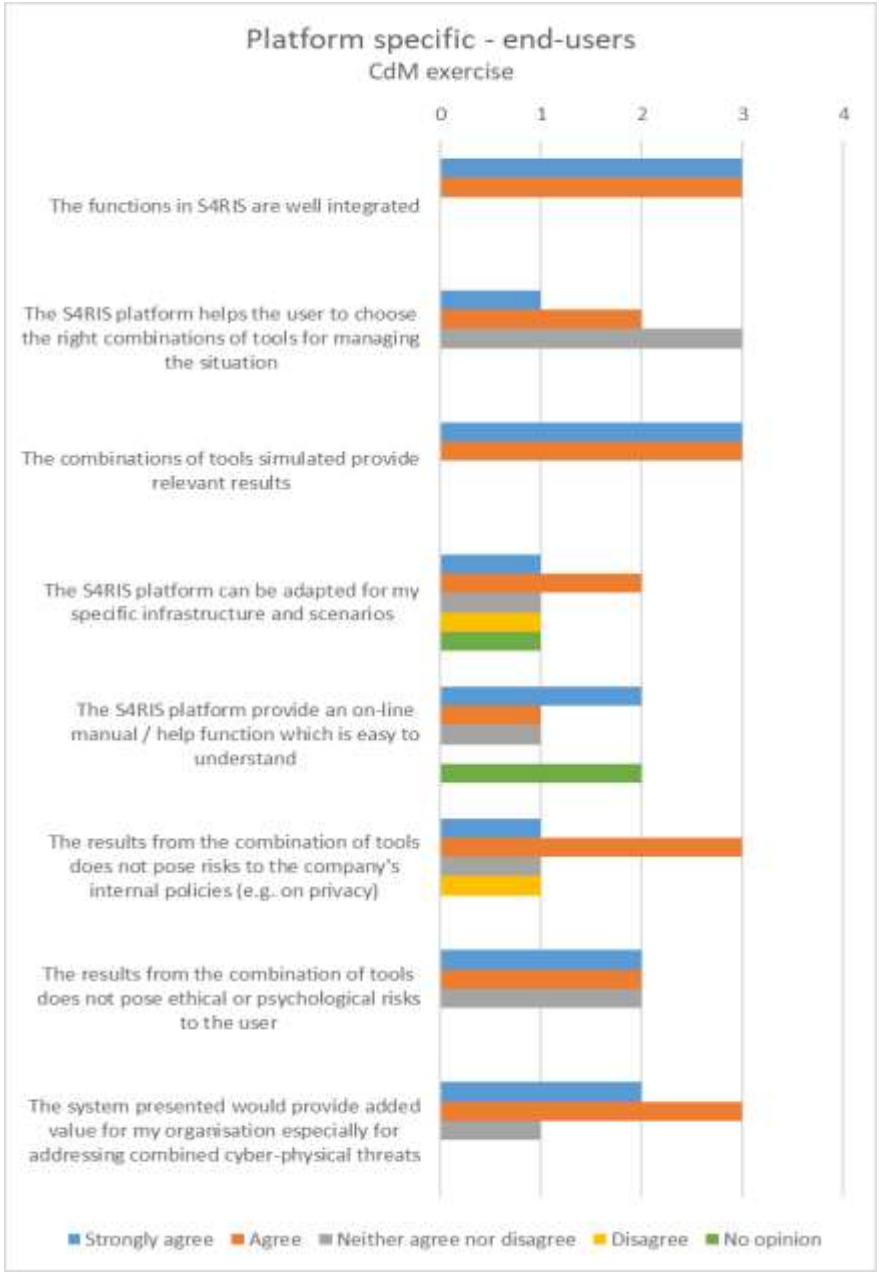
What complexity / functions are not necessary and can be deleted or reduced?

What could be improved to make the handling more transparent?

- Which pieces of information in the integrated (DMS) system get processed/consumed by which tool, how much the tools (outputs) are relying/depending on that specific information/alert (or the lack of that).
- This question seems more relevant for the contributory tools rather than the S4RIS GUI
- Transparent login to other tools in the S4RIS platform

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

CDM PLATFORM SPECIFIC QUESTIONNAIRE 3



Were there situations where you did not understand what the system was doing?

- No all situations were clear

Would you recommend the system presented to your colleagues and why?

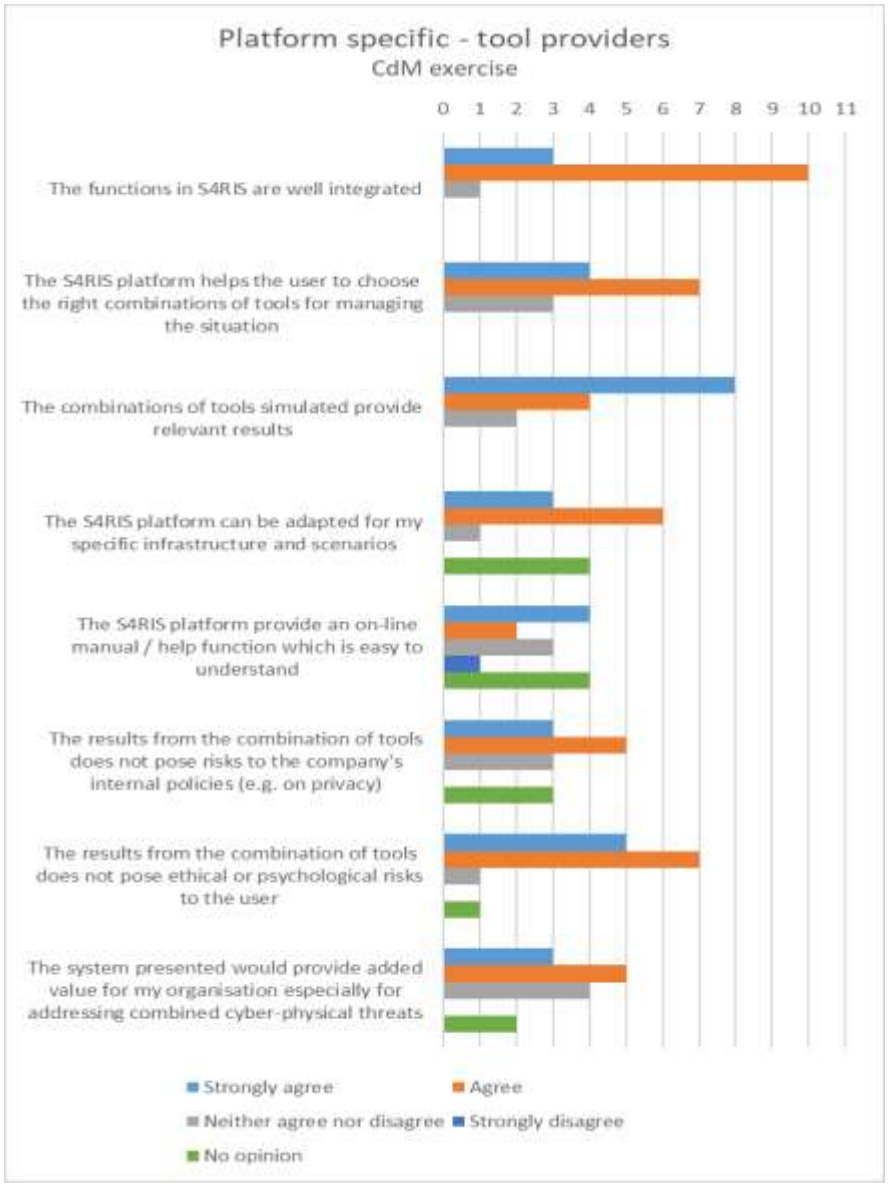
- Yes I would because of its strategic functioning
- I should use it directly before saying anything about this
- yes the integration of the different tools help to increase the resilience of the overall system
- I would recommend to follow the advances and to provide feedback in order to increase the global TRL.
- Yes since the S4RIS platform is a good example of how large numbers of heterogeneous tools can be integrated to provide added value with regards to the security and resilience of railway stations.

What could be improved in the context of this scenario?

- The communication part
- The data and information should be more precise and therefore previsions and reliability will be more useful for the Municipality
- bette r address how to communicate to the citizens and stakeholders involved in the crisis management
- A comparison between the scenario happening with the current end-user procedures and the implementation of S4RIS would help understand the added value brought by S4RIS

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- Focus more on end-user's perspectives. The addition of training programmes/manuals for end-user companies could help, but I guess this is another project.



Were there situations where you did not understand what the system was doing?

- The situation is clear and unambiguous.
- There were situation where it was not transparent how the system was doing, rather than what it was doing
- The differences between the "risk analysis" tools SecuRail, CAMS, and SARA are not always clear. I think there is an opportunity for better interplay and integration between these tools.
- No - since it was explained. But I am not sure, if the web applications of the tools are intutive enough for the end-users to use by their own.

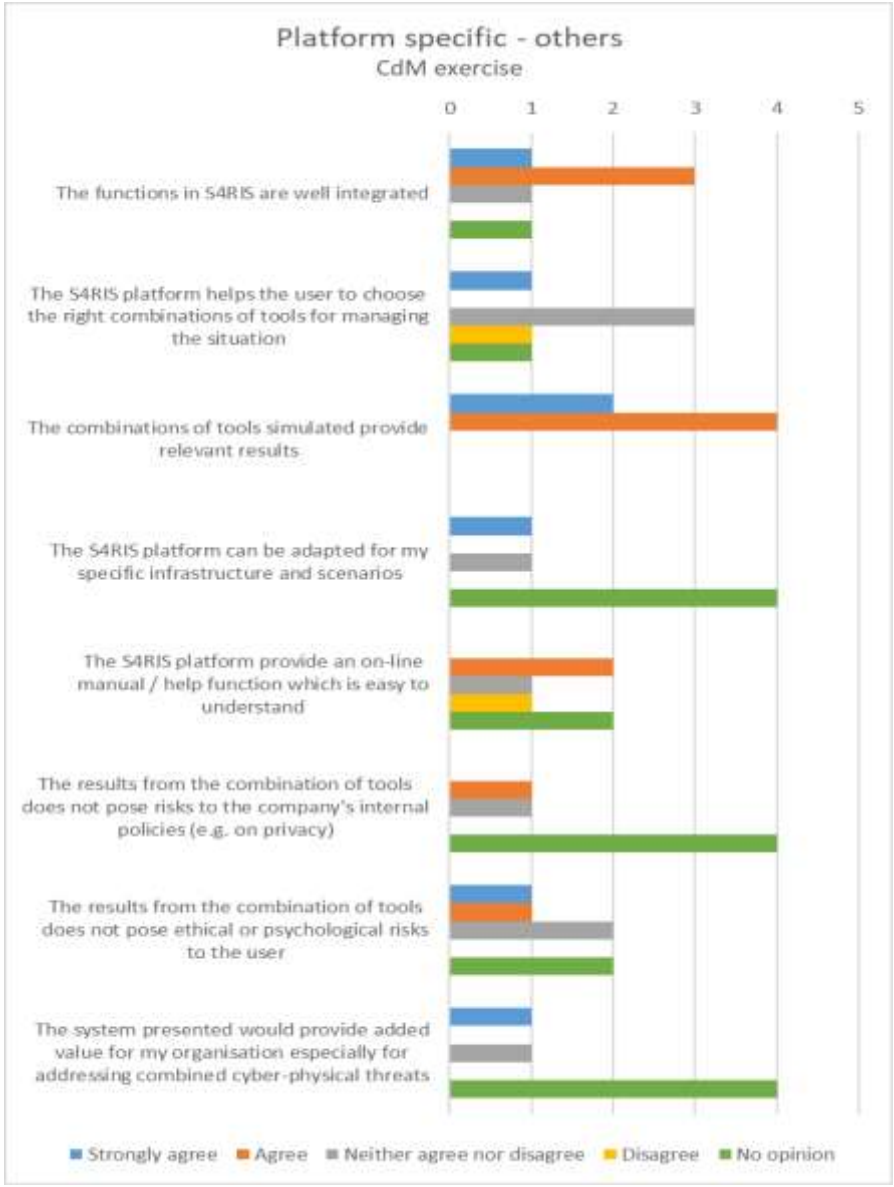
Would you recommend the system presented to your colleagues and why?

- As a result of the integration, multiple tools are involved in different phases of prevention, detection, response, and recovery, so it could also be useful for others.
- Yes, in general it provides a full toolkit fo functionalities that monitor relevant information
- Yes, to have a complete platform to cope with cyber and physical threats in every phase
- Yes, great resource
- yes, because it delivers a interesting combination of toolsets
- Not in its current form. Tolls are still loosely connected and safety of info exchange is not very clear.
- Yes, for specific situations, but they would need help in the form of e.g. a user manual and first steps as presented by DATAFAN

What could be improved in the context of this scenario?

- In order to improve the context of the scan, we need a dynamic database that combines both historical data and real-time data from the users, and we need to integrate all tools that are used during the analysis, and comparing tool outputs of all related phases and incidents in a single review will be more effective.
- To enahnce data exchange
- the decisions that S4RIS would have facilitated the stakeholder, i.e. for which problem would S4RIS have helped in the decision making.
- Tighter integration in the context of secure data and info exchange. Might be advisable to host all tools at the premises of the customer.
- To make the results more realistic and transparent by showing which data are EXACTLY used - the real data that we got from the end-users or only artificial data.

	Any proposals for revisions and/or additions to the requirements and specifications defined to date? • Updating in specific time and integrating tools as well as understanding a dynamic database that combines historical data and real-time data from users, as well as integrating all tools used during analysis, and comparing tool outputs of all phases to incidents in one review. • Single sign-on; • A user manual and /or tutorial to guide the users through a realistic scenario - as presented by DATAFAN.



Were there situations where you did not understand what the system was doing?

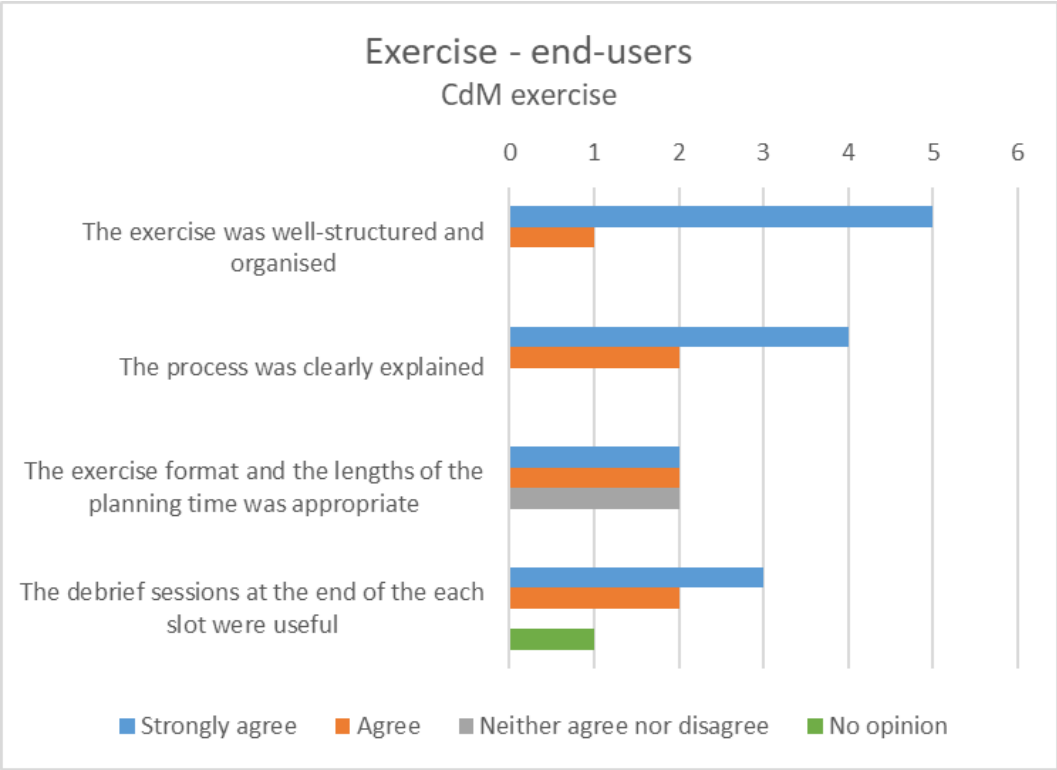
Would you recommend the system presented to your colleagues and why?

What could be improved in the context of this scenario?

- Wrote disagree under "The S4RIS platform provide an on-line manual..." and "The S4RIS platform helps the user to choose the right combinations of tools for managing the situation" as not presented / demonstrated. (Also most contributory tools did not identify help/manuals (DATAFAN was an exception identifying availability of manual)

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

CDM EXERCISE EVALUATION QUESTIONNAIRE 3



Which part of the exercise did you find the most useful and why?

- The whole development, seeing all the tools working and communicating together
- joint simulation that demonstrate the integration of the tools
- The live tool demonstrations, because it facilitates the understanding of the tools.

Were there any parties missing whose participation would have given added value for the exercise?

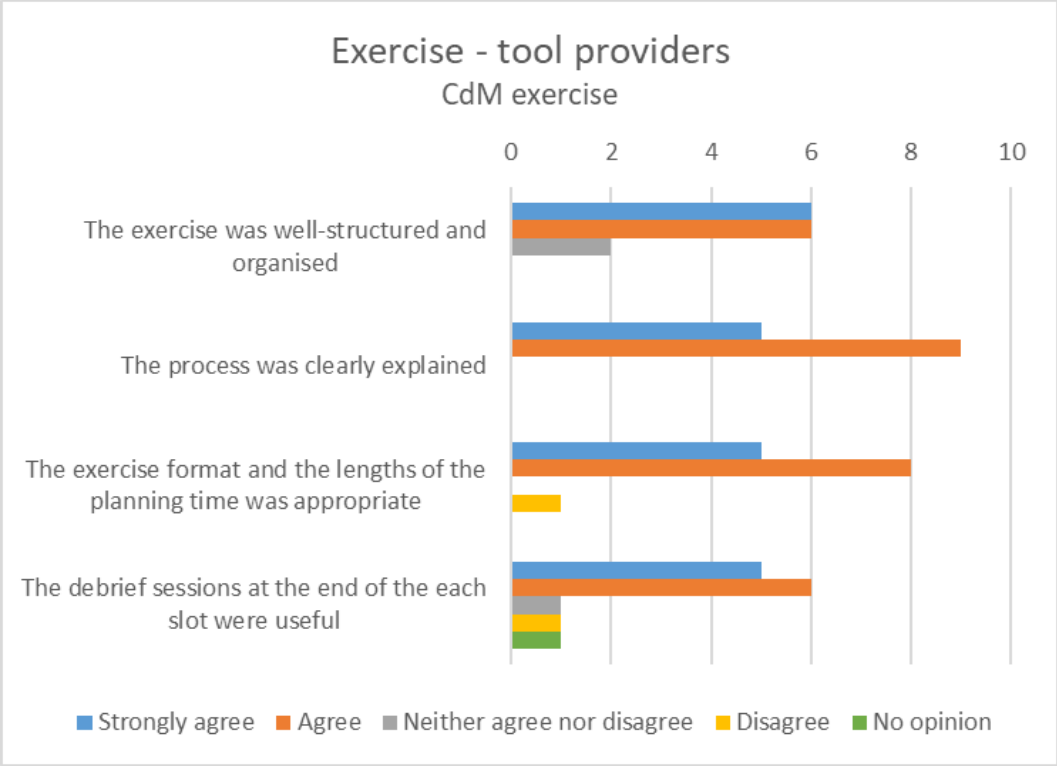
- Additional stakeholders linked to Comune di Milano
- the transport companies (stakeholders)
- Perhaps more end-users representatives

What can be done differently for the next exercises or what improvement need to be made?

- I would suggest to design the Simulation exercise to be more interactive with participants
- Next exercise could have more time for preparation and data collection
- I would suggest to make more debriefing questionnaires, but shorter. Right after each tool demonstration, a questionnaire. I think it might help the responders to focus more on each tool.

What are the main lessons learnt for you and why?

- always rely on rehearsal phase :)
- Data availability is essential for the efficiency of the tools - training is needed to use the tool in an efficient way –
- Crisis management is multifactorial and has many stakeholders involved. It is useful to work on a centralised tool like S4RIS to realise this and to learn where should the efforts go.



Which part of the exercise did you find the most useful and why?

- The project was greatly benefited by participating in a number of tools.
- Joint exercise
- Both. Presenting tools prior to demos allowed for better understanding of the latter ones.
- All - first explaining the scenario - also by the host CDM - then explaining the tools and their specifications to the sceanario and then the debriefing session. But the debriefing session was to short - there should be more time please to get more specific answers.

Were there any parties missing whose participation would have given added value for the exercise

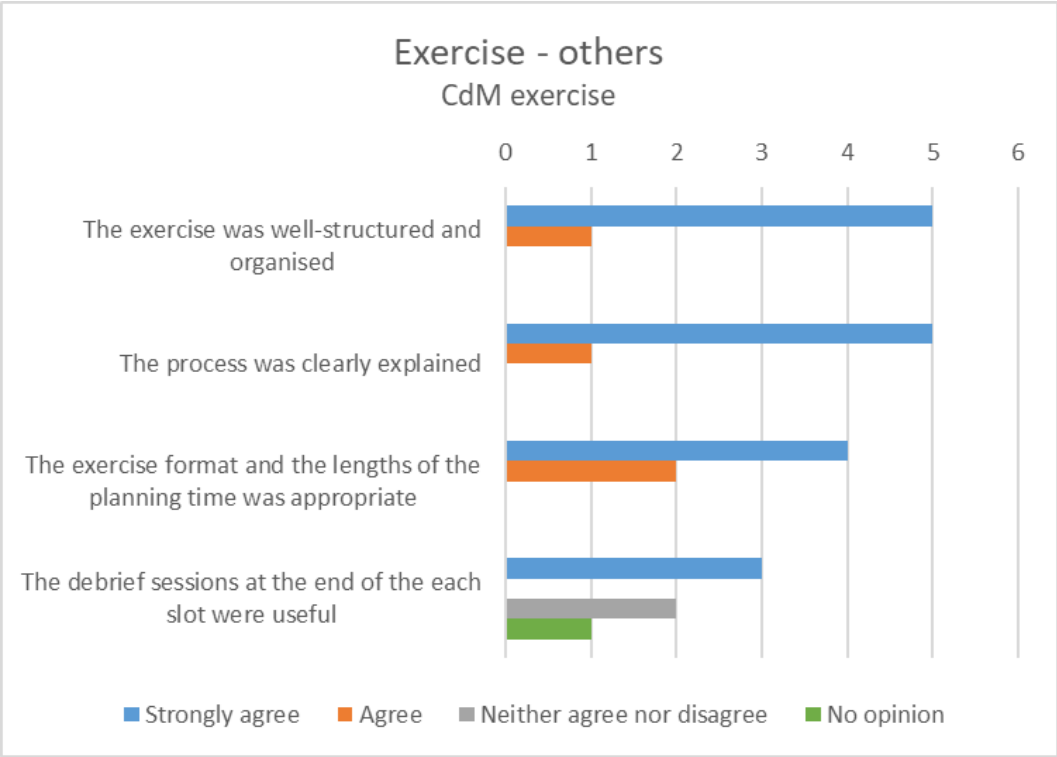
- MOre tools on recovery
- More stakeholder or advisors participating and direct stakeholder/advisory feedback after each session (the good and the bad feedback)
- Yes, Intracom. Our tools could have offered added value.
- The members and experts of the Advisory Board in presence were missing.

What can be done differently for the next exercises or what improvement need to be made?

- organization of the event at the actual premises of where the exercise targets (e.g. railway stations)
- The different phases with respect to the scenario could be made clearer; an open discussion after the a phase or after the questionnaire would increase the involvement persons in giving different feedback.
- More time for the debriefing session and inviting the members of the Advisory Board in presence and early in time and funding their travel costs.

What are the main lessons learnt for you and why?

- The project was greatly benefited by participating in a number of tools.
- Combination of tools can be successfully demosntrated if a clear flow of events is defined
- The feedback for the questionnaire could be better. It would be now very interesting to know, how many people responded who participated online and how many people who participated in presence.



Which part of the exercise did you find the most useful and why?

- All equally relevant and valuable.

Were there any parties missing whose participation would have given added value for the exercise?

- Additional contributory tools which in principle could have been part of the scenario; demonstrating also their live connection to the S4RIS GUI and DMS.

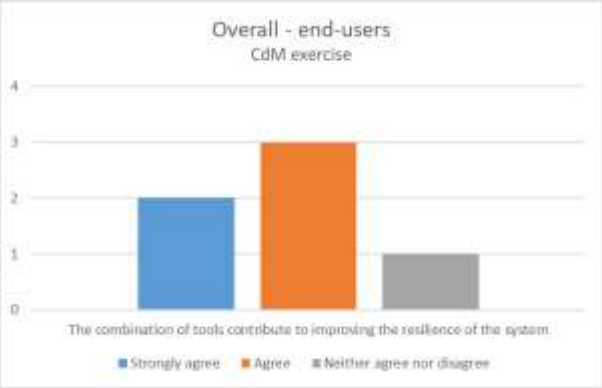
What can be done differently for the next exercises or what improvement need to be made?

- Next possibility would be at final event. Combination of more of the contributory tools. Further demonstration of DMS publish/subscribe e.g. SeucRail asset topology list + CuriX.

What are the main lessons learnt for you and why?

- Remote/online participation cannot completely substitute for actual presence, live discussions (especially the informal parts).
- Demonstration of the SAFETY4RAILS approach incl. S4RIS platform architecture with S4RIS GUI and DMS working in live geographically distributed environment.

CDM OVERALL QUESTIONS QUESTIONNAIRE 3



Which capabilities are the most important/useful for this scenario?

- the capability of predicting costs and impacts per each scenario, so that it can be easily translated in preferring one choice to another
- early detection of the flod and its consequences to be able to react as soon as possible and evacuate people
- The detection tools

What are the current obstacles for adopting such a system?

- Different stakeholders involved with their own tools. Integration of different systems.
- The municipality is just one actor, the major obstacle is about having three different management systems still working on different paths and not taking one single managerial orientation
- availability of data especially asset inventory
- The internal procedures, manners and culture of the railway operators (end-users), which have been established for years and decades. Additionally, the legislation for safety and security needs to be complied, which leads to more work.

What could be improved in the context of this scenario?

- Collect more data and refine information
- include the communication to the public and how the tools can help
- Comparison between the current end-user procedures reacting to this scenario with the S4RIS implementation

Has any limitation of tools been discovered during the exercise? If so, please specify.

- I have not enough information for answering by now
- tools are very linked to the data/sensors that are available :- level of water and how it evolve on the network could be useful - how to adapt the installations to protect some of them from the flood

What is the overall added value as may be assessed from your own experience in your current daily work?

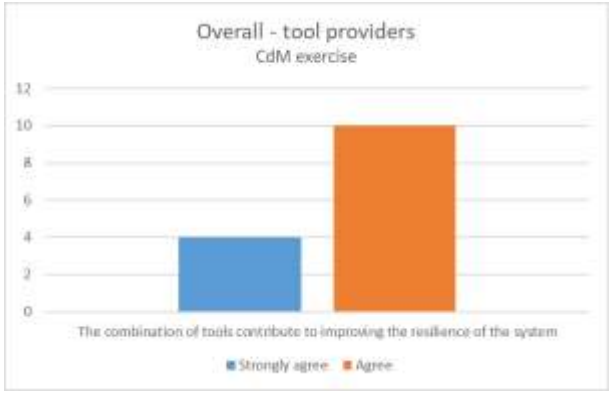
- The opportunity to make a clear assessment of each mitigation/management measure by its impact or cost

What were the main lessons learnt by you and why?

- the difficulties to put together different management approach between different companies

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- Already responded this in the previous questions. Thanks!



Which capabilities are the most important/useful for this scenario?

- Integration of tools, categorization of scenarios.
- prevention (prediciton of events)
- Prevention
- the combination of detection and response measures
- Cyber-physical detection and rapid threat/risk mitigation.
- To insert the output of other tools as input data and work with them

What are the current obstacles for adopting such a system?

- End-users do not have access to real-time data from the system.
- Event based integration (individual tool communication) and a combined information brief on the S4RIS platform
- The whole systems needs to undergo a pilot phase where it actually gets installed at an infrastructure with real administrators to provide feedback
- Lack of data concerning features of assets (cost, position, etc)
- seamless integration with the normal functionalities of the end-user
- Ability to convince customers about the reliability of info and knowledge produced and offered to them. Safety and security of such systems, such that they do not add extra risk factor to customer system operation are always issues for potential customers in such domains.
- Data protection and licening rights since it is still under construction

What could be improved in the context of this scenario?

- The more imaginary incidents we add to the list, the more complicated the cyber and physical incidents will become.
- More focus on natural hazards
- the scenario was very specific where a lot of the tools are not primarily equipped for this kind of scenario, i.e. a lot of tools were not fitting in the scenario
- To be more specific for the scenarios to use the real data that we got in the project - since we got any.

Has any limitation of tools been discovered during the exercise? If so, please specify.

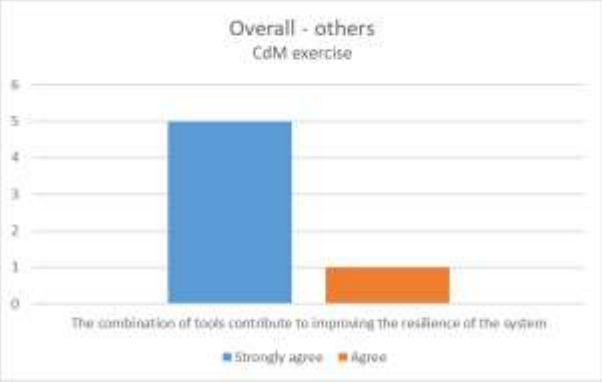
- Having access to historical data and real-time data was a big challenge for our tool..
- some lack of synchronization among tools (but it is challenging, each tool has its own data model)
- rather the limitation of the tools not partcipating
- No, not to my knowledge.

What is the overall added value as may be assessed from your own experience in your current daily work?

- Being able to work with many participants at the same time and different tolls at the same time is a great advantage.
- Having an unique platform covering all the phases of resilience
- Some ideas for improving our own tools
- The combination and collaboration of various tools in a specific event.

What were the main lessons learnt by you and why?

	• By utilizing integrated tools within DMS for prevention, detection, response, and recovery, the end-user can save time and money by using integrated tools within DMS. • Being concrete is better for end-users to make them understanding benefits of tools • There is a strong need for such a platform, expecially in the crisis communication. Any proposals for revisions and/or additions to the requirements and specifications defined to date? • Periodically updating all versions of the tools and testing them in KAFKA, as well as making multi-language environments for end-users, could be helpful.



Which capabilities are the most important/useful for this scenario?

What are the current obstacles for adopting such a system?

What could be improved in the context of this scenario?

Has any limitation of tools been discovered during the exercise? If so, please specify.

What is the overall added value as may be assessed from your own experience in your current daily work?

What were the main lessons learnt by you and why?

- A proper balance between the level of integration "under the hood" and transparency of processing of raw/source data, and the process pipeline should be kept for systems/architecture design/engineering/analysis.

Any proposals for revisions and/or additions to the requirements and specifications defined to date?

ANNEX XIII Assessment of how far the CdM scenario objectives were met based on evaluation

The correspondence of the evaluation results with the objectives set for the tools in each exercise phase is presented in following tables. In the estimation of the achievement of objectives the following classification has been used:

- Fulfilled according to the majority – more than half of the respondents have answered “strongly agree” or “agree” to question “The objective was successfully met”
- Partially fulfilled according to the majority – half of more of the respondents have answered “neither agree nor disagree” to question “The objective was successfully met”
- Not fulfilled according to the majority – more than half of the respondents have answered “disagree” or “strongly disagree” to question “The objective was successfully met”

WARNING: The “good faith” evaluation is based on the data provided in the Annex XII which can include only limited responses and was based on what was seen at the simulation exercise.

CdM SIMULATION EXERCISE - REQUIREMENTS FOR THE PREVENTION PHASE

Tool	**Objective for the CdM exercise**	**Integrated in S4RIS (Y/N)**	**Result of evaluation**
CaESAR	• Identification of critical stations/components based on a grid representation of the metro network • Stochastic simulation of various what-if scenarios to identify critical combinations of threats and impacted stations/components	Y	Fulfilled according to the majority

Tool	Objective for the CdM exercise	Integrated in S4RIS (Y/N)	Result of evaluation
SECURAIL	• Allow risk analysis of the metro infrastructure to understand the level of risk for each critical asset for a given hazardous event	Y	Fulfilled according to the majority
DATAFAN	• Prediction of the expected number of passengers for a given target station (here: Milan Porta Garibaldi) and its surrounding stations based on historical time-series data. • Analysis of events with large crowd concentrations (here: Olympic opening ceremony) using what-if scenarios that affect the free capacity of the target station (e.g. due to the closure of a station).	Y	Fulfilled according to the majority
SARA	• Definition of the physical model of the station, for both the structural and equipment part • Description of the people ingress in the station, both for departures and arrivals. • Definition of each scenario, which consist on the definition of the threats and the damage caused on the structural part and on the equipment components. • Definition of different kind of mitigation measure, as hardening, replacing and redundancy of the equipment component. • Evaluation on the economic loss due to direct damage on structure, analysis of the cascading effect on the equipment, computation of the service interruption and/or reduction and its relative economic indirect loss, and at last the evaluation of the affected people and the relative equivalent economic loss.	Y	Fulfilled according to the majority

CdM SIMULATION EXERCISE - REQUIREMENTS FOR THE DETECTION PHASE

Tool	**Objective for the CdM exercise**	**Integrated (Y/N)**	**Result of evaluation**
CuriX	Data regarding the consumption of electric energy and/or voltage levels are monitored, which can be collected from smart meter devices collecting data from the power supply system for the Porta Garibaldi station. Using the anomaly detection capabilities of CuriX on the monitored data, an anomalous behaviour is detected due to the blackout and a corresponding alarm is raised. Additional data from other systems may be monitored, such as the ticketing system and lighting. The latter is also operational during a blackout due to auxiliary power supplies or uninterruptible power supplies.	Y	Fulfilled according to the majority
WINGSPARK	• Train speed anomaly identification • Estimated crowd concentration and alerting when the people density exceeding predefined thresholds • Provide evacuation guidelines	Y	Fulfilled according to the majority

CdM SIMULATION EXERCISE - REQUIREMENTS FOR THE RESPONSE PHASE

Tool	**Objective for the CdM exercise**	**Integrated (Y/N)**	**Result of evaluation**
CaESAR	• Quantified resilience assessment based on performance-time curves for the threats of the exercise and estimation of resilience indicators • Comparison of certain mitigation measures (as defined in the exercise) to reduce the impact of the threats of the exercise • Visualization of the model, the impact propagation based on different concepts (connectivity based, agent-based) and the resilience assessment	Y	Fulfilled according to the majority
WINGSPARK	• The objective of WINGSPARK is to forward the alerts to RAM2 in case the specified thresholds have been exceeded and provide evacuation guidelines to ease the situation.	Y	Fulfilled according to the majority
RAM2	• Reception via interface with DMS of the alarms provided by the tools, relating to the events of the scenario. • Display of alarms with description of possible mitigation actions	Y	Fulfilled according to the majority

CdMSIMULATION EXERCISE - REQUIREMENTS FOR THE RECOVERY PHASE

Tool	**Objective for the CdM exercise**	**Integrated (Y/N)**	**Result of evaluation**
CAMS	• Providing accurate recovery cost for assets involved in a sudden event through the assessment of final assets damage. The final damage is assessed using the initial condition (before incident) and the impact measure of the specific incident on the asset. The end-user is then provided with a budget needed to restore the service. • As well prediction of normal deterioration due to aging of railway assets in the system considered, Maintenance and repair budget calculation for railway components • In this scenario CAMS used to inform the station operator on the budget to allocate to repair, maintain, and rehabilitate the infrastructure after a set of possible events.	Y	Fulfilled according to the majority

ANNEX XIV Good faithassessment of D1.4 requirements/specifications test coverage in SEs

ID	SimulationExercise
MA	Madrid
A	Ankara
R	Rome
MI	Milan

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

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
1	S4RIS platform specific	P-01	Platform modularity	Essential	x	x	x	x		x			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.
2	S4RIS platform specific	P-02	Consolidation of end-user inputs	Conditional						x			In principle possible via the Distributed Messaging System (DMS) with publish/subscribe.
3	S4RIS platform specific	P-03	End User configuration	Essential							x		The indication is that end-users would need support for the deployment of the S4RIS platform and the (chosen) contributory tools.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
4	S4RIS platform specific	P-04	Minimum requirements for S4RIS use	Essential							x		
5	S4RIS platform specific	P-05	Identification of useful S4RIS contributory tool combinations	Essential	x	x	x	x		x			Partially identified for SEs during the project.
6	S4RIS platform specific	P-06	Data exchange – end user sources to S4RIS	Essential						x			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	S4RIS platform specific	P-07	Data exchange – S4RIS to end-users	Essential						x			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	S4RIS platform specific	P-08	Data exchange – Between S4RIS tools	Essential	x	x	x	x		x			Possible via the Distributed Messaging System (DMS) with publish/subscribe. Not tested for all tools.
9	S4RIS platform specific	P-09	Synchronisation	Essential						x			In principle possible via the Distributed Messaging System (DMS) with publish/subscribe.
10	S4RIS platform specific	P-10	Input quality check	Essential							x		
11	S4RIS platform specific	P-11	Self-diagnostics	Essential							x		
12	S4RIS platform specific	P-12	Archive	Essential						x			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.

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
13	S4RIS platform specific	P-13	Data integrity	Essential							x		
14	S4RIS platform specific	P-14	Data authenticity	Essential							x		
15	S4RIS platform specific	P-15	Manual	Essential						x			Individual contributory tools providing varying degress of manuals and/or on-line help.
16	S4RIS platform specific	P-16	Skill / training	Essential								x	
17	S4RIS platform specific	P-17	Security	Essential								x	The focus on the project was on demonstrating the potential of the S4RIS. Detailed security requirements will be fulfilled in the time after the end of the project before market introduction. Specifications for security of the platform and tools can be found in the standards section.
18	S4RIS platform specific	P-18	Public accessibility	Optional						x			The basic S4RIS GUI access page is available but there is no detailed information available publicly to date.
19	S4RIS platform specific	P-19	Global unique identification of entities	Essential	x	x	x	x		x			Partially achieved for the specific SEs where there was communication via the DMS.
20	S4RIS platform specific	P-20	Messaging System	Essential	x	x	x	x		x			DMS implemented - not all tools tested
21	S4RIS platform specific	IO-1 (P-18 above)	Data exchange – Between S4RIS tools	Essential	x	x	x	x		x			DMS implemented - not all tools tested

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
22	S4RIS platform specific	IO-2 (P-09 above)	Synchronisation	Essential						x			In principle possible via the Distributed Messaging System (DMS) with publish/subscribe.
23	S4RIS platform specific	P-21 (IO-3 in D2.3)	Data exchange with end-users' system	Essential						x			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. In principle possible to download to existing tools via the Distributed Messaging System (DMS) with publish/subscribe.
24	S4RIS platform specific	P-22 (IO-4 in D2.3)	Data exchange – Upload already existing data in the S4RIS	Essential	x	x	x	x		x			Achieved through upload to individual contributory tools as relevant
25	S4RIS platform specific	P-23 (IO-5 in D2.3)	Data exchange format for the S4RIS	Essential						x			Provided through DMS solution and JSON formats agreed for individual SEs
26	S4RIS platform specific	P-24 (IO-6 in D2.3)	The S4RIS shall provide a possibility to connect to not specified systems	Essential						x			Provided through DMS solution and JSON formats agreed for individual SEs
27	Knowledge / Usability	EU+U01	Usability	Essential	x	x	x	x		x			Based on the answers to questionnaires. Additional time for testing the system by the end-users required.
28	Graphical User Interface - GUI	GUI-R01	Web-based interface	Essential				x	x				
29	Graphical User Interface - GUI	GUI-R02	Login page	Essential				x	x				

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
30	Graphical User Interface - GUI	GUI-R03	Single point of access to the tools	Essential				x		x			This functionality has been delivered and demonstarted in the S4RIS GUI for those tools with their own GUI in a web application and thepossibility to download .exe programmes has been demonstrated.
31	Graphical User Interface - GUI	GUI-R04	Grouping of tools	Essential				x			x		
32	Graphical User Interface - GUI	GUI-R05	How to launch tools	Essential				x		x			
33	Graphical User Interface - GUI	GUI-R06	Display of tools based on user role	Essential								x	
34	Graphical User Interface - GUI	GUI-R07	Tools keywords and short descriptions	Essential				x	x				Functionality delivered, descriptions subject to update.
35	Graphical User Interface - GUI	GUI-R08	Log-out button	Essential						x			
36	Graphical User Interface - GUI	GUI-R09	Home page button	Essential				x	x				
37	Graphical User Interface - GUI	GUI-R10	Account management -	Essential								x	

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
38	Graphical User Interface - GUI	GUI-R11	Settings and configuration	Essential								x	
39	Graphical User Interface - GUI	GUI-R12	Language	Essential	x	x	x	x			x		
40	Graphical User Interface - GUI	GUI-R13	Bar with additional functions	Conditional				x			x		
41	Graphical User Interface - GUI	GUI-R14	Opening web-based tools	Essential				x	x				
42	Graphical User Interface - GUI	GUI-R15	Opening desktop tools	Essential								x	
43	Graphical User Interface - GUI	GUI-R16	Opening CLI tools	Conditional								x	
44	Graphical User Interface - GUI	GUI-R16a	Opening CLI tools - BB3d	Conditional								x	
45	Graphical User Interface - GUI	GUI-R16b	Opening CLI tools - CaESAR	Conditional								x	No longer relevant as CaESAR delivered a web application GUI

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
46	Graphical User Interface - GUI	GUI-R16c	Opening CLI tools - SARA	Conditional								x	
47	Graphical User Interface - GUI	GUI-R17	User confirmation on certain actions	Essential							x		
48	Graphical User Interface - GUI	GUI-R18	Font type and size	Conditional				x	x				
49	Graphical User Interface - GUI	GUI-R19	Error display	Essential								x	
50	Graphical User Interface - GUI	GUI-R20	S4RIS account creation	Optional				x	x				Not tested in simulation exercises
51	Graphical User Interface - GUI	GUI-R21	Help and documentation	Conditional				x			x		
52	Graphical User Interface - GUI	GUI-R22	Frequently/recently used tools	Optional							x		
53	Graphical User Interface - GUI	GUI-R23	Dashboard	Conditional				x		x			Individual tools GUIs available as iFrame or in new Tab (if individual tool has web application).
54	Graphical User Interface - GUI	GUI-R24	Mobile interface	Conditional								x	

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
55	Graphical User Interface - GUI	GUI-25	S4RIS public accessible part optimized for mobile devices	Conditional								x	
56	Standards	STD-R01	Human user identification and authentication	Essential								x	Not assessed as part of WP8.
57	Standards	STD-R02	Human user identification and authentication - multifactor for remote connection	Conditional								x	Not assessed as part of WP8.
58	Standards	STD-R03	Human user identification and authentication - multifactor	Conditional								x	Not assessed as part of WP8.
59	Standards	STD-R04	Non-human user identification and authentication	Conditional								x	Not assessed as part of WP8.
60	Standards	STD-R05	Account management	Essential								x	Not assessed as part of WP8.
61	Standards	STD-R06	User account uniqueness	Essential								x	Not assessed as part of WP8.
62	Standards	STD-R07	Secure log-on	Essential								x	Not assessed as part of WP8.
63	Standards	STD-R08	Secure log-on feature 1	Conditional								x	Not assessed as part of WP8.
64	Standards	STD-R09	Secure log-on feature 2	Conditional								x	Not assessed as part of WP8.
65	Standards	STD-R10	Secure log-on feature 3	Conditional								x	Not assessed as part of WP8.
66	Standards	STD-R11	Secure log-on feature 4	Essential								x	Not assessed as part of WP8.
67	Standards	STD-R12	Secure log-on feature 5	Conditional								x	Not assessed as part of WP8.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
68	Standards	STD-R13	Secure log-on feature 6	Conditional								x	Not assessed as part of WP8.
69	Standards	STD-R14	Secure log-on feature 7	Conditional								x	Not assessed as part of WP8.
70	Standards	STD-R15	Secure log-on feature 8	Essential								x	Not assessed as part of WP8.
71	Standards	STD-R16	Password management	Essential								x	Not assessed as part of WP8.
72	Standards	STD-R17	Password management feature 1	Essential								x	Not assessed as part of WP8.
73	Standards	STD-R18	Password management feature 2	Essential / Conditional								x	Not assessed as part of WP8.
74	Standards	STD-R19	Password management feature 3	Conditional								x	Not assessed as part of WP8.
75	Standards	STD-R20	Password management feature 4	Conditional								x	Not assessed as part of WP8.
76	Standards	STD-R21	Public Key Infrastructure	Conditional								x	Not assessed as part of WP8.
77	Standards	STD-R22	Public Key authentication	Conditional								x	Not assessed as part of WP8.
78	Standards	STD-R23	Monitoring of access from untrusted networks	Conditional								x	Not assessed as part of WP8.
79	Standards	STD-R24	User access provisioning	Essential								x	Not assessed as part of WP8.
80	Standards	STD-R25	Information access restriction	Essential								x	Not assessed as part of WP8.
81	Standards	STD-R26	Identification and monitoring of access through wireless connection	Conditional								x	Not assessed as part of WP8.
82	Standards	STD-R27	Session lock	Essential								x	Not assessed as part of WP8.
83	Standards	STD-R28	Termination of remote sessions	Essential								x	Not assessed as part of WP8.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
84	Standards	STD-R29	Limit of contemporary sessions	Essential								x	Not assessed as part of WP8.
85	Standards	STD-R30	Audit of events related to security	Essential								x	Not assessed as part of WP8.
86	Standards	STD-R31	Audit storage	Conditional								x	Not assessed as part of WP8.
87	Standards	STD-R32	Alerting of audit process fail	Conditional								x	Not assessed as part of WP8.
88	Standards	STD-R33	Timestamp for audit	Essential								x	Not assessed as part of WP8.
89	Standards	STD-R34	Non-repudiation of users	Essential								x	Not assessed as part of WP8.
90	Standards	STD-R35	Access to audit information	Essential								x	Not assessed as part of WP8.
91	Standards	STD-R36	Information classification	Essential / Conditional								x	Not assessed as part of WP8.
92	Standards	STD-R37	Information classification scheme	Essential / Conditional								x	Not assessed as part of WP8.
93	Standards	STD-R38	Information labelling	Essential / Conditional								x	Not assessed as part of WP8.
94	Standards	STD-R39	Information labelling scheme	Essential / Conditional								x	Not assessed as part of WP8.
95	Standards	STD-R40	Protection of communications	Essential								x	Not assessed as part of WP8.
96	Standards	STD-R41	Dealing with errors in a secure way	Essential								x	Not assessed as part of WP8.
97	Standards	STD-R42	Information backup	Essential								x	Not assessed as part of WP8.
98	Standards	STD-R43	Recovery and restore	Essential								x	Not assessed as part of WP8.
99	Standards	STD-R44	Inventory of assets	Conditional								x	Not assessed as part of WP8.
100	Standards	STD-R45	Source code protection	Essential								x	Not assessed as part of WP8.
101	Standards	STD-R46	Infrastructure monitoring	Essential								x	Not assessed as part of WP8.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
102	Standards	STD-R47	Integration of a security incident tracking system form	Essential								x	Not assessed as part of WP8.
103	Standards	STD-R48	Overall security event / incident / vulnerability database	Essential								x	Not assessed as part of WP8.
104	Standards	STD-R49	Automatic correlation of different incidents detected	Conditional								x	Not assessed as part of WP8.
105	Standards	STD-R50	Security incident management system governance	Essential								x	Not assessed as part of WP8.
106	Standards	STD-R51	Attributes relevant for security incident management	Essential								x	Not assessed as part of WP8.
107	Standards	STD-R52	Collection of evidence before shutdown.	Essential								x	Not assessed as part of WP8.
108	Standards	STD-R53	Guidelines to inform who is responsible for internal and external communications	Essential								x	Not assessed as part of WP8.
109	Standards	STD-R54	Video Coding and metadata representation	Conditional								x	Not assessed as part of WP8.
110	Standards	STD-R55	Alerting protocol for emergencies	Conditional								x	Not assessed as part of WP8.
111	Data Protection	GDPR-R01	GDPR Compliance	Essential						x			GDPR provisions were respected for all SE activities. The tools and S4RIS platform itself partially provide this full functionality already or are prepared for providing features to fulfil this requirement in the product version.

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
112	Open source intelligence technologies for the S4RIS	OSINT_1	Data acquisition of OSINT	Essential	x	x	x			x			SE1-3 TISAIL (cyber threat), SE2-SE3 OSINT (none TISAIL, physical threat). Partially achieved marked as in WP8 all details of specifications not possible to evaluate.
113	Open source intelligence technologies for the S4RIS	OSINT_2	Pre-Processing and Analytics	Essential	x	x	x			x			SE1-3 TISAIL (cyber threat), SE2-SE3 OSINT (none TISAIL, physical threat). Partially achieved marked as in WP8 all details of specifications not possible to evaluate.
114	Open source intelligence technologies for the S4RIS	OSINT_3	Storage and representation	Essential						x			Partially achieved marked as in WP8 all details of specifications not possible to evaluate.
115	Open source intelligence technologies for the S4RIS	OSINT_4	Data set analytics	Conditional						x			Partially achieved marked as in WP8 all details of specifications not possible to evaluate.
116	Open source intelligence technologies for the S4RIS	OSINT_5	Data access and messaging	Essential						x			Partially achieved marked as in WP8 all details of specifications not possible to evaluate.
117	Blockchain technology	Blockchain_01	Technological requirements for the blockchain	Essential								x	Not assessed as part of WP8.

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
118	Blockchain technology	Blockchain_02	Data ingestion	Essential								x	Not assessed as part of WP8.
119	Blockchain technology	Blockchain_03	Data analytics	Optional								x	Not assessed as part of WP8.
120	Blockchain technology	Blockchain_04	Data access	Essential								x	Not assessed as part of WP8.
121	Railways in the Smart City	UR-SM-1	Enhanced coordination of the transport services available in the city	Essential								x	As stated in D1.4: "This requirement is not within the scope of SAFETY4RAILS and will not be covered in the project". Not assessed as part of WP8.
122	Railways in the Smart City	UR-SM-2	Adequate coordinated crisis management and support structures	Essential								x	As stated in D1.4: This requirement…. will be facilitated in SAFE-TY4RAILS." Not assessed as part of WP8.
123	Railways in the Smart City	UR-SM-3	Joint risk and threat assessment in transport hub.	*not specified*		x				x			As stated in D1.4: "Will only be covered to the extent that the transport hub's railway infra-structure and network can be modelled to perform a risk analysis." SE2 - CaESAR. Not assessed directly as part of WP8.
124	Railways in the Smart City	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								x	As stated in D1.4: "The tools and S4RIS platform itself will be prepared for providing fea-tures to fulfil this requirement in the later versions of product version." Not assessed as part of WP8.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
125	Railways in the Smart City	UR-SM-5	Signalisation in hub with several transportations modes and levels for passengers both under normal circumstances and during a crisis is key element in the overall system.	Conditional								x	As stated in D1.4: "The tools and S4RIS platform itself will be prepared to be easily interoperable with such communication system." Not assessed as part of WP8.
126	Railways in the Smart City	UR-SM-6	Cooperation between security providers in a hub.	*not specified*								x	As stated in D1.4: "The tools and S4RIS platform itself will be prepared to be easily interoperable with such cooperation platform" Not assessed as part of WP8.
127	Railways in the Smart City	UR-SM-7	Fostering communication/reporting about delays/ irregularities and common/coordinated reactions between different stakeholders of a common transport hub.	*not specified*								x	As stated in D1.4: "The tools and S4RIS platform itself will be prepared to be easily interoperable with such cooperation platform" Not assessed as part of WP8.
128	Railways in the Smart City	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*								x	As stated in D1.4: "Will not be covered within SAFETY4RAILS." Not assessed as part of WP8.
129	Railways in the Smart City	UR-SM-9	Provision of predictive information for joint crisis management with various stakeholders	*not specified*								x	As stated in D1.4: "Will not be covered within SAFETY4RAILS." Not assessed as part of WP8.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
130	Railways in the Smart City	UR-SM-10	Reliable communication means used by stakeholders.	*not specified*								x	As stated in D1.4: "Will not be covered within SAFETY4RAILS." Not assessed as part of WP8.
131	Crisis Management	UR-CM-R01	Adequate crisis management and support structures.	*not specified*	x	x	x	x		x			RAM2 in SE1-SE4 demonstrating ability to manage incident through its life cycle.
132	Crisis Management	UR-CM-R02	Cooperation between stakeholders.	*not specified*	x	x	x	x		x			Primarily a stakeholder organisational and interoperability requirement. S4RIS provided users with information which can be useful for cooperation with other security bodies based on available information and processing steps within S4RIS.
133	Crisis Management	UR-CM-R03	Clear definition of role and responsibilities.	*not specified*	x	x	x	x				x	The exercises have followed a scenario where the roles and responsibilities are clear. Not assessed as part of WP8.
134	Crisis Management	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*	x	x	x			x			As stated in D1.4: "The system infrastructure enables subject matter experts to define logic for risk assessment and business process workflows for emergency procedures."
135	Crisis Management	UR-CM-R05	Training and exercises.	*not specified*	x	x	x	x				x	As stated in D1.4: "Will not be covered." Not assessed as part of WP8.
136	Crisis Management	UR-CM-R06	Blast wave impact in case of an explosion.	*not specified*	x				x				See BB3d requirements/specifications no. 170-175.
137	Crisis Management	UR-CM-R07	Crowd simulation in case of an incident.	*not specified*	x	x			x				See iCrowd requirements/specifications no. 221-227.
138	Crisis Management	UR-CM-R08	Cascade effect simulation.	*not specified*	x	x	x	x	x				See CaESAR requirements/specifications no. 176-183.

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
139	Crisis Management	UR-CM-R09	Early warning systems to alarm in case of forecast problematic weather conditions to be implemented in all prevention tools.	*not specified*								x	As stated in D1.4: "The system architecture enables the interface to early warning systems." Not assessed directly as part of WP8.
140	Crisis Management	UR-CM-R10	Threat Intelligence.	*not specified*	x	x	x	x	x				See RAM2, WINGSPARK, CuriX, GANIMEDE, TISAIL/OSINT, DATA FAN, Senstation& TISAIL requirements/specifications below.
141	Crisis Management	UR-CM-R11	Detection of abnormal situation/anomalies regarding sensors, IT systems, assets, behaviour, forbidden objects, suspicious items, etc.	*not specified*	x	x	x	x	x				See RAM2, WINGSPARK, CuriX, GANIMEDE, TISAIL/OSINT, DATA FAN, Senstation& TISAIL requirements/specifications below.
142	Crisis Management	UR-CM-R12	Detection of combined attacks.	*not specified*	x	x	x		x				
143	Crisis Management	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*	x	x	x	x		x			See RAM2 requirements/specifications no. 235-241.
144	Crisis Management	UR-CM-R14	Harmonised reporting tool for exchanging information.	*not specified*	x	x	x	x		x			"Data exist in different formats" (NGT2). See RAM2 requirements/specifications no. 235-241.

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
145	Crisis Management	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*	x	x	x	x		x			As stated in D1.4: "The decision support system defines the severity level of the incident based on the input of the incident manager, who is defined as the incident assignee, this will be based on the guidelines included within the D3.5. Therefore, the severity level and the characteristics of the incident, as seen by all the stakeholders involved in the incident management, are one and the same." Not assessed directly with "both sides" as part of WP8.
146	Crisis Management	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*	x	x	x	x		x			As derived from D1.4: Monitoring tools have the capability to set or deal with parameters that influence alarming. Not assessed directly as part of WP8.
147	Crisis Management	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*								x	As derived from D1.4: Monitoring tools have the capability to set or deal with parameters that influence alarming. Not assessed directly as part of WP8.
148	Crisis Management	UR-CM-R18	The reporting from the Central IT Body or the Operation Centres.	*not specified*								x	As stated in D1.4: "The decision support system enables human in the loop decision making for the purpose of defining the incident's characteristics and the risks arising from it. The decision support system's reporting tools include an internal module for displaying the incident status to all stakeholders, as well as a mass notification system." Decision support system = RAM2. Not assessed directly as part of WP8.
149	Crisis Management	UR-CM-R19	Information on the situation to be given to the company staff.	*not specified*								x	As stated in D1.4: "The decision support system includes applications enabling to share and disseminate information concerning the incident to company staff. These include tools such as Web client, as well as information dissemination tools such as email." Decision support system = RAM2. Not assessed directly as part of WP8.

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
150	Crisis Management	UR-CM-R20	Ensures the standardised and simplified.	*not specified*								x	As stated in D1.4: "The decision support system includes applications enabling to share and disseminate information concerning the incident to companies' staff. These include tools such as Web client as well as information dissemination tools such as email." Decision support system = RAM2. Not assessed directly as part of WP8.
151	Crisis Management	UR-CM-R21	Reliable communication and early warning.	*not specified*	x	x	x	x		x			As stated in D1.4: "Decision support system will provide an early warning depending on the monitoring tools information. Within SAFETY4RAILS early warning capabilities will be demonstrated without a real-time integration into end-user systems. All demonstrated features will be shown over the direct access to S4RIS GUI and tools (G)UIs. Decision support system = RAM2.
152	Crisis Management	UR-CM-R22	Mutual early warning system for the operators of different means of transport.	*not specified*								x	As stated in D1.4: "The sharing of information is dependent on the operator agreeing to it…. Decision support system will provide an early warning depending on the monitoring tools information." Decision support system = RAM2. Not assessed as part of WP8.
153	Crisis Management	UR-CM-R23	Mutual early warning system for the operators of different means of transport.	*not specified*								x	as above
154	Crisis Management	UR-CM-R24	Cross-border exchange with the use of different languages must be considered.	*not specified*								x	As stated in D1.4: "This issue can be handled by using the decision support system's infor-mation dissemination tools, the use of the system's Web client application." Decision support system = RAM2. Not assessed as part of WP8.
155	Crisis Management	UR-CM-R25	Situational awareness.	*not specified*	x	x	x	x		x			As stated in D1.4 "SAFETY4RAILS will provide decision support capabilities which can contribute to situational awareness. It is out of the scope to cover full situational awareness."

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q**5)*
156	Crisis Management	UR-CM-R26	Impact and cascading effect simulation.	*not specified*	x	x	x	x	x				See CaESAR requirements/specifications below.
157	Crisis Management	UR-CM-R27	Crowd management.	*not specified*	x	x	x	x	x				See iCrowd requirements/specifications below.
158	Crisis Management	UR-CM-R28	Resumption of all operations of the multimodal transport system – complying with mutual interdependencies.	*not specified*								x	Not assessed as part of WP8.
159	Crisis Management	UR-CM-R29	Evaluation and explanation of common "lessons learned" to be implemented in the next prediction/prevention phase..	*not specified*								x	Not assessed as part of WP8.
160	Crisis Management	UR-CM-R30	Security Risk Assessment Index	Essential								x	Not assessed as part of WP8.
161	Communication with the public	UR-CC-R01	Coordinate with relevant stakeholders.	Essential								x	Not assessed as part of WP8, but see D10.7
162	Communication with the public	UR-CC-R02	Create a crisis communication plan.	Essential								x	Not assessed as part of WP8, but see D10.7
163	Communication with the public	UR-CC-R03	Communicate about preparedness actions to take when facing potential risks	Conditional								x	Not assessed as part of WP8, but see D10.7

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
164	Communication with the public	UR-CC-R04	Provide timely information.	Essential								x	Not assessed as part of WP8, but see D10.7
165	Communication with the public	UR-CC-R05	Provide upstream communication in transportation hub	Optional								x	Not assessed as part of WP8, but see D10.7
166	Communication with the public	UR-CC-R06	Continue to update about the situation.	Conditional								x	Not assessed as part of WP8, but see D10.7
167	Communication with the public	UR-CC-R07	Specific communication to regain passengers´ confidence for the multimodal approach.	Essential								x	Not assessed as part of WP8, but see D10.7
168	Communication with the public	UR-CC-R08	Apply lessons learned.	Essential								x	Not assessed as part of WP8, but see D10.7
169	Costs	C01	Cost benefit balance	Essential	x	x	x	x				x	Not directly or fully assessed as part of WP8. Although the end-user feedback indicated that there was in general agreement that a system/tool(s) which are reliable, depending on the price, could lead to cost savings or extra cost but which is justified due to increase in security/resilience (which on the other hand could also be amoriised through avoidance or less cost caused by incidents).
170	BB3d (RINA-C)	BB3d_01	Bomb blast loading	Essential	x				x				MA Q1, MA Q4
171	BB3d (RINA-C)	BB3d_02	Bomb blast usability	Essential								x	Not assessed as part of WP8, but see D10.7

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
172	BB3d (RINA-C)	BB3d_03	Bomb blast damage and casualties	Essential	x					x			
173	BB3d (RINA-C)	BB3d_04	Bomb blast computing performance	Essential								x	Not assessed as part of WP8, but see D10.7
174	BB3d (RINA-C)	BB3d_05	Bomb blast tool integration	Essential								x	Not assessed as part of WP8, but see D5.5, Annex 1, chapter 5, regarding integration with the Distributed Messaging system (DMS).
175	BB3d (RINA-C)	BB3d_06	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential								x	Not assessed as part of WP8 to go beyond this evaluation.
176	CaESAR (Fraunhofer)	CaESAR_01	CaESAR should estimate how disruptive events impact the infrastructure, its components and their functionalities.	Essential			x	x	x				R Q1, MI Q1, MI Q2
177	CaESAR (Fraunhofer)	CaESAR_02	CaESAR should identify weak points in the railway/metro system	Essential	x	x			x				MA Q2, A Q2, A Q3

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
178	CaESAR (Fraunhofer)	CaESAR_03	CaESAR should estimate the propagation of a failure caused by disruptive events to/from interdependent infrastructures, i.e. • Propagation from railway to metro • Propagation from metro to railway • Intra-propagation within railway/metro • Propagation to other critical infrastructures (power or telecommunication) • Propagation to other transportation infrastructures (bus networks)	Essential								x	Not fully assessed as part of WP8, but see D5.3.
179	CaESAR (Fraunhofer)	CaESAR_04	CaESAR should apply several strategies to recover from disruptive events and evaluate their impact on the infrastructure resilience.	Conditional			x	x	x				R Q1, MI Q1, MI Q2
180	CaESAR (Fraunhofer)	CaESAR_05	Implementation and evaluation of mitigation measures	Essential	x	x	x	x	x				MA Q3, A Q3, A Q5, R Q1, R Q4, MI Q1, MI Q2
181	CaESAR (Fraunhofer)	CaESAR_06	CaESAR should be able to handle the following different types of attacks • Physical • Cyber and • cyber-physical	Essential								x	Not fully assessed as part of WP8, but see D5.3.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
182	CaESAR (Fraunhofer)	CaESAR_07	Implementation of What-If-Scenarios and varying disruptive event attributes	Essential			x	x	x				R Q4, MI Q1, MI Q2
183	CaESAR (Fraunhofer)	CaESAR_08	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential						x			Not assessed as part of WP8 to go beyond this evaluation, but see D5.3.
184	CAMS (RMIT)	CAMS_01	Prediction of normal deterioration due to aging and degradation of as-sets	Essential	x	x	x	x	x				
185	CAMS (RMIT)	CAMS_02	Maintenance and repair budget calculation	Essential	x	x	x	x	x				MA Q1, A Q1
186	CAMS (RMIT)	CAMS_03	State-dependent fragility analysis	Essential	x	x	x	x	x				
187	CAMS (RMIT)	CAMS_04	Resilience module	Essential	x	x	x	x	x				
188	CAMS (RMIT)	CAMS_05	Risk / Cost Evaluation	Essential	x	x	x	x		x			
189	CAMS (RMIT)	CAMS_06	Backlog estimation	Essential								x	Not assessed as part of WP8, but see D7.5.
190	CAMS (RMIT)	CAMS_07	Optimization of budget	Essential	x	x	x	x	x				
191	CAMS (RMIT)	CAMS_08	Extension of the framework to IT assets	Conditional	x	x	x	x	x				

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
192	CAMS (RMIT)	CAMS_09	Analysis of compromise between maintenance, repair, rehabilitation and resilience enhancement efforts	Essential							x		Not assessed as part of WP8, but see D7.5.
193	CAMS (RMIT)	CAMS_10	Assessment of recovery	Conditional	x	x	x	x	x				MA Q4, A Q1, R Q3, MI Q3
194	CAMS (RMIT)	CAMS_11	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential				x		x			Not assessed as part of WP8 to go beyond this evaluation.
195	CuriX (CuriX)	CuriX_01	Anomaly detection (univariate and multivariate)	Essential	x	x	x	x	x				A Q3, A Q4, R Q2, R Q4, MI Q2
196	CuriX (CuriX)	CuriX_02	Catalogue-Based Outage Prevention	Essential	x					x			MA Q3
197	CuriX (CuriX)	CuriX_03	Infrastructure Monitoring (including cyber threats)	Essential	x		x	x	x				MA Q3, R Q2, R Q4, MI Q2
198	CuriX (CuriX)	CuriX_04	CuriX User-Friendly Dashboard	Essential	x	x	x	x	x				MA Q3, A Q3, A Q4, R Q2, R Q4, MI Q2. GUI feedback from exercises
199	CuriX (CuriX)	CuriX_05	System resource optimization for the Railway infrastructure	Conditional								x	
200	CuriX (CuriX)	CuriX_06	CuriX Dashboard to be provided multilingual	Conditional							x		
201	CuriX (CuriX)	CuriX_07	CuriX integration (connectors) to S4RIS and interfaces to other tools	Essential	x	x	x	x		x			

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
202	CuriX (CuriX)	CuriX_08	Hardening anomaly detection against data interruptions	Optional								x	
203	CuriX (CuriX)	CuriX_09	System intelligence and visualisation.	Optional	x	x	x	x	x				MA Q3, A Q3, A Q4, R Q2, R Q4, MI Q2. GUI feedback from exercises
204	CuriX (CuriX)	CuriX_10	How to use CuriX (configuration and dashboard)	Conditional								x	
205	CuriX (CuriX)	CuriX_11	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	x	x	x	x		x			Not fully assessed as part of WP8.
206	DATAFAN (Fraunhofer)	DATAFAN-1	Reliable and understandable machine learning (ML)-based results	Essential	x	x	x	x	x				Was continously improved. To this end, a Reliablilty Score (RLI) was developed and provided.
207	DATAFAN (Fraunhofer)	DATAFAN-2	High prediction performance of results, e.g. anomaly detection	Essential	x	x	x	x	x				MA Q2, MA Q3, A Q2, A Q3, A Q5, R Q1, R Q4, MI Q1. For clarification, anomaly detection, as primarily referred to in SAFETY4RAILS (e.g. expected v actual data in operational use), not actually applied in WP8 with DATA FAN, beyond "0" passengers. Applied algorithms provide prediction of passenger capacity / free capacity.
208	DATAFAN (Fraunhofer)	DATAFAN-3	Software application with a user-friendly interface	Essential		x			x				Incorporated user feedback and added new layout for the presentation of results into the GUI. Furthermore, tooltips help guide the user.
209	DATAFAN (Fraunhofer)	DATAFAN-4	How to use the software	Essential				x	x				

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
210	DATAFAN (Fraunhofer)	DATAFAN-5	Moderate hardware requirements for using the software	Essential	x				x				A standard laptop is sufficient to run the software
211	DATAFAN (Fraunhofer)	DATAFAN-6	Webservice for computation of expensive ML-algorithms	Essential							x		A stand-alone GUI that is available for download from the S4RIS Platform was developed instead
212	DATAFAN (Fraunhofer)	DATAFAN-7	Manner of the applied anomaly detection	Essential	x	x		x	x				MA Q3, A Q3, A Q5. A feature to integrate and visualize a detected anomaly was implemented. For clarification, as stated in D1.4, anomalies here refer to e.g. outliers and novelties in the in data set used for training.
213	DATAFAN (Fraunhofer)	DATAFAN-8	Requirements for the used data	Essential							x		
214	DATAFAN (Fraunhofer)	DATAFAN-9	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential				x		x			Not assessed as part of WP8 to go beyond this evaluation.
215	Ganimede (LDO)	Ganimede_1	Audio pattern detection	Essential			x			x			R Q2, R Q4. Demonstrated in SE3 for gun shot.
216	Ganimede (LDO)	Ganimede_2	Enhanced abandoned baggage detection	Essential		x	x		x				A Q3, A Q4 R Q2, R Q4.
217	Ganimede (LDO)	Ganimede_3	People re-identification	Conditional		x	x		x				A Q3, A Q4, R Q2, R Q4
218	Ganimede (LDO)	Ganimede_4	Man down	Essential								x	This functionality was not used in the SEs as it was not foreseen in the corresponding scenarios. It has been tested in laboratory (T6.4)
219	Ganimede (LDO)	Ganimede_5	Event visualization	Essential			x		x				Achieved through use of the SC2 tool with Ganimede

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
220	Ganimede (LDO)	Ganimede_6	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential		x	x					x	Not assessed as part of WP8 to go beyond this evaluation.
221	iCrowd (NCSRD)	iCrowd_01	Simulate realistic crowd congestion levels	Essential	x	x			x				MA Q3
222	iCrowd (NCSRD)	iCrowd_02	Simulate an evacuation because of terrorism (bomb, gas release) or natural disaster (fire/flood)	Essential	x	x			x				MA Q1, A Q1
223	iCrowd (NCSRD)	iCrowd_03	Simulate crowd behaviour considering cyber agents (electronic boards)	Conditional						x			NCSRD - Implemented but not tested in any SE
224	iCrowd (NCSRD)	iCrowd_04	Detect blind-spots because of guards' movements and insufficient cameras	Optional	x				x				MA Q1
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			x				
226	iCrowd (NCSRD)	ICrowd_06	Guards' distraction simulation	Optional						x			NCSRD - Implemented but not tested in any SE
227	iCrowd (NCSRD)	iCrowd_07	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	x	x				x			Not assessed as part of WP8 to go beyond this evaluation.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q**5)*
228	PRIGM (ERARGE)	PRIGM_01	PRIGM must have hardware encryption and random number generator modules	Essential		x			x				Indication from SE2 was that this was acheived.
229	PRIGM (ERARGE)	PRIGM_02	PRIGM must have a standardised API to connect to a Computer	Essential		x			x				Indication from SE2 was that this was acheived.
230	PRIGM (ERARGE)	PRIGM_03	PRIGM should be connected to the end user's central control unit	Essential		x			x				Indication from SE2 was that this was acheived.
231	PRIGM (ERARGE)	PRIGM_04	PRIGM should give service for end nodes and create outputs for end-users	Essential		x			x				Indication from SE2 was that this was acheived.
232	PRIGM (ERARGE)	PRIGM_05	PRIGM should work as a utility for the management of certification and IoT device authentication	Conditional		x			x				Indication from SE2 was that this was acheived.
233	PRIGM (ERARGE)	PRIGM_06	PRIGM operations must be GDPR compliant	Essential		x			x				Indication from SE2 was that this was acheived.
234	PRIGM (ERARGE)	PRIGM_07	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential		x						x	Not assessed as part of WP8 to go beyond this evaluation.
235	RAM^2 (ELBIT)	RAM2_01	RAM2 should provide risk assessment and prioritization	Essential	x	x	x	x	x				MA Q2, MA Q3, A Q3, R Q4, MI Q2. Full specification not tested in WP8.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
236	RAM² (ELBIT)	RAM2_02	RAM2 should generate correlated insights	Essential	x	x	x	x	x				MA Q3, A Q3, R Q4
237	RAM² (ELBIT)	RAM2_03	RAM2 should provide alert and insight mitigation steps	Essential	x	x	x	x	x				R Q4. Input required from the specific end-user where the system is being used need to help define/confirm the mitigation steps.
238	RAM² (ELBIT)	RAM2_04	RAM2 should provide an operational hierarchy context	Essential								x	Not possible to determine whether done in WP8 SEs.
239	RAM² (ELBIT)	RAM2_05	RAM2 Dashboard	Essential	x	x	x	x	x				Full specification not tested in WP8.
240	RAM² (ELBIT)	RAM2_06	RAM2 integration for input data and export to additional systems	Essential	x	x	x	x		x			RAM2 has capability to subscribe to topics in Distributed Messaging system (DMS). Alerts from real-tme monitoring tools demonstarted in SEs. Asset data from SecuRail in Ses not demonstrated.
241	RAM² (ELBIT)	RAM2_07	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential								x	Not assessed as part of WP8 to go beyond this evaluation.
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.MI Q1
243	SARA (RINA-C)	SARA-2	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential								x	Not assessed as part of WP8 to go beyond this evaluation.
244	SecaaS (ICOM)	SecaaS_01	Monitoring of network traffic for signs of abnormality	Conditional								x	Not assessed as part of WP8.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
245	SecaaS (ICOM)	SecaaS_02	Interfaces to comply with S4Rails WEB service methodology	Essential								x	Not assessed as part of WP8.
246	SecaaS (ICOM)	SecaaS_03	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential								x	Not assessed as part of WP8.
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				Libraries exist and are accessible from the UI. In the creation of a station, as an example, the user can choose to add assets from a predetermined list. While when setting up the scenario, the user can choose the threat to be analysed.
248	SecuRail (STAM)	SECURAIL_2	Localization on the Map	Conditional	x	x		x	x				In the home of the app, there is a map with a georeferenced presentation of the railway network
249	SecuRail (STAM)	SECURAIL_3	Computation of Risk	Essential	x	x		x	x				MA Q1, A Q2, MI Q1
250	SecuRail (STAM)	SECURAIL_4	Real time automatic risk assessment	Conditional				x		x			Even though SecuRail is connected to Kafka broker, the real-time risk analysis has been tested only with fake alerts through HTTP calls
251	SecuRail (STAM)	SECURAIL_5	Multilinguality	Optional	x	x		x	x				There is the option to change the language of the UI. At the moment, Italian and English have been configured, but the structure of the code is made to be easily extendible to other languages
252	SecuRail (STAM)	SECURAIL_6	Cost-Benefit Analysis	Conditional		x		x	x				A Q2, MI Q1
253	SecuRail (STAM)	SECURAIL_7	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential	x	x		x		x			Not assessed as part of WP8 to go beyond this evaluation.

No.	**Requirement/ Specification type**	**Requirement/ Specification ID**	**Short name**	**Priority**	**TEST CONTENT**				**EVALUATION**				**COMMENT**
					MA	**A**	**R**	**MI**	**A**	**P**	**NA**	**NK**	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q**5)*
254	Senstation (ERARGE)	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	Essential		x			x				Indication from SE2 was that this was acheived. Full specification not tested in WP8.
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				A Q3, A Q4. Indication from SE2 was that this was acheived.
256	Senstation (ERARGE)	SENSTATION_03	Senstation must encrypt sensory data on the communication channel	Essential		x			x				Indication from SE2 was that this was acheived.
257	Senstation (ERARGE)	SENSTATION_04	Temperature, smoke, acceleration and velocity sensors should be collected through the Senstation tool and used for anomaly detection.	Conditional		x			x				Indication from SE2 was that this was acheived.
258	Senstation (ERARGE)	SENSTATION_05	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential		x						x	Not assessed as part of WP8 to go beyond this evaluation.
259	SISC2 (ICOM)	SISC2_01	Software integration platform for surveillance, collaboration, coordination and administration of security and operations management events	Conditional								x	Not assessed as part of WP8.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
260	SISC2 (ICOM)	SISC2_02	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential								x	Not assessed as part of WP8.
261	TISAIL (TREE)	TISAIL_1	Detection of cyber-threats related to the railway sector: Malware	Essential			x			x			R Q1
262	TISAIL (TREE)	TISAIL_2	Detection of cyber-threats related to the railway sector: Internet-Exposed Assets and credential leaks	Essential	x	x	x		x				MA Q1, A Q2, A Q3, R Q1
263	TISAIL (TREE)	TISAIL_3	Detection of cyber-threats related to the railway sector: Threat Intel feeds and Social Media	Optional								x	Social media intelligence delivered by OSINT module (sepaarte to TISAIL)
264	TISAIL (TREE)	TISAIL_4	Detection of cyber-threats related to the railway sector: Vulnerabilities	Essential	x	x	x			x			MA Q3, R Q1
265	TISAIL (TREE)	TISAIL_5	Detection of cyber-threats related to the railway sector: Spear Phishing	Optional	x		x			x			MA Q3, R Q1
266	TISAIL (TREE)	TISAIL_6	Integrate alerts related to cyber-threats in the railway sector with a MISP repository	Essential		x			x				A Q3, A Q5, R Q1
267	TISAIL (TREE)	TISAIL_7	Use a Railway Threat Taxonomy on TISAIL	Optional	x	x	x		x				Indication from SE1-3 was that this was acheived, see alo D4.2.

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
268	TISAIL (TREE)	TISAIL_8	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential								x	Not assessed as part of WP8 to go beyond this evaluation.
269	uni|MS™ (ICOM)	UNIMS_01	Unified management for networks, infrastructure and systems	Conditional								x	Not assessed as part of WP8.
270	uni|MS™ (ICOM)	UNIMS_02	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential								x	Not assessed as part of WP8.
271	WIBAS (ICOM)	WiBAS_01	Advanced Wireless Broadband Access for Enterprise Users	Conditional								x	Not assessed as part of WP8.
272	WIBAS (ICOM)	WiBAS_02	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential								x	Not assessed as part of WP8.
273	WINGSPARK (WINGS)	WINGS_01	Data ingestion from devices	Essential								x	
274	WINGSPARK (WINGS)	WINGS_02	Data Management/Analysis	Essential	x		x	x	x				
275	WINGSPARK (WINGS)	WINGS_03	Support of A.I. techniques	Essential	x		x	x	x				MA Q3, R Q3, R Q4
276	WINGSPARK (WINGS)	WINGS_04	User-friendly GUI	Essential			x	x	x				GUI feedback from exercises

No.	Requirement/ Specification type	Requirement/ Specification ID	Short name	Priority	TEST CONTENT				EVALUATION				COMMENT
					MA	A	R	MI	A	P	NA	NK	*(Note: When the assessment of the tool's requirement/specification is based directly on the answers to the SEs questionnaires, there are the markings: **MA**drid, **A**nkara, **R**ome and **Mil**an; Questionnaires **Q1**-**Q5**)*
277	WINGSPARK (WINGS)	WINGS_05	Conformity with overarching and S4RIS platform specific requirements included in section 2.2	Essential			x	x		x			Not assessed as part of WP8 to go beyond this evaluation.