<

SAFETY4RAILS

First version of evaluation report

Deliverable 8.4

Lead Author: LAU

Contributors: ETRA, UIC, Fraunhofer

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.

D8.4 First version of evaluation report	
Deliverable number:	8.4
Version:	1.2
Delivery date:	13/12/2022
Dissemination level:	PU - Public
Nature:	Report
Main author(s)	LAU
Contributor(s) to main deliverable production	ETRA UIC LDO Fraunhofer
Internal reviewer(s)	Fraunhofer MdM
External reviewer(s)	Magdalena Kujacińska *(in process, feedback input to future work)*

Document control			
Version	Date	Author(s)	Change(s)
0.1	15/02/2022	LAU	Draft structure.
0.1	28/02/2022	LAU	Chapter 3 and Evaluation results
0.2	26/03/2022	LAU	Chapters 1 and 2
0.3	28/03/2022	LAU	Updated according to ETRA feedback
0.4	29/03/2022	LAU	Final draft
0.5	30/30/2020	LAU	Updated according to UIC feedback
0.9	04/04/2022	LAU	Further updates and new chapter on conclusions added Updated according to LDO feedback
0.10	11/04/2022	Fraunhofer	Acceptance of Fraunhofer updates to V.9, plus restructuring and formatting and further updates
1.0	13/04/2022	LAU	Finalisation
1.1	13/04/2022	Fraunhofer	Minimal formatting and editing
1.2	13/12/2022	LAU, Fraunhofer	Explanation for a low number of replies to evaluation questionnaires added in 3.1.1

DISCLAIMER AND COPYRIGHT

ABOUT SAFETY4RAILS

SAFETY4RAILS is the acronym for the innovation project: **Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS**. Railways and Metros are safe, efficient, reliable and environmentally friendly mass carriers, and they are becoming even more important means of transportation given the need to address climate change. However, being such critical infrastructures turns metro and railway operators as well as related intermodal transport operators into attractive targets for cyber and/or physical attacks.

The SAFETY4RAILS project delivers methods and systems to increase the safety and recovery of track-based inter-city railway and intra-city metro transportation. It addresses both cyber-only attacks (such as impact from WannaCry infections), physical-only attacks (such as the Madrid commuter trains bombing in 2004) and combined cyber-physical attacks, which are important emerging scenarios given increasing IoT infrastructure integration.

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

SAFETY4RAILS will improve the handling of such events through a holistic approach. It will analyse the cyber-physical resilience of metro and railway systems and deliver mitigation strategies for an efficient response, and, in order to remain secure given everchanging emerging risks, it will facilitate continuous adaptation of the SAFETY4RAILS solution; this will be validated by two rail transport operators and the results will support the re-design of the final prototype.

TABLE OF CONTENT

List of tables

List of figures

Executive summary

The Task T8.3 Evaluation – end-user and developer feedback for improvements- aim is to provide conclusions on applicability, feasibility and success of the developed S4RIS platform. This document is the deliverable D8.4 – First Version of Evaluation Report– of SAFETY4RAILS, aiming at presenting the first evaluation results of the SAFETY4RAILS Information System (S4RIS) platform. This report presents the evaluation results of the first simulation exercise that was carried out in M17 (February 2022) in Madrid hosted by Metro De Madrid.

The basis for the implementation of the evaluation was the deliverable D8.1 - Evaluation Methodology, end-user requirements specified in D1.4 – Specification of the overall technical architecture and D8.2 - First version of development of a blueprint exercise handbook. The evaluation was mainly performed by the end-users of the project participating in the exercises and 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, (referenced back to e.g. tool specific requirements/specifications identified in D1.4).

The results presented in this deliverable are based on the first questionnaires and debriefs from the first exercise. The evaluation will continue in the coming exercises and complementary surveys as well as group-based techniques will be used for the evaluation. The deliverable D8.5 – Final version of evaluation report – M22 (July 2022) will present the whole outcome of the evaluation.

1. Introduction

1.1 Overview

This deliverable presents the evaluation/validation including lessons learnt from the first simulation exercise organized in February 2022 in Madrid. This report concentrates on optimization potentials for both conducting future evaluation and technical aspects of the S4RIS. The initial evaluation of the S4RIS and its contributory is also initial input into demonstrating and identifying potential to improve business continuity management and the crisis management in railway and metro companies.

The Madrid exercise was carried out using online and on-site possibilities to attend the exercise due to Covid-19 restrictions. The primary evaluators of the exercise were twenty-four representatives from eight end-users represented in the consortium: 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 Rail Organisation).

The main output of the SAFETY4RAILS project is the SAFETY4RAILS Information System (S4RIS). 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" [1]. The SAFETY4RAILS project aims at a prototype of the S4RIS which can be demonstrated and validated in an operational environment. The overall philosophy is 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.[2]

Four simulation exercises, which represent 4 scenarios, will be organised within the project to test and evaluate the S4RIS platform. The first simulation was carried out in February (project month 17) and the three remaining demonstrations will be carried out between April 2022 (project month 19) and July 2022 (project month 22), with time between the simulations to implement identified potential for improvement of the developed information system. The analysis of the results based on all four simulation exercises will be provided in the D8.5 Final version of evaluation report after all the evaluation material is available.

For each scenario, the tool capabilities that can be provided either through the S4RIS platform or as a standalone (in the first exercises) is described in D8.2 and D8.3[3] (D8.2 first version and D8.3 final version– development of a blueprint exercise handbook).

The evaluation focuses on 2 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 D8.2.

In the evaluation of the organisation of the simulation exercise the feedback of all the participants was collected to help the preparations of the next exercises as well as future simulation exercises. The focus was on what can be done differently for the next exercises or what improvements need to be made.

The end-users evaluation of the S4RIS was based on the over 300 requirements and connected specifications 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. In the first simulation exercise not all tools and not all functionalities were included as such also not all requirements and connected

[1] SAFETY4RAILS Grant Agreement, version 2.0

[2] SAFETY4RAILS Deliverable D1.4

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

specifications could be evaluated. Future simulation exercises should include evaluation of further requirements and connected specifications.

All these requirements are documented and the specification in answer to each requirement is provided in SAFETY4RAILS Deliverable D1.4.[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.*"

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 specified context of use".[5] As part of the usability, the Graphical User Interface (GUI) has been evaluated.

The main objective of scenario-based requirements evaluation, is 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 D8.2 "First 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 will be tested for each resilience stage of the scenario with the specific objectives of the simulation and the expected performance to be evaluated.

As mentioned above, this deliverable will evolve into D8.5: Final version of evaluation report, which takes into account all simulation exercises.

1.2 Structure

This deliverable is structured as follows:

- Section 1 introduces the deliverable.
- Section 2 presents an overview of evaluation methodologies applied in SAFETY4RAILS.
- Section 3 introduce the exercise 1 (Madrid exercise).
- Section 4 provides the Madrid exercise results.
- Section 5 provides the conclusion of the deliverable.

[4] SAFETY4RAILS Deliverable D1.4

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

2. Applying evaluation methodology to SAFETY4RAILS exercises

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 base do their present development status 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. This means that this report does not take into account every single tool within the S4RIS project scope. The methodology enabled feedback for the planning of future exercise and for development iterations.

2.1 Exercise 1 (Madrid, Spain)

During the second week of February 2022 (8th-11th), the first SAFETY4RAILS Simulation Exercise (SE) was performed at the Metro de Madrid facilities, following the DoA. 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. Before fixing the date of the demonstration, the consortium discussed on the individual and country level constraints for travelling. All partners reached a consensus on performing the demonstration in a hybrid mode.

The minimum condition to have the physical meeting component was decided to be the hosting of more than 50% of the end-user partners in the consortium. It was determined this would provide the necessary physical interactions and improve how feedback on the technology was gathered in this phase. This condition was met: MDM, FGC, UIC, TCDD & EGO expressed their interest and attended physically, while RFI, CDM and PRO attended virtually.

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 (City De 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 Rail Organisation).

In the following, the consortium presents the simulation schedule agreed by all partners to clarify all actions to be done during the days of the event.

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

FIGURE 2.1: PHOTO OF PHYSICAL ATTENDEES

2.2 Objective of the exercise

The objective of the simulation exercise that was held in Madrid 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 D8.2.

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.

2.3 Exercise participants and evaluators

The evaluation was conducted by:

- End-user representatives organising the exercise:
  - The Metro of Madrid security team and other relevant departments.
- End-user representatives from the Consortium:
  - Rail partners: FGC, PRORAIL, RFI, TCDD.
  - Metro partners: EGO.
  - Local authority: CDM.
  - World-wide trade association: UIC.

This included 13 representatives of the end-users in the consortium participating physically and 11 in remote mode. A total of 24 end-user participants attended, including UIC.

FIGURE 2.2: INTRODUCTION AND SET-UP

FIGURE 2.3: BB3D PRESENTATION

FIGURE 2.4: DATA FAN PRESENTATION

2.4 How were the evaluations completed?

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 session were conducted, one after each workshop/resilience phase. The online debrief were organised using the Microsoft Forms questionnaires. The final debrief included also a discussion session where participants were asked to provide oral feedback on pre-prepared questions. The exercise schedule is presented in ANNEX II and as an example the questionnaire used for the Prevention Phase 1 is presented in ANNEX III.

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.

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 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 was 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 provide 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.

3. Results of Exercise 1 (Madrid, Spain)

3.1 Overview

3.1.1 Respondent replies

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 other 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 exist no significant differences when 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.

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.

3.1.2 Structure of the rest of the chapter

The results are presented in this chapter 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

For each tool and phase the “MDM scenario objective” is given as stated in D8.2 (which refers back to specific requirements and specifications included in the D1.4.). The respondents’ opinions in answer to closed questions are expressed for individual tools on the basis of number of responses. Unfiltered answers are expressed as percentages based on the compilation of individual tools results.

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 Prevention phase

3.2.1 BB3d

BB3d 01 - 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.

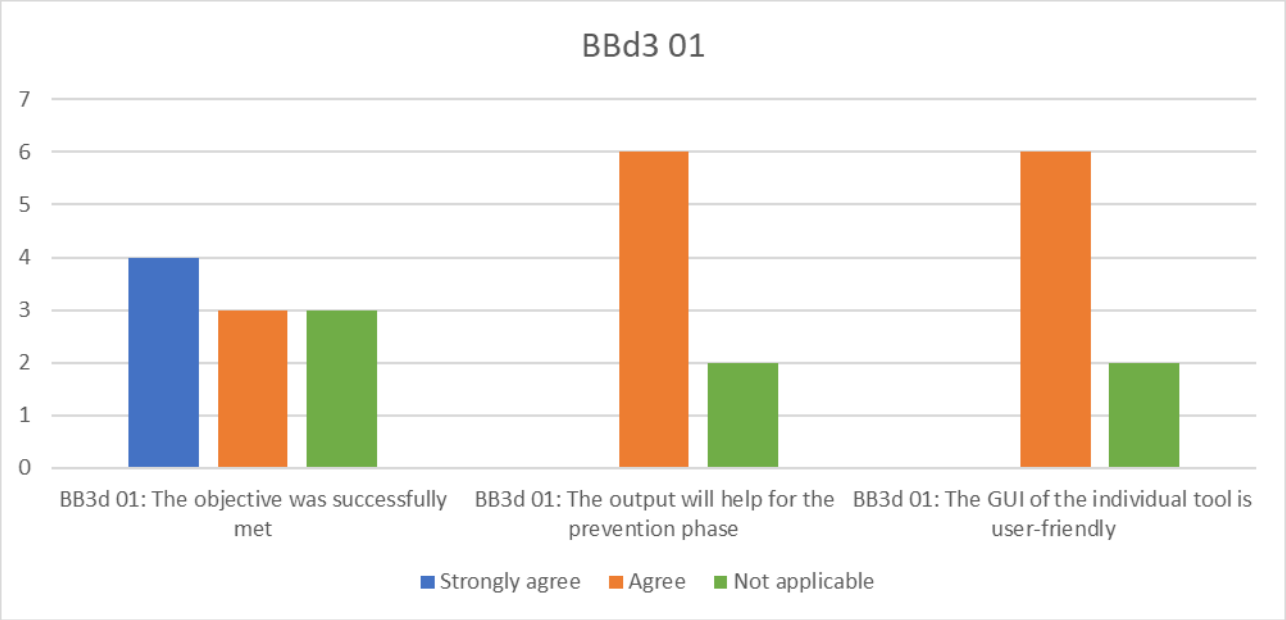

FIGURE 3.1: MDM SIMULATION EXERCISE PREVENTION PHASE - BB3D 01

Q1: 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.*

Q2: 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*

3.2.2 CAMS

CAMS 02 - 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.

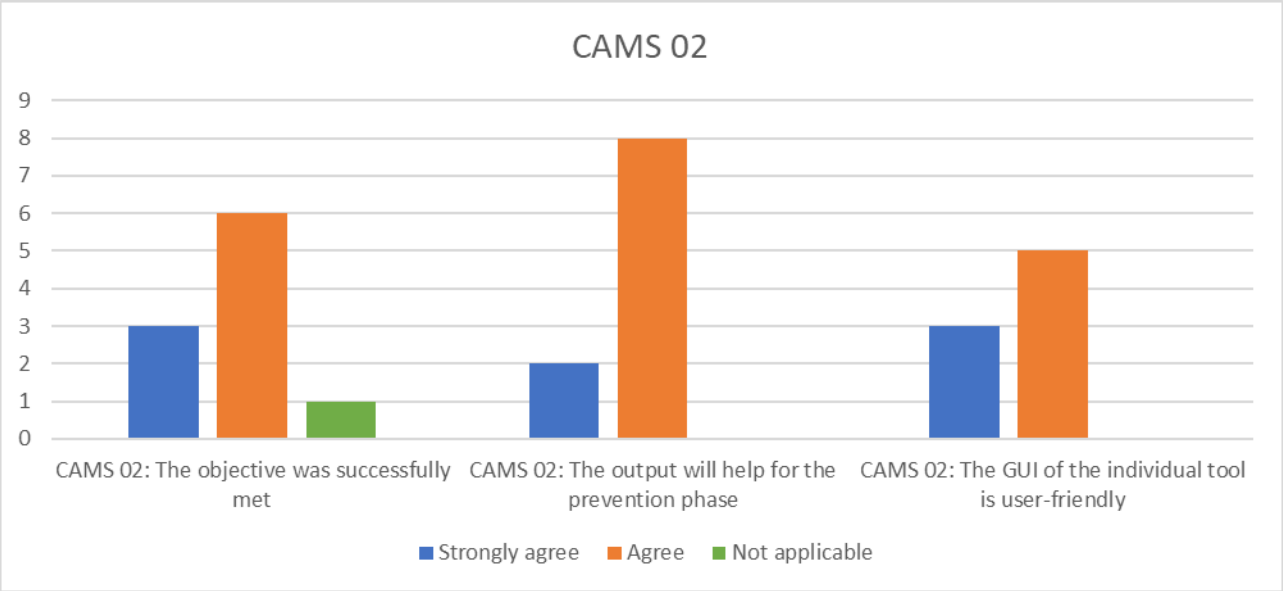

FIGURE 3.2: MDM SIMULATION EXERCISE PREVENTION PHASE - CAMS 02

Q1: 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*

Q2: 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*

3.2.3 SecuRail

SECURAIL 3 - Enable off-line risk analysis of the metro infrastructure to understand the level of risk for each critical asset during a given hazardous event.

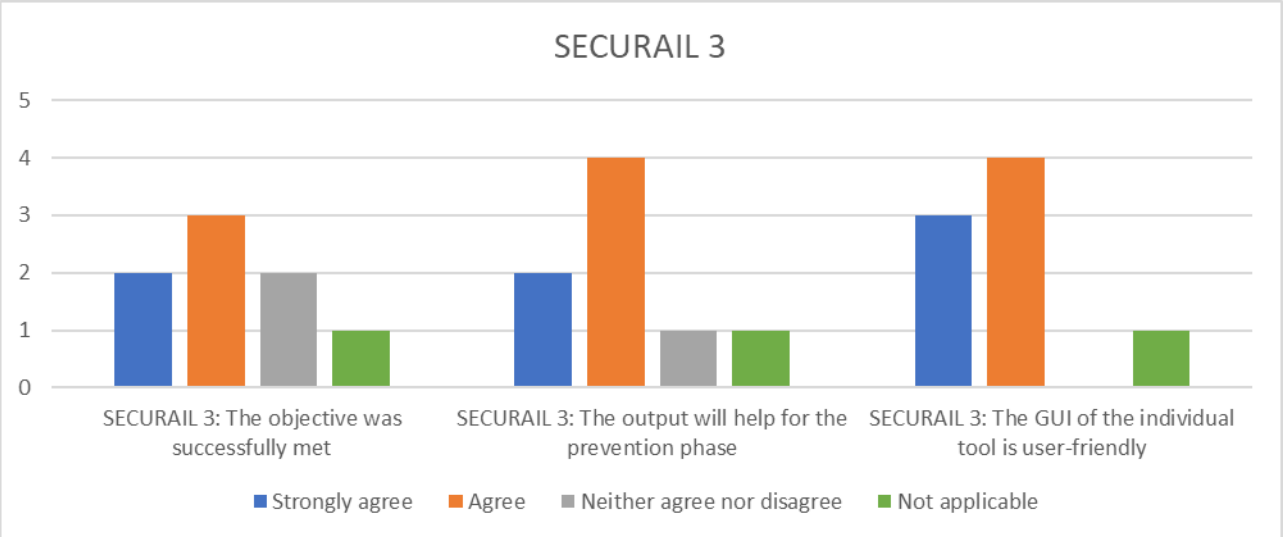

FIGURE 3.3: MDM SIMULATION EXERCISE PREVENTION PHASE - SECURAIL 3

Q1: 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.*

Q2: 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.*

3.2.4 TISAIL

TISAIL 2 - Provide vulnerability and security gaps assessment, along with risk assessment for each of the operational units in the metro system.

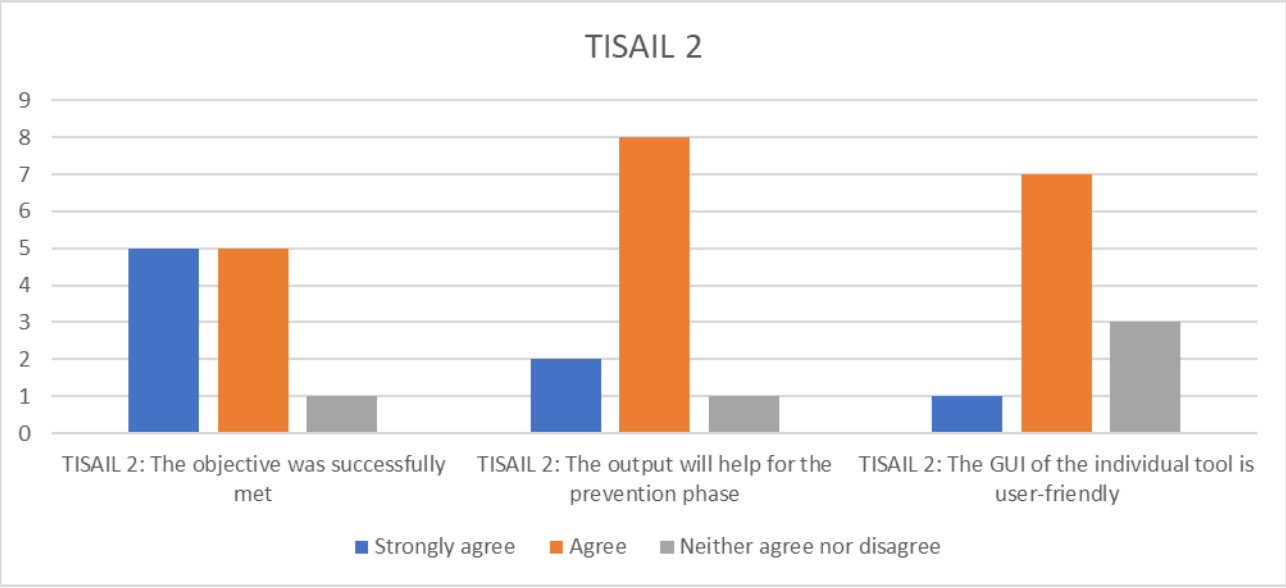

FIGURE 3.4: MDM SIMULATION EXERCISE PREVENTION PHASE - TISAIL 2

Q1: 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.*

Q2: How could this tool be improved in the context of this scenario?

- *Integration with existing tools (monitoring, alarm systems, etc.) in Metro de Madrid*

3.2.5 iCrowd

iCrowd 02 - Provide simulation capabilities to understand better the chances of detection during infiltration/escape per configuration (camera and guards locations) and infiltration/escape total times.

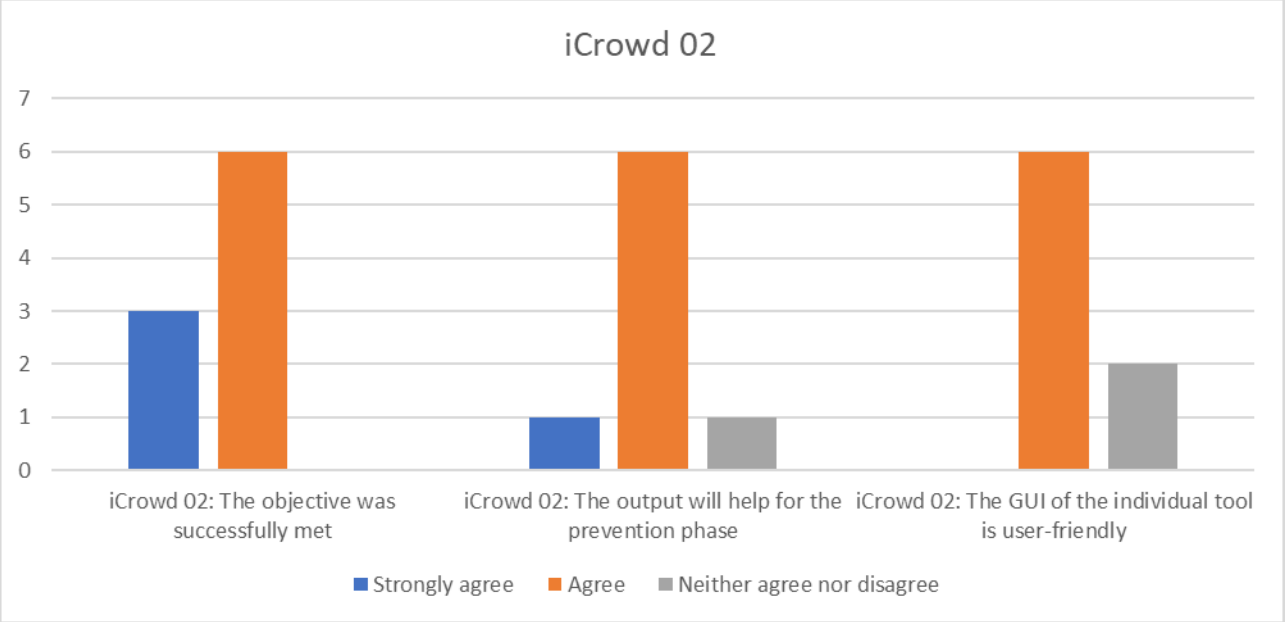

FIGURE 3.5: MDM SIMULATION EXERCISE PREVENTION PHASE - ICROWD 02

Q1: 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.*

Q2: 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 04 - Revealing blind spots and other related vulnerabilities in case of a threat actor trying to escape.

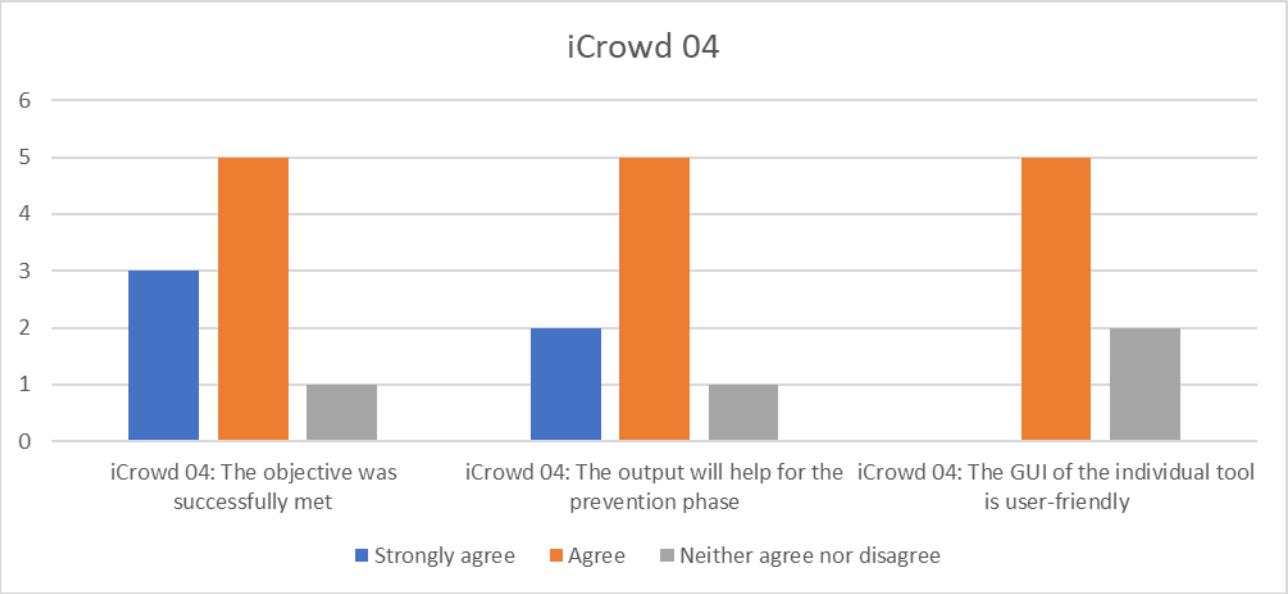

FIGURE 3.6: MDM SIMULATION EXERCISE PREVENTION PHASE - ICROWD 04

Q1: 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.*

Q2: How could this tool be improved in the context of this scenario?

- *N/A*

3.2.6 PRIGM

PRIGM 04 - 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.

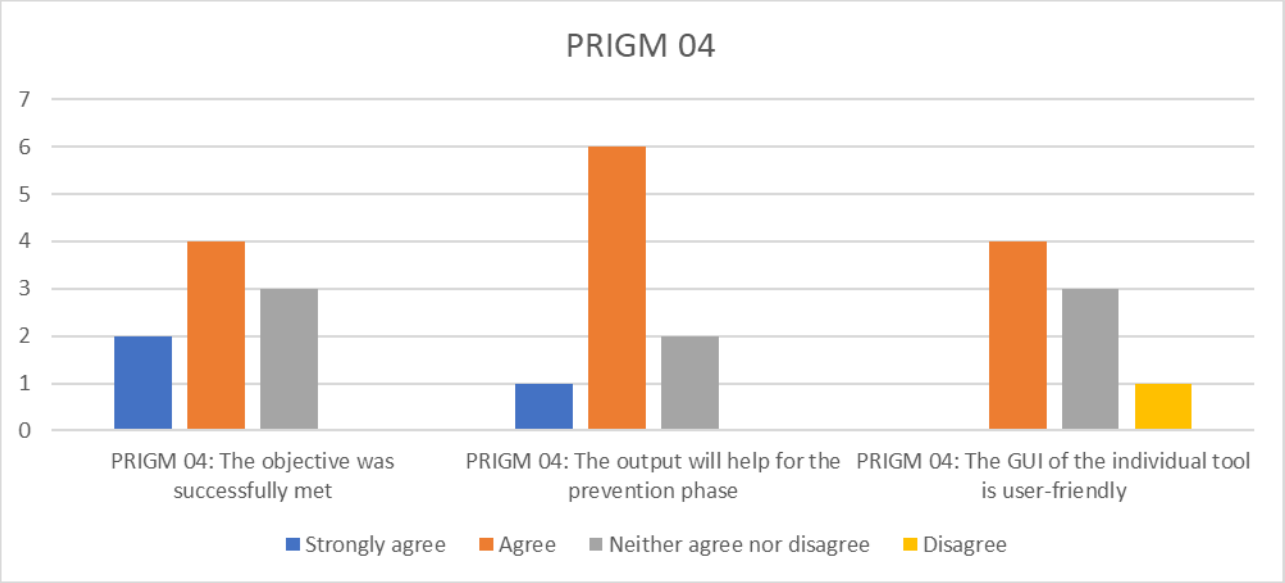

FIGURE 3.7: MDM SIMULATION EXERCISE PREVENTION PHASE - PRIGM 04

Q1: 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*

Q2: How could this tool be improved in the context of this scenario?

- *Integration in COMMIT systems*

3.2.7 DATA FAN

DATA FAN 2 - 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.[6]

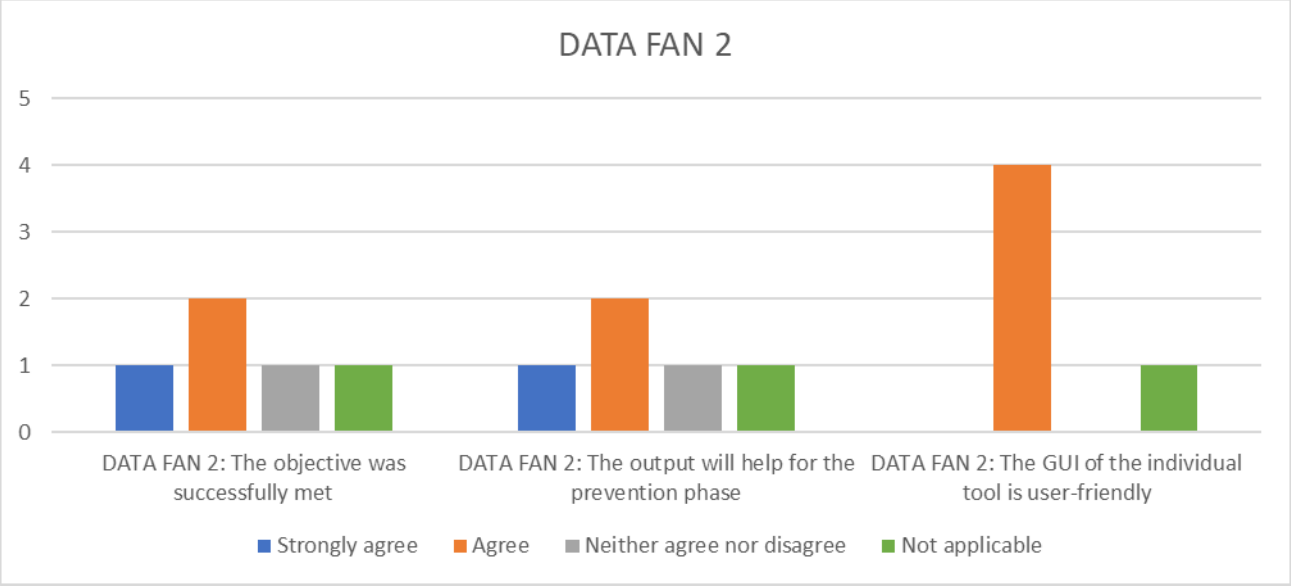

FIGURE 3.8: MDM SIMULATION EXERCISE PREVENTION PHASE - DATA FAN 2

Q1: 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.*

Q2: How could this tool be improved in the context of this scenario?

[6] Objective slightly adapted removing scenario specific detail for this Public report.

- *Take into account more variables in the movements*
- *Maybe the recommendations for the end user when a simulation is run could be applied automatically*

3.2.8 CaESAR

CaESAR 02 - 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.

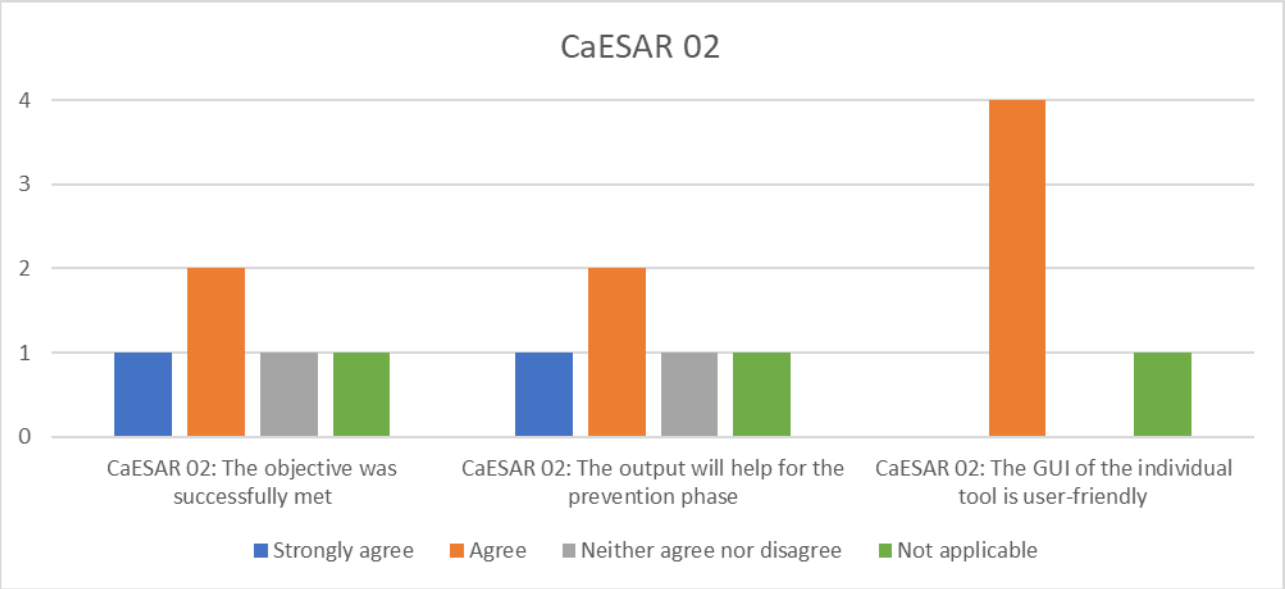

FIGURE 3.9: MDM SIMULATION EXERCISE PREVENTION PHASE - CAESAR 02

Q1: 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.*

Q2: How could this tool be improved in the context of this scenario?

- *Quick response*
- *Better integration with other tools*

3.2.9 RAMS2

RAM2 01 - Provide vulnerability and security gaps assessment, along with risk assessment for each of the operational units in the metro system.

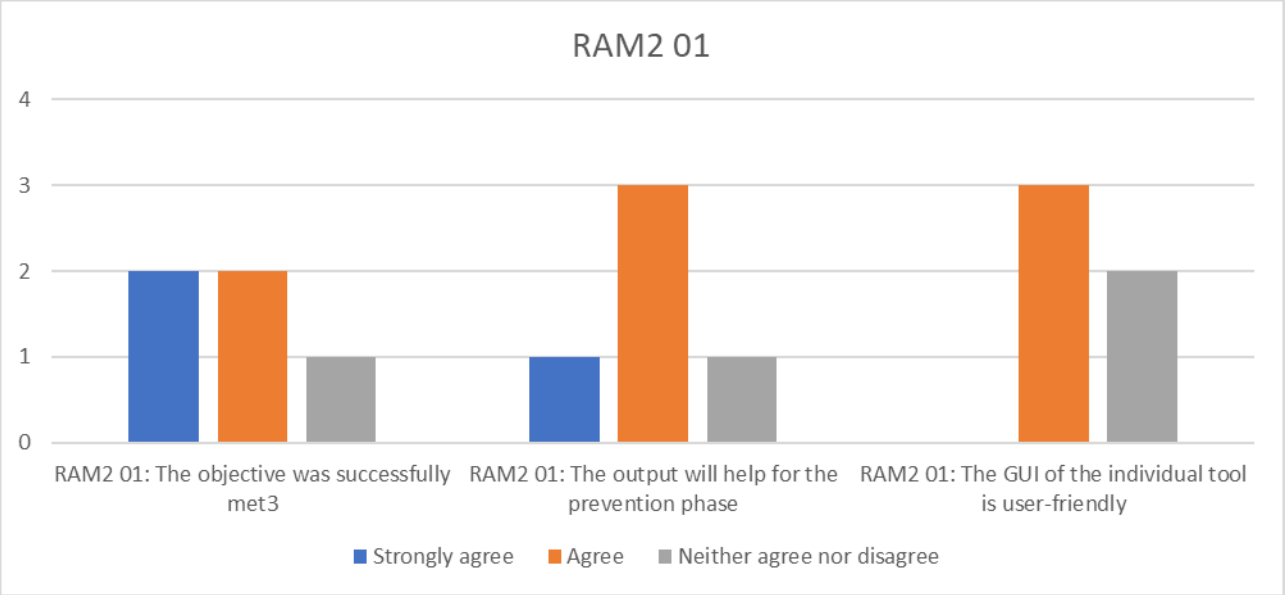

FIGURE 3.10: MDM SIMULATION EXERCISE PREVENTION PHASE - RAM2 01

Q1: 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.*

Q2: How could this tool be improved in the context of this scenario?

- *I will check more in detail*

3.2.10 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 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.

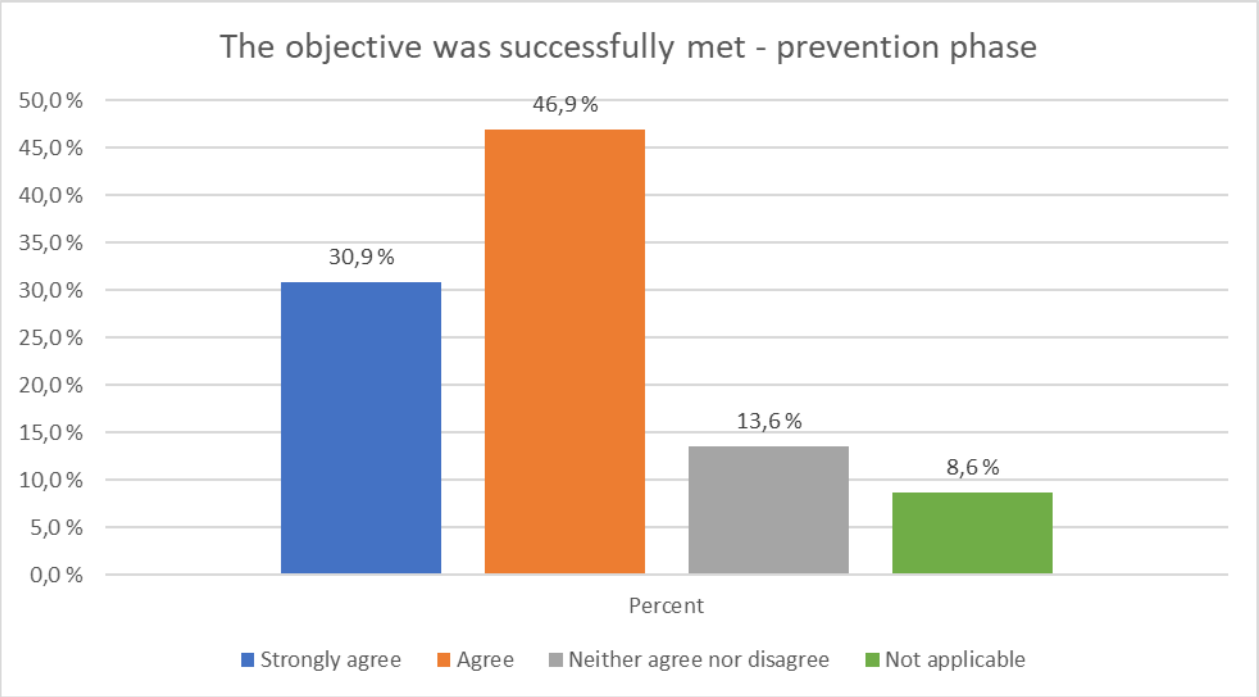

FIGURE 3.11: MDM SIMULATION EXERCISE PREVENTION PHASE - THE OBJECTIVE WAS SUCCESSFULLY MET

The end-users' opinion of the tools' GUIs 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.

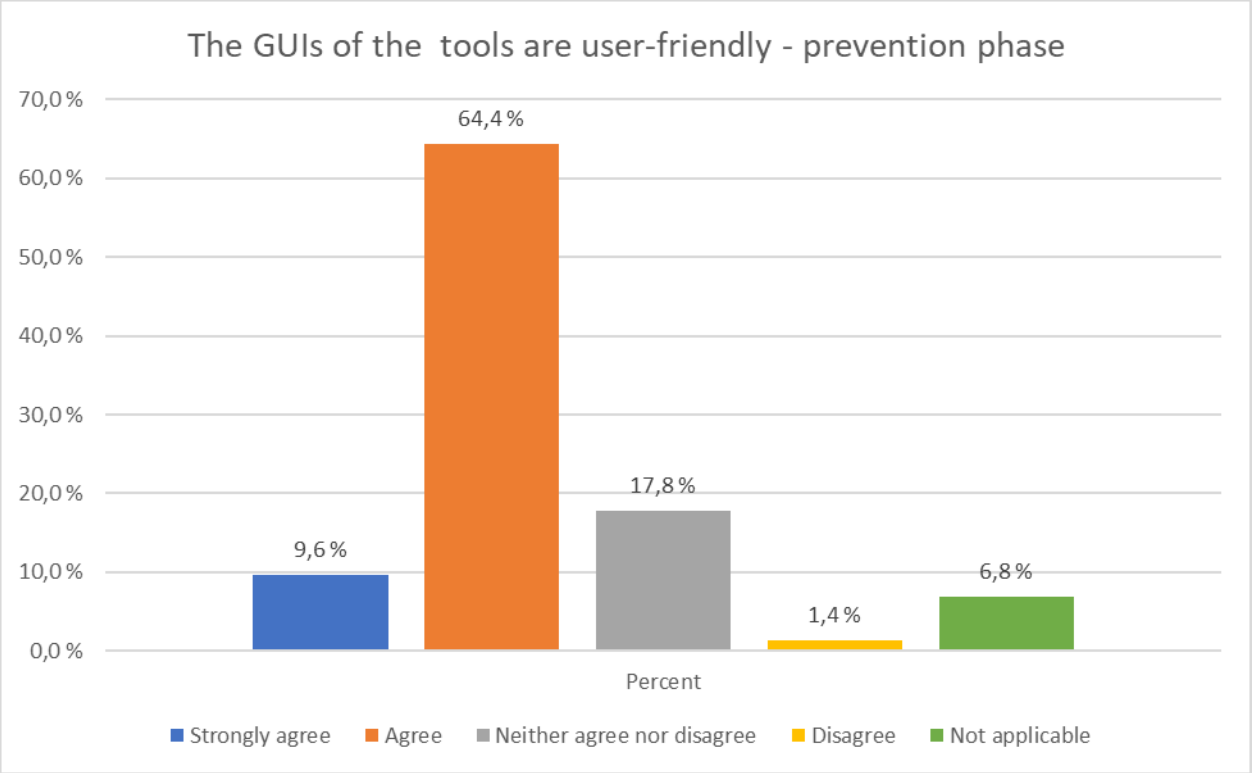

FIGURE 3.12: MDM SIMULATION EXERCISE PREVENTION PHASE - GENERAL OPINION OF THE TOOLS' GUIS

3.3 Detection and response phase

3.3.1 TISAIL

TISAIL 4 - 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.

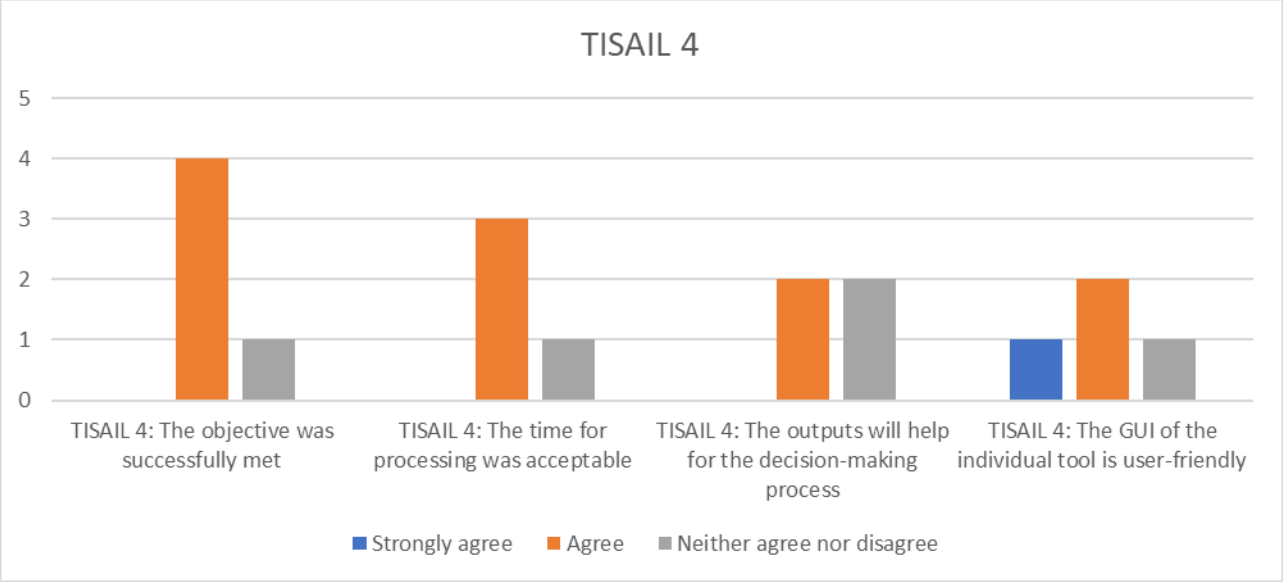

FIGURE 3.13: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - TISAIL 4

Q1: What would be your acceptable time to be processed?

- *already answered*
- *In real time*

Q2: 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.*

Q3: What could be improved in the context of this scenario?

- *N/A*

TISAIL 5 - Inform the Crisis Manager about possible spear-phishing campaigns targeting mail domains of the MDM personnel.

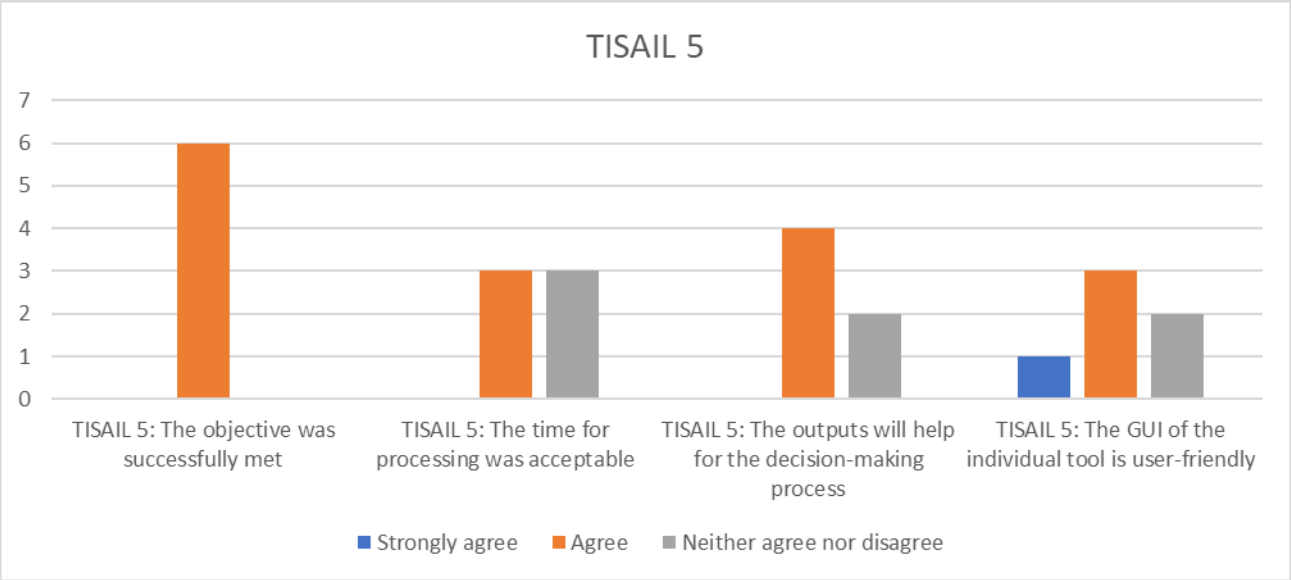

FIGURE 3.14: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - TISAIL 5

Q1: What would be your acceptable time to be processed?

- *30 minutes*
- *In real time*

Q2: 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*

Q3: What could be improved in the context of this scenario?

- *N/A*

3.3.2 CuriX

CuriX 02 - 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.

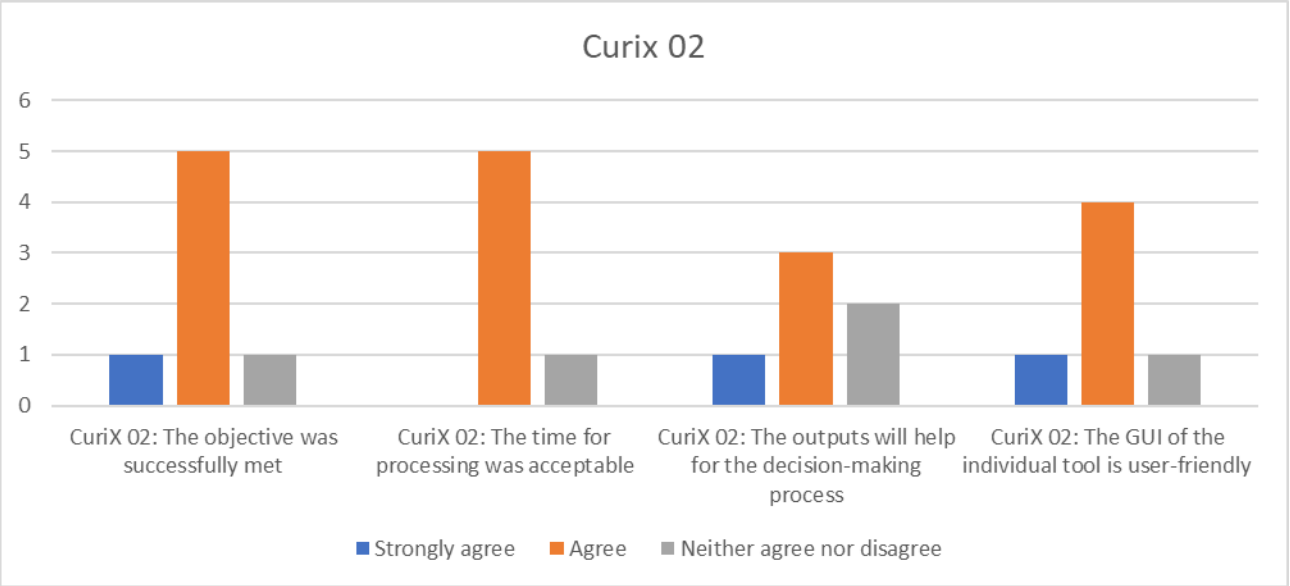

FIGURE 3.15: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - CURIX 02

Q1: What would be your acceptable time to be processed?

- *5 minutes*
- *In real time*

Q2: 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.*

Q3: What could be improved in the context of this scenario?

- *N/A*

CuriX 03 - The crisis manager can monitor the health of the monitored technical system.

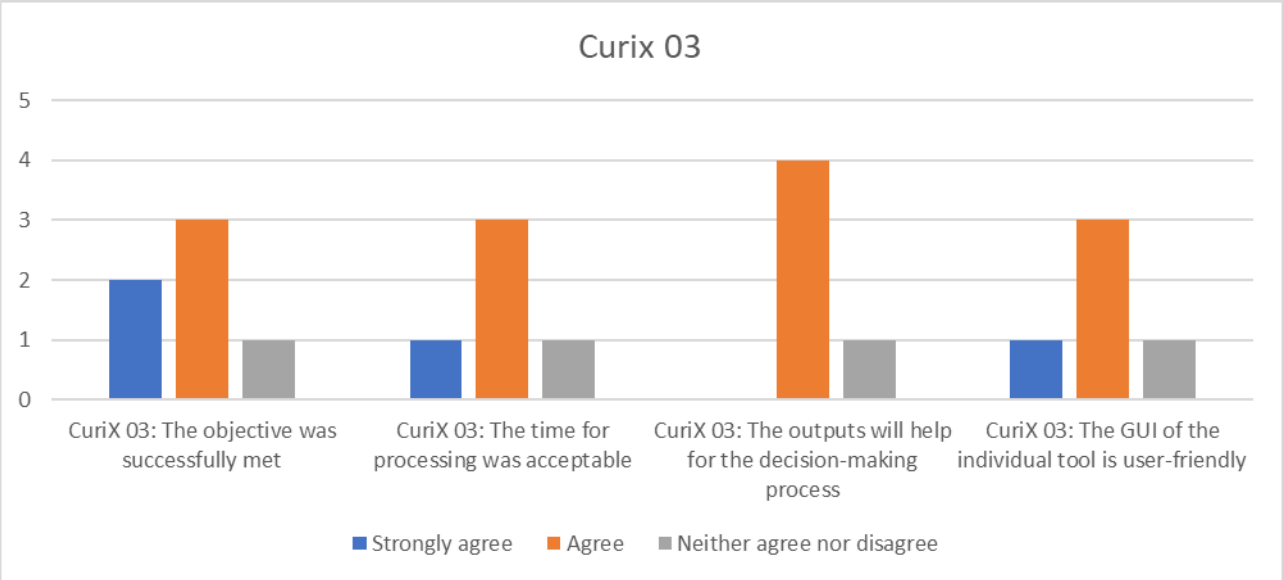

FIGURE 3.16: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - CURIX 03

Q1: What would be your acceptable time to be processed?

- *5 minutes*
- *In real time*

Q2: 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*

Q3: What could be improved in the context of this scenario?

- *N/A*

3.3.3 WINGSPARK

WINGS 03 (detection) - 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.

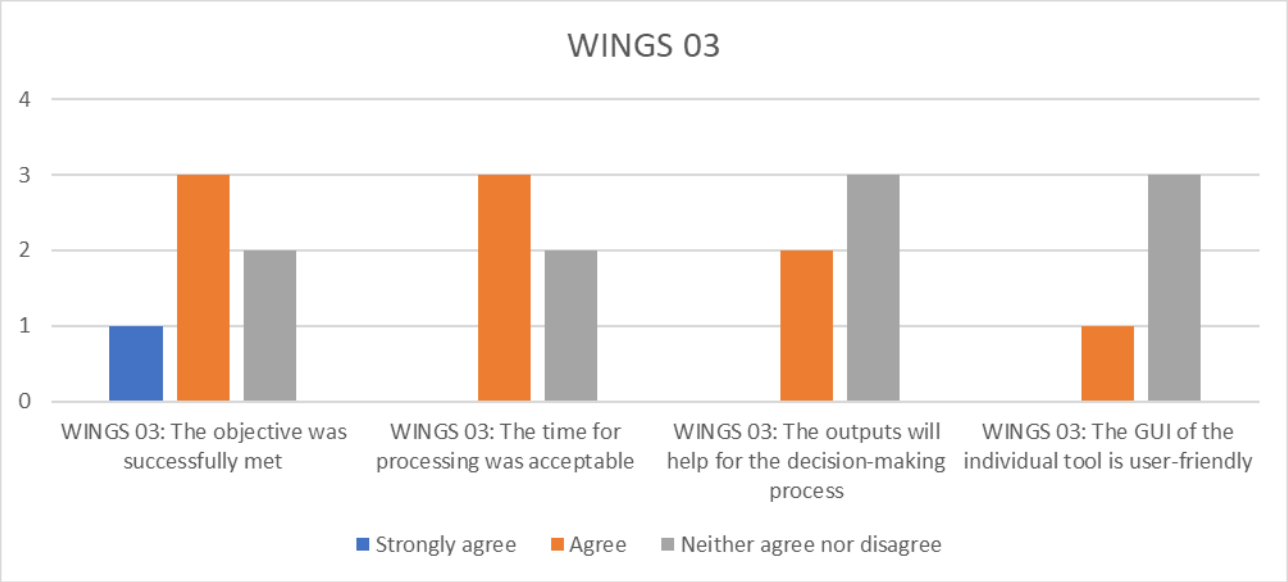

FIGURE 3.17: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - WINGS 03

Q1: What would be your acceptable time to be processed?

- *5 minutes*
- *Real time*
- *Within minutes*

Q2: 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.*

Q3: What could be improved in the context of this scenario?

- *N/A*

WINGS 03 (response) - 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.

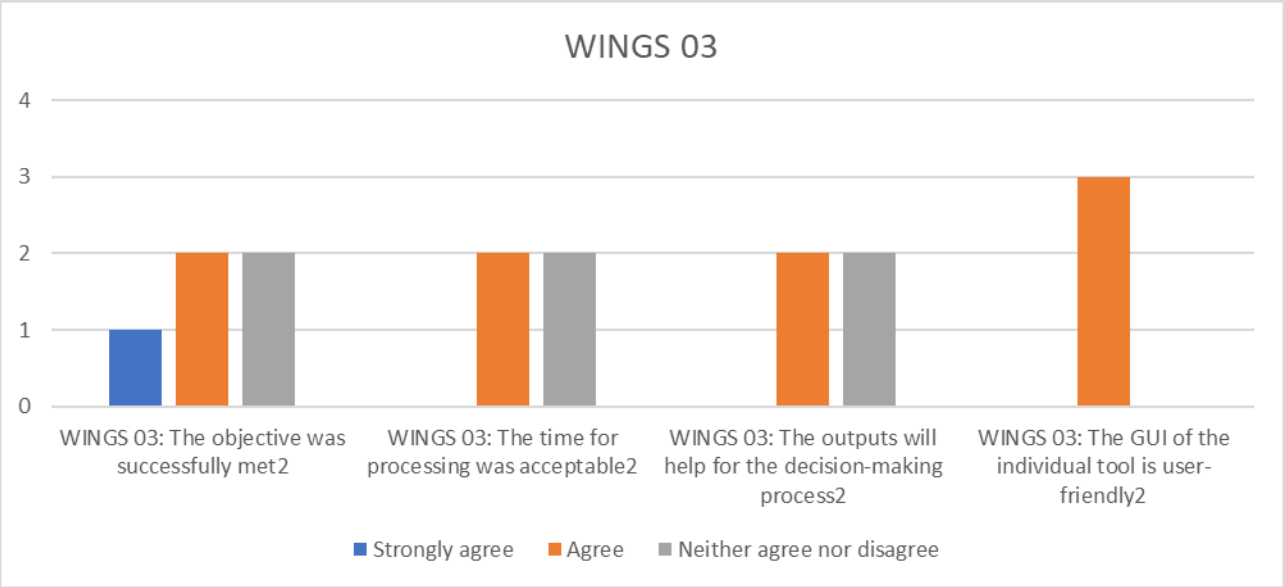

FIGURE 3.18: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - WINGS 03

Q1: What would be your acceptable time to be processed?

- *15 minutes*
- *Real time*

Q2: 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.*

Q3: What could be improved in the context of this scenario?

- *N/A*

3.3.4 DATA FAN

DATA FAN 2 - 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.

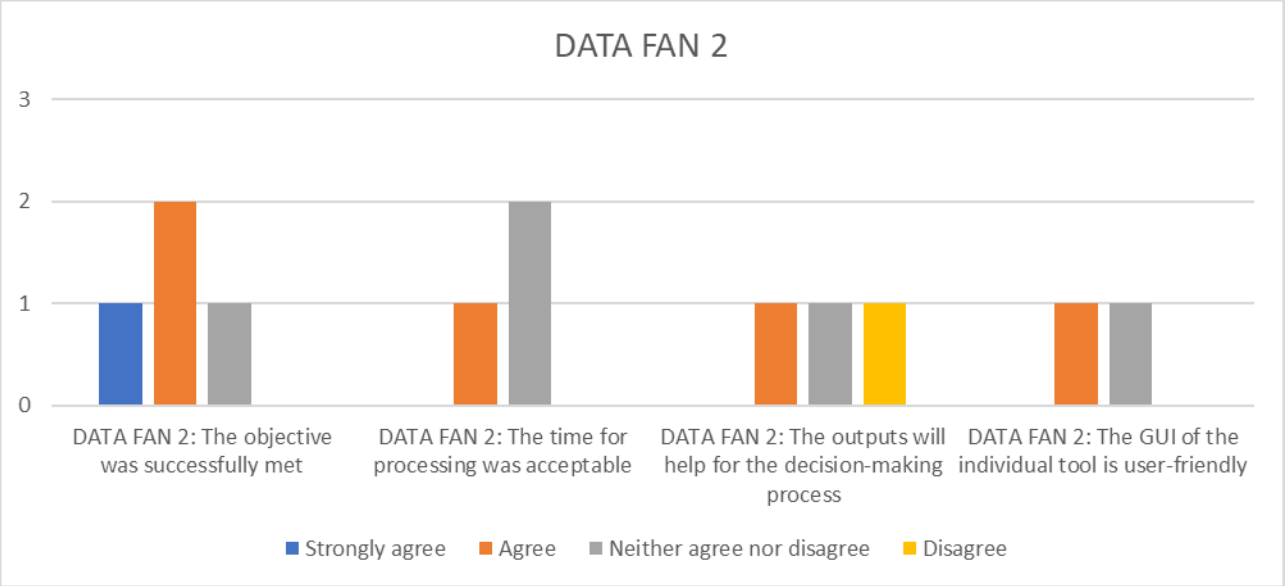

FIGURE 3.19: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - DATA FAN 2

Q1: What would be your acceptable time to be processed?

- *already answered*
- *15 minutes*

Q2: 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.*

Q3: What could be improved in the context of this scenario?

- *N/A*

DATA FAN 7 - 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.

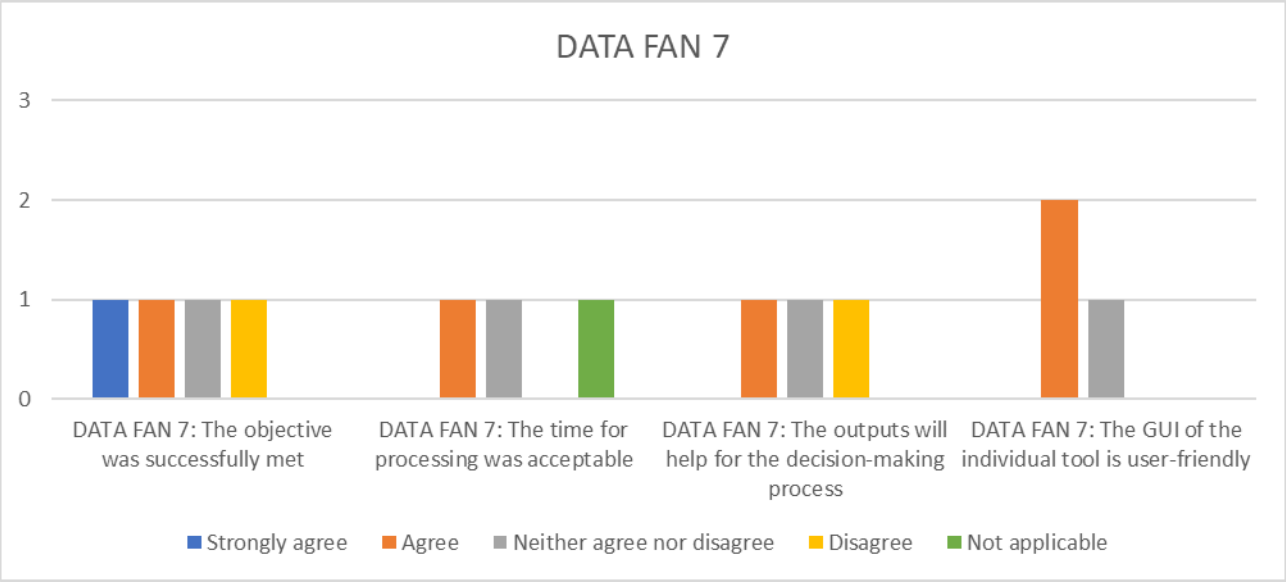

FIGURE 3.20: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - DATA FAN 7

Q1: What would be your acceptable time to be processed?

- already answered

Q2: 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.*

Q3: What could be improved in the context of this scenario?

- *No added value, we already work with this information in real time*

3.3.5 RAMS2

RAM2 02 - 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.

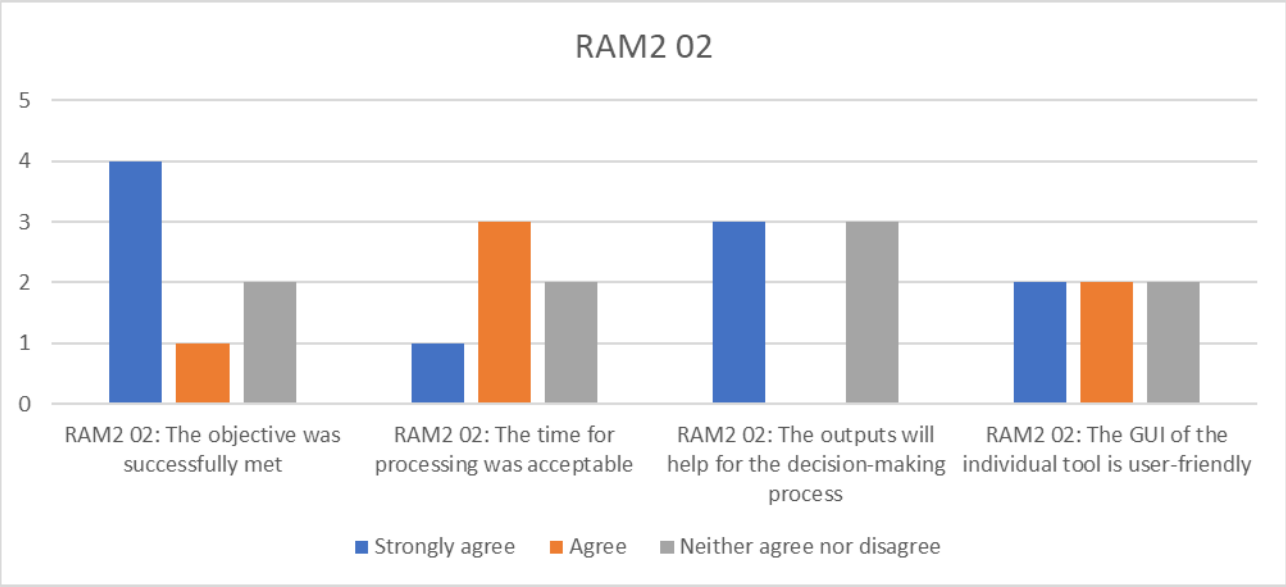

FIGURE 3.21: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - RAM2 02

Q1: What would be your acceptable time to be processed?

- *minutes*
- *Real time*

Q2: 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.*

Q3: What could be improved in the context of this scenario?

- *N/A*

RAM2 01 - 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.

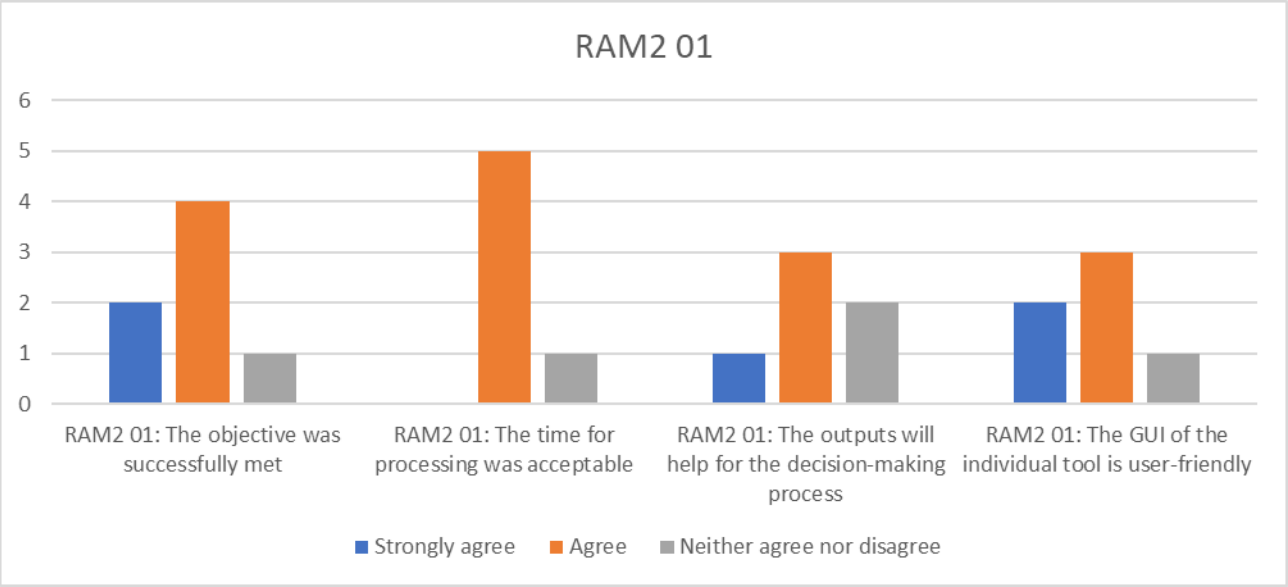

FIGURE 3.22: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - RAM2 01

Q1: What would be your acceptable time to be processed?

- *5 minutes*
- *Real time*

Q2: 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*
- *High added value. We would have the necessary information to define the action plan prioritizing the risks with the greatest impact.*

Q3: What could be improved in the context of this scenario?

- *N/A*

3.3.6 CaESAR

CaESAR 05 - 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.

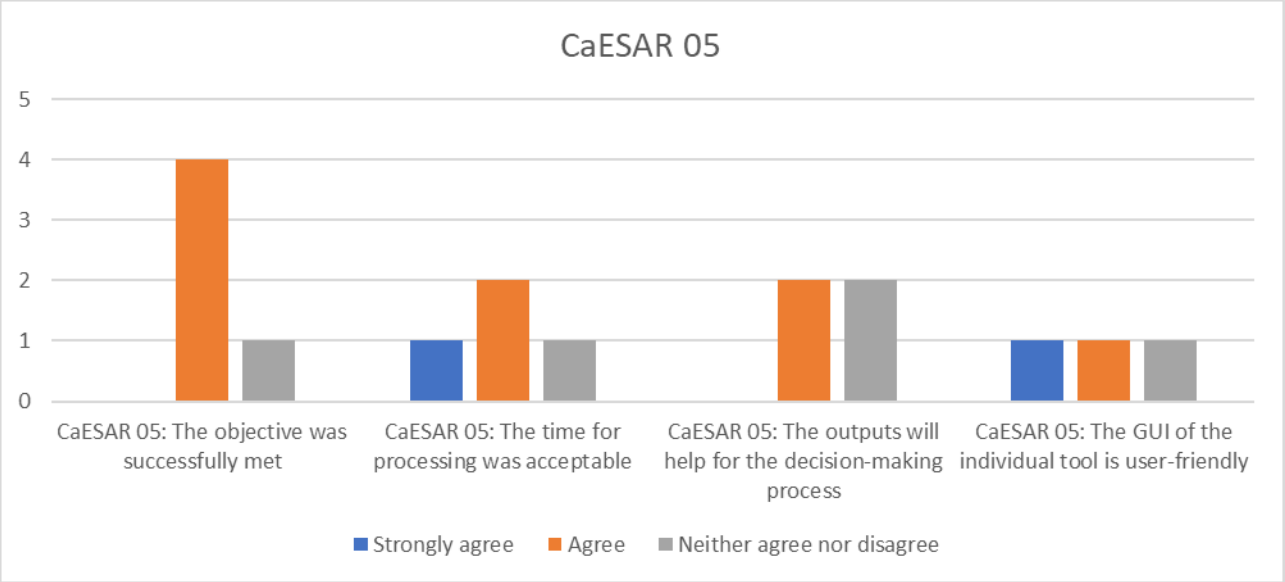

FIGURE 3.23: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - CAESAR 05

Q1: What would be your acceptable time to be processed?

- *already answered*
- *5 minutes*
- *Real time*

Q2: 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.*

Q3: 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.

3.3.7 iCrowd

iCrowd 01 - Crowd simulator providing advanced insights regarding crowd movement and behaviour for a set of boundary conditions related to the event.

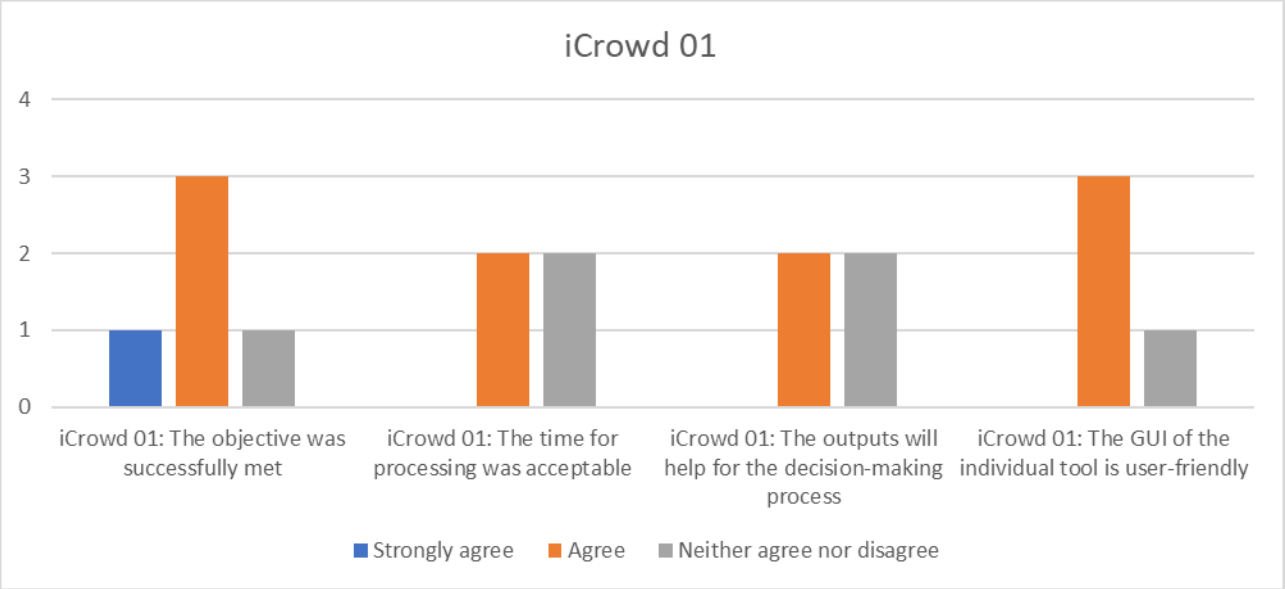

FIGURE 3.24: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - ICROWD 01

Q1: What would be your acceptable time to be processed?

- *15 minutes*
- *Real time*

Q2: 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.*

Q3: What could be improved in the context of this scenario?

- *N/A*

Further note based on on-site discussions: The iCrowd 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.

3.3.8 Overall achievement of objective and GUIs for detection & response phase

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 below. The percentages are based on the replies of seven (7) respondents.

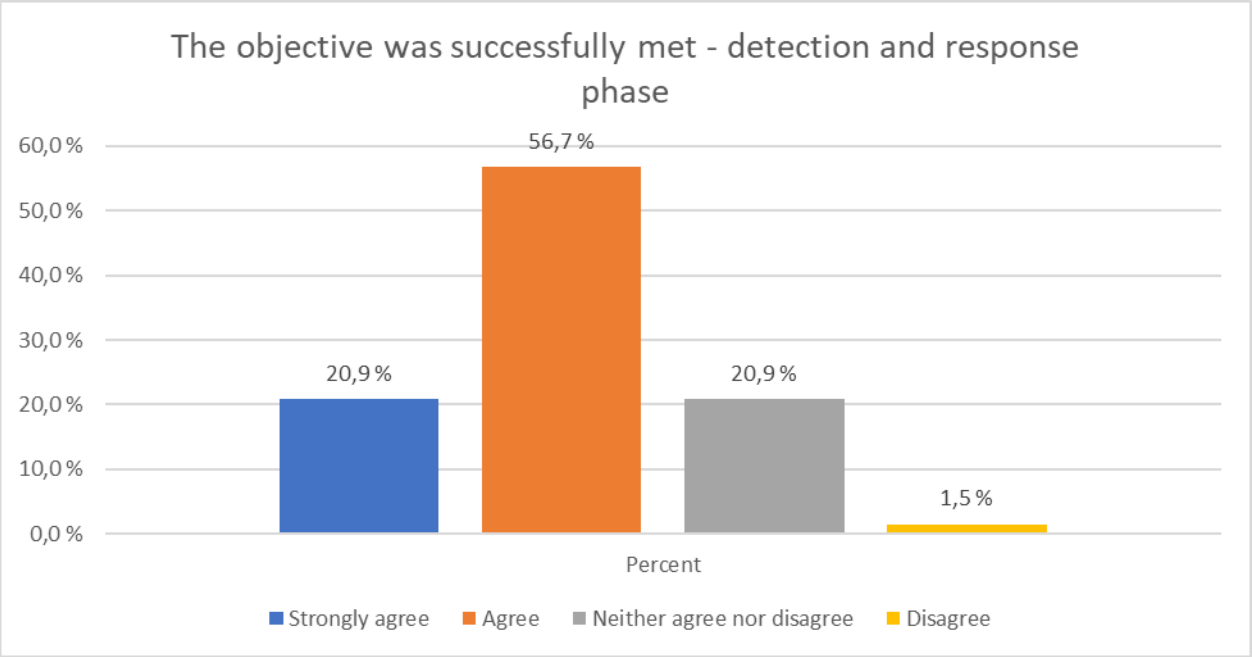

FIGURE 3.25: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - THE ACHIEVEMENT OF THE OBJECTIVES

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 below. The percentages are based on the replies of seven (7) respondents.

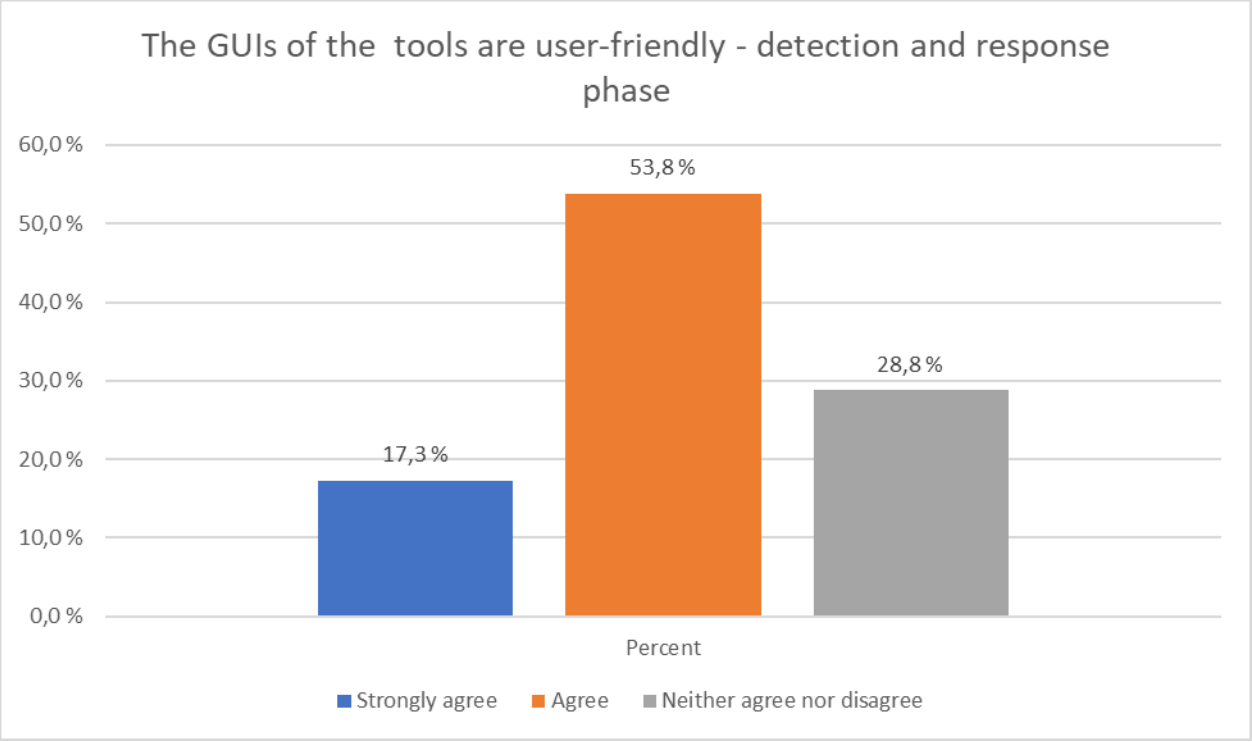

FIGURE 3.26: MDM SIMULATION EXERCISE DETECTION AND RESPONSE PHASE - GENERAL OPINION OF THE TOOLS' GUIS

3.4 Recovery phase

3.4.1 CAMS

CAMS 10 - 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.

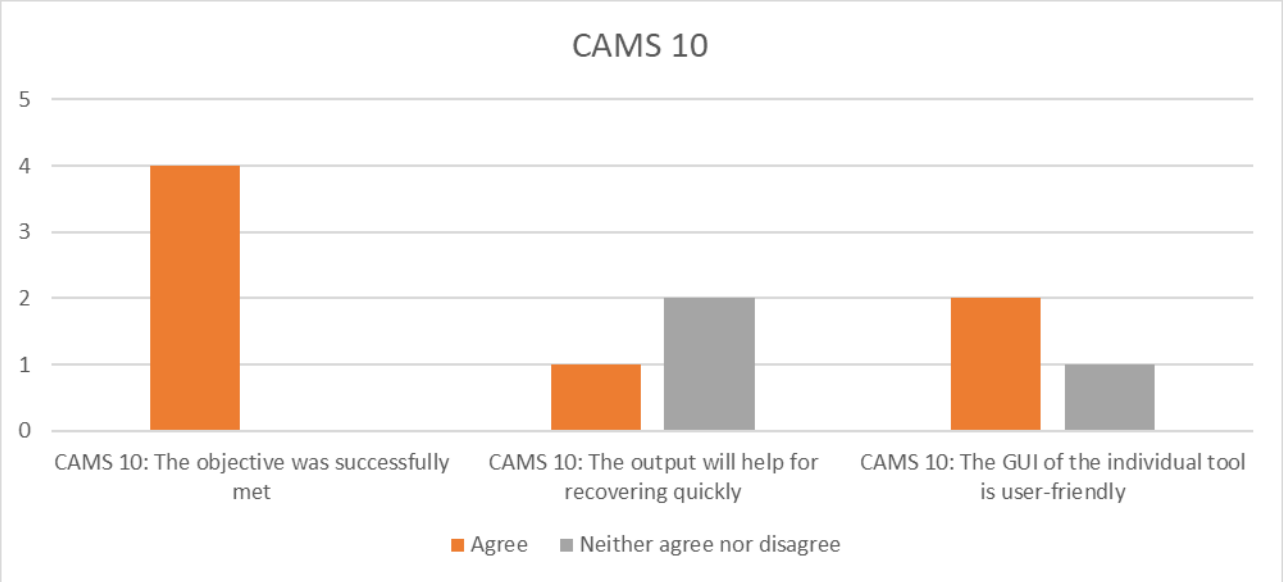

FIGURE 3.27: MDM SIMULATION EXERCISE RECOVERY PHASE – CAMS 10

Q1: 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.*

Q2: What could be improved in the context of this scenario?

- *N/A*

3.4.2 BB3d

BB3d 01 - 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.

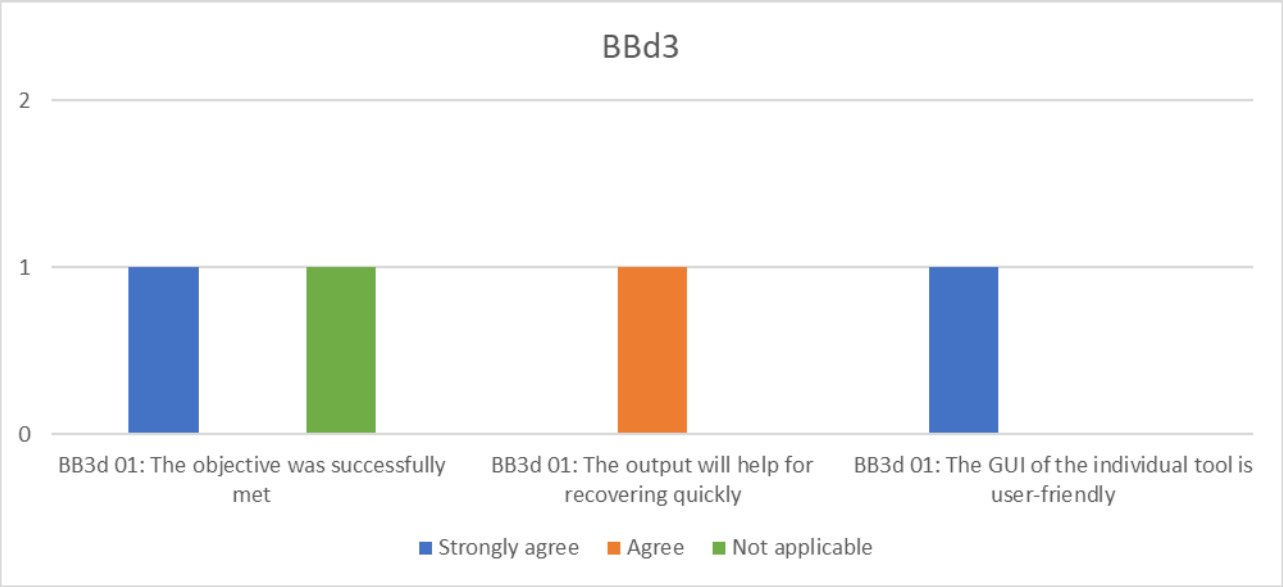

FIGURE 3.28: MDM SIMULATION EXERCISE RECOVERY PHASE – BBD3

3.4.3 Overall achievement of objective and GUIs for the response 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 below. 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.

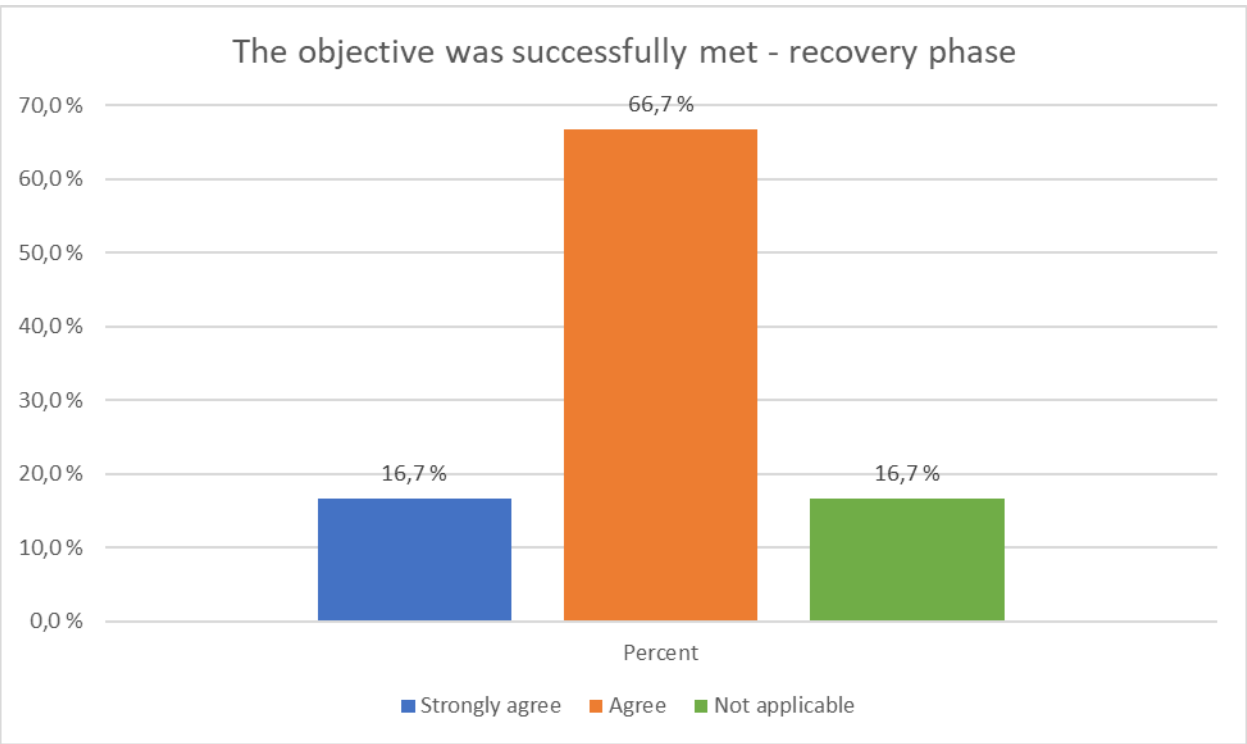

FIGURE 3.29: MDM SIMULATION EXERCISE RECOVERY PHASE – THE ACHIEVEMENT OF THE OBJECTIVES

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

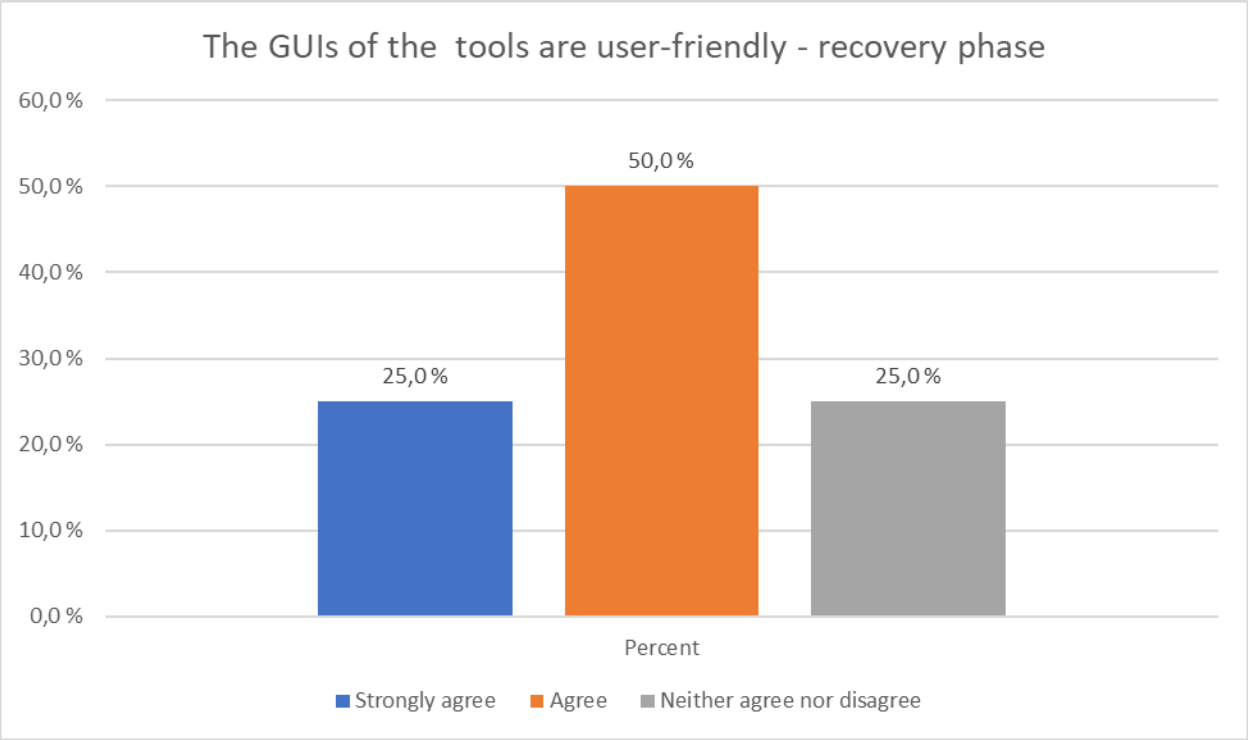

FIGURE 3.30: MDM SIMULATION EXERCISE RECOVERY PHASE – GENERAL OPINION OF THE TOOLS' GUIS

3.5 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 below. 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.

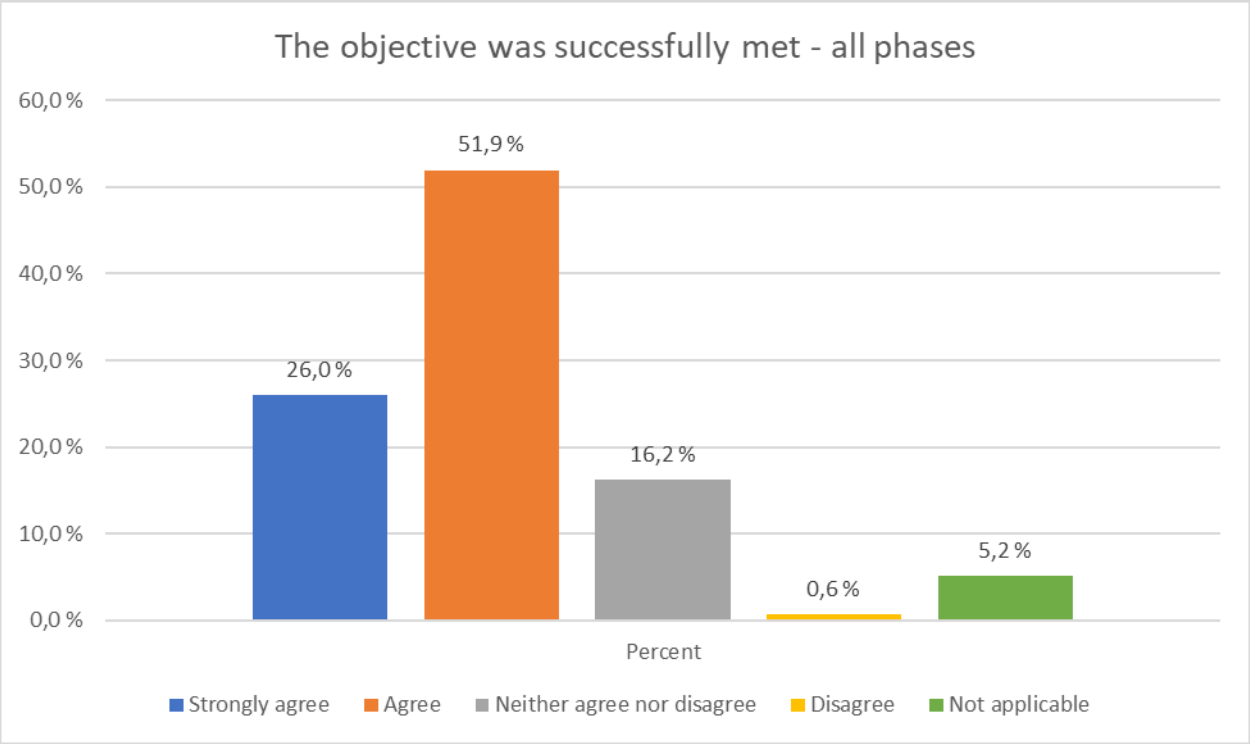

FIGURE 3.31: MDM SIMULATION EXERCISE - THE ACHIEVEMENT OF THE TOOLS' OBJECTIVES

The end-users' opinion of the tools' GUIs generally based on the feedback of all the tools is presented in the figure below. 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.

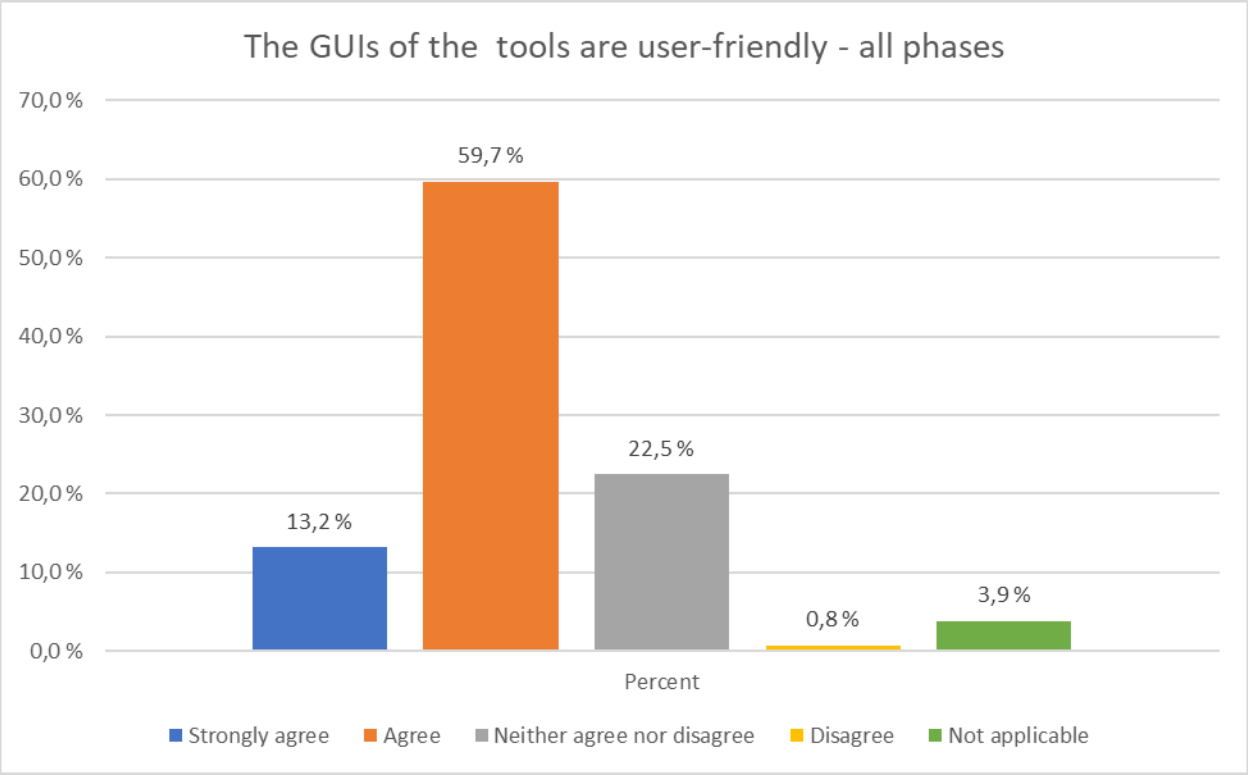

FIGURE 3.32: MDM SIMULATION EXERCISE - GENERAL OPINION OF THE TOOLS' GUIS COMMONLY

3.6 SAFETY4RAILS GUI and platform specific feedback

SAFETY4RAILS GUI and the platform were evaluated using both Likert scale and open-ended questions.

3.6.1 GUI

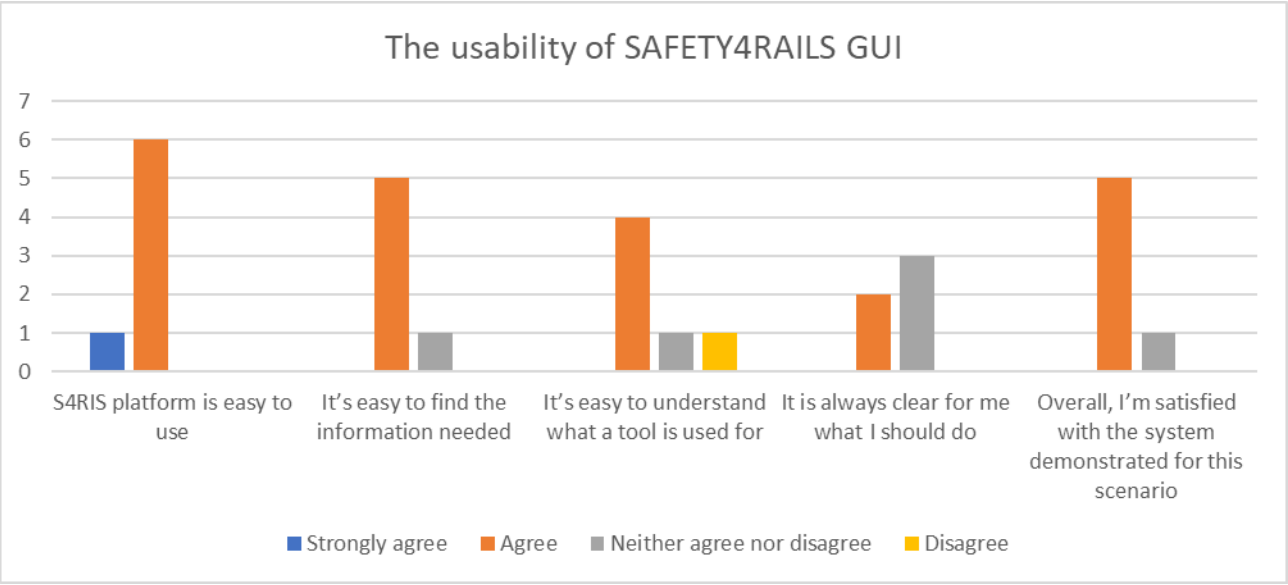

FIGURE 3.33: MDM SIMULATION EXERCISE - THE USABILITY OF SAFETY4RAILS GUI

Q1. 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.*

Q2: 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*

Q3: What could be improved to make the handling more transparent?

- *It is okay*

Q4: 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.*

3.6.2 SAFETY4RAILS platform specific

The bars are expressing the number of given responses. Unfiltered answers to open-ended questions are following the Likert scale figures.

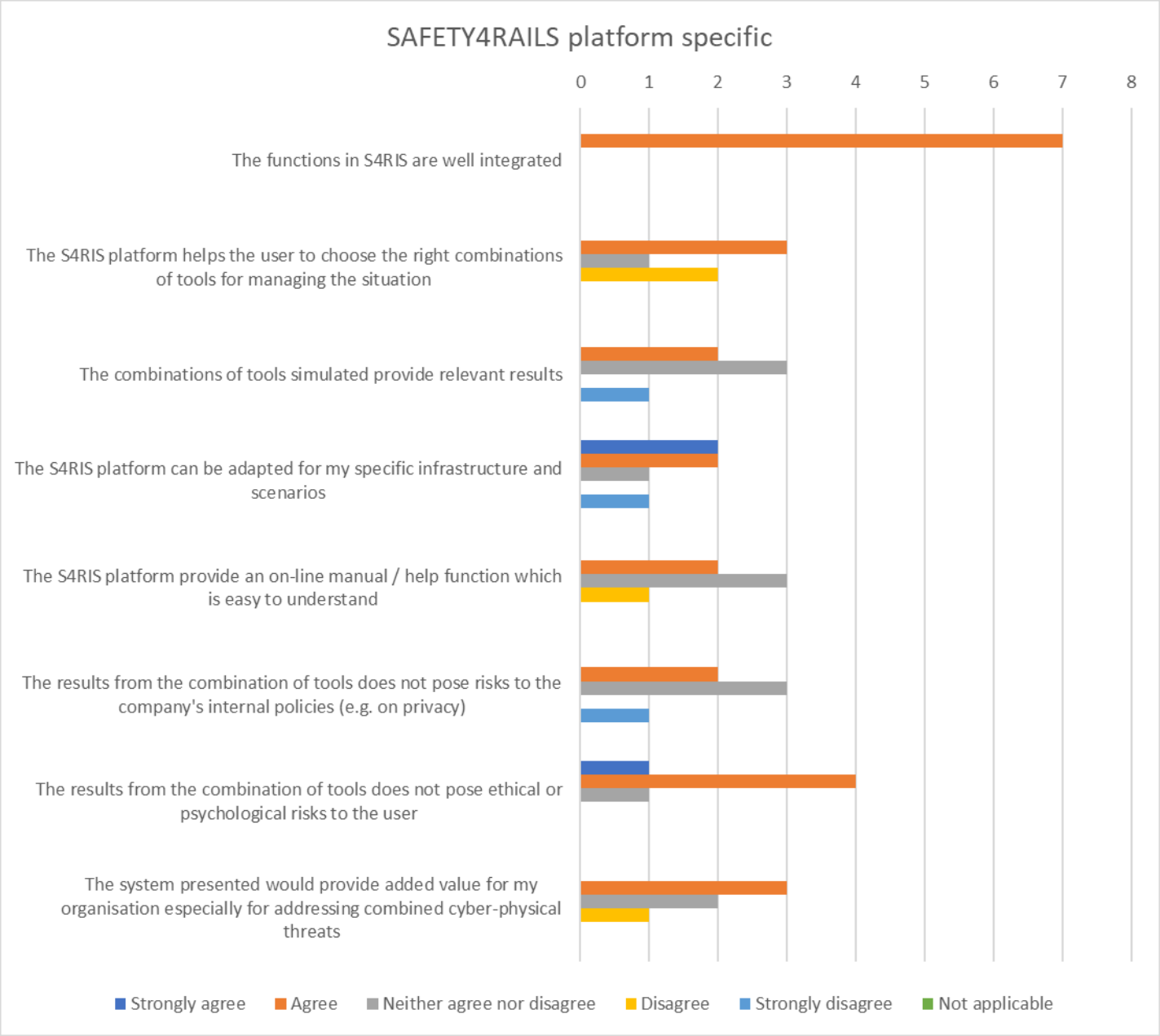

FIGURE 3.34: MDM SIMULATION EXERCISE - SAFETY4RAILS PLATFORM SPECIFIC

Q1: 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*

Q2: 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.*

Q3: 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*

Q4: Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- *Try to add more user requirements*

3.7 Overall objectives of MdM evaluation and organization of the exercise

The achievement of the overall objectives of the exercise and the organization of the exercise were evaluated using both Likert scale and open-ended questions. In what follows we present the answers to the questionnaires, including responses to open-ended questions. The pillars are expressing the number of given responses.

Questions related to overall objectives and organisation of the exercise were presented in connection to the questionnaire of the last phase of the exercise, this timing seems to have affected the number of the responses.

3.7.1 Overall objectives

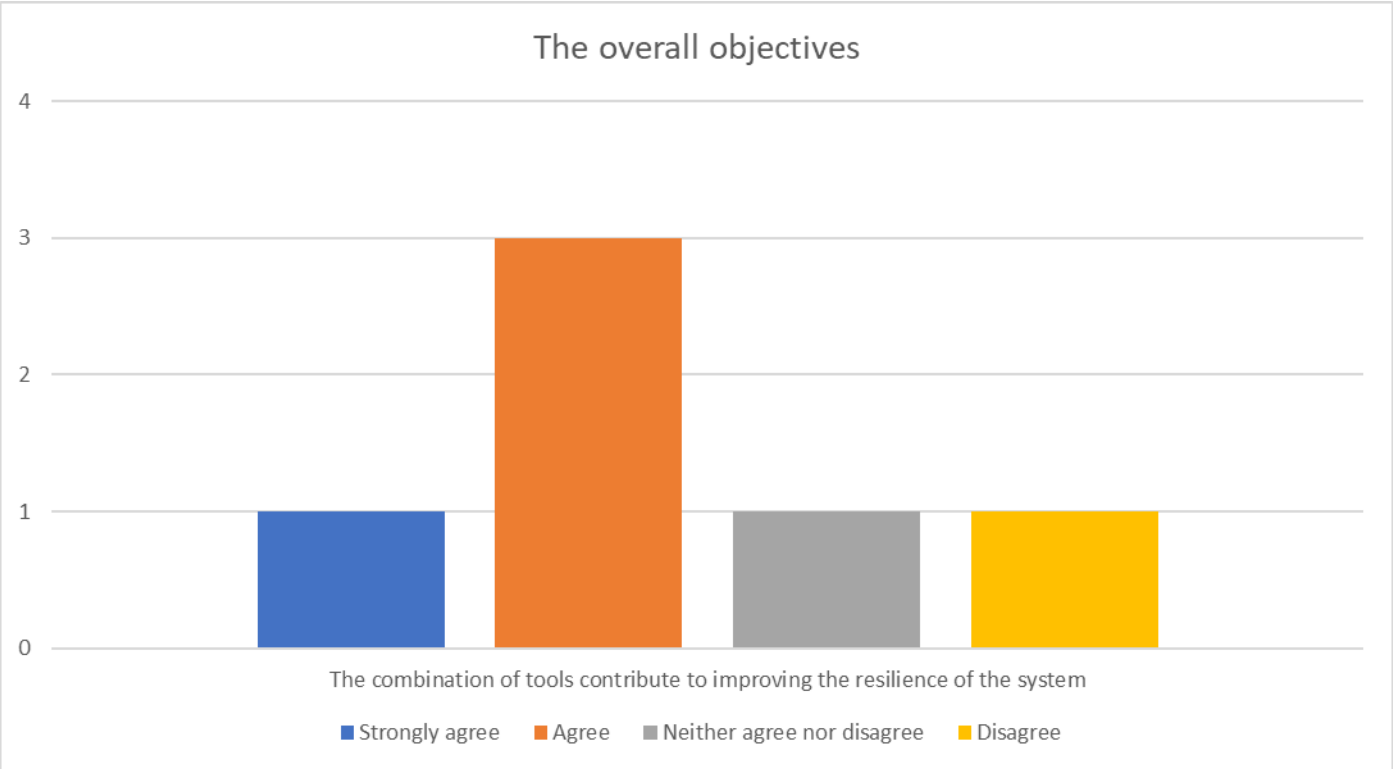

FIGURE 3.35: MDM SIMULATION EXERCISE - THE OVERALL OBJECTIVES IN THE CONTEXT OF THE SCENARIO

Q1: 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*

Q2: 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.*

Q3: What could be improved in the context of this scenario?

- *N/A*

Q4: 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.*

Q5: 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.*

Q6: 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.*

Q7: Any proposals for revisions and/or additions to the requirements and specifications defined to date?

- *N/A*

3.7.2 The organization of the exercise

The pillars in the figure below are expressing the number of given responses. Unfiltered answers to open-ended questions are following the Likert scale figures.

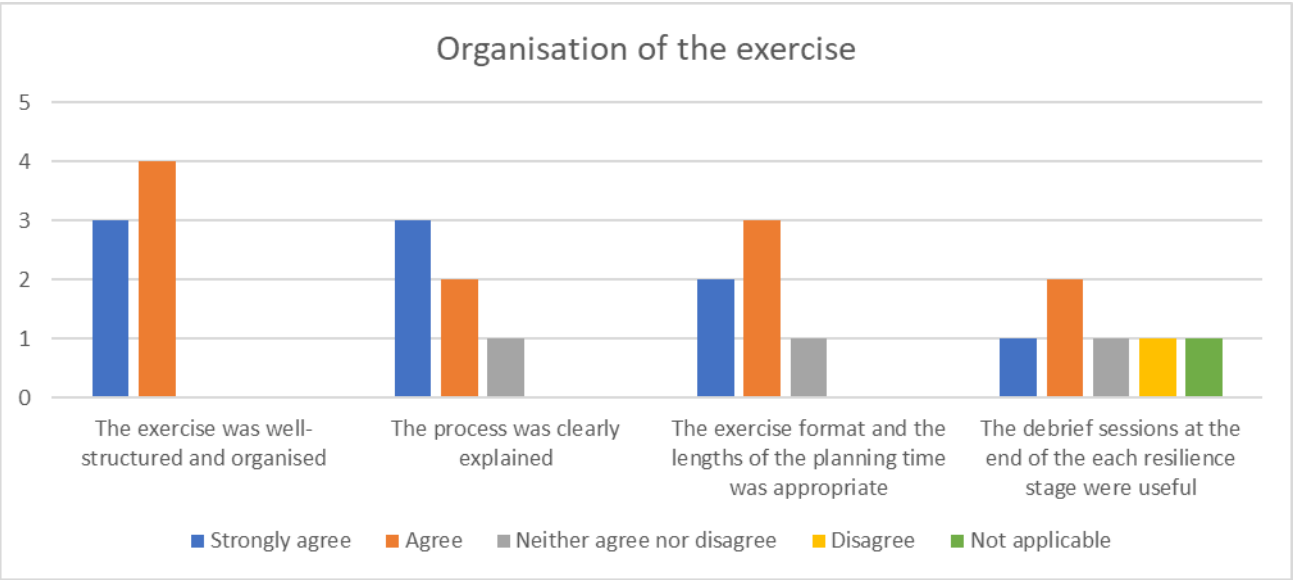

FIGURE 3.36: MDM SIMULATION EXERCISE - THE ORGANISATION OF THE EXERCISE

Q1: 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*

Q2: 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.)*

Q3: 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*

Q4: 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.*

4. Lessons learned

4.1 Lessons learned from first exercise

Looking at the methodology used in the first simulation exercise, and still expecting for the remaining three simulation exercises to occur as of this writing, it is vitally important to gather the lessons learned so that the process can be improved. The Covid-19 pandemic is still ongoing, with bursts impossible to predict. The geopolitical situation is unstable as well due to the war in Ukraine. Therefore, there are considerable challenges even in the very basic function of gathering to a specific location for a few specific days. Optimally, all challenges would be in the conduction of the actual exercise.

The following two sub-chapters will include distilled recommendations for organizing the exercises, and recommendations for organizing the future evaluations. If one single aspect should be pointed out, it is that it should remain a target to increase the number of individual end-user evaluations. The organization of the exercises is important in this respect: how many are and can be invited, who are they and how many will actually attend? Also, the organization of the evaluations are equally important: one cannot force answers to appear on the forms. How much time does one need to answer, and answer with proper consideration? All end-user evaluators should be familiar requirements and specifications included in the D1.4 sections 2.2 and 2.3. The main objective of the simulation exercise is to receive feedback from the end-users on how well these requirements and specifications have been met by the prototype S4RIS and its contributory tools. Too radical changes between exercise will however also may make comparison between results impossible challenging.

Though there will not be a separate deliverable after the second and third exercises, the process will be followed and iterated each time. The final evaluation report (D8.5) will contain a reflection on these iterations.

4.2 Recommendations for future exercises

In light of the data as provided in chapter 3, the following recommendations can be given for the remaining three exercises:

- All tools should be integrated to S4RIS
- 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 also the responses provided informally during the breaks and in follow-up conversations.

4.3 Recommendations for future evaluations

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:

- It is checked 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.

5. Conclusion

5.1 Summary

This deliverable D8.4 presented the evaluation and validation results including lessons learned from the first simulation exercise organized in February 2022 in Madrid. The Madrid exercise was carried out using online and the on-site possibility to attend the exercise due to Covid-19 restrictions. The evaluation was mainly performed by the end-users of the project participating in the exercises and focused on 2 main aspects:

1) The organisation of the exercise.
2) 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 (referencing again to D1.4 for e.g. tool specific requirements/specifications identified)

The results presented in this deliverable are based on the first questionnaires and debriefs from the first exercise. 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 10 persons have represented end-users from the Consortium (and therefore observing the pilot case). There exist no significant differences when 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 deliverable is based on these first 16 responses. Further responses were provided also informally during the breaks and in follow-up conversations.

Based on on-site discussions, end-users positively rated the individual tools as well as the S4RIS platform presented to date. The combination of tools was very positively regarded, with some concerns though related to the Detection & Response phase, where fast and efficient decision-support and crisis management capabilities were considered key, and not all tools supported that.

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.

5.2 Future work

The methodology applied in this deliverable will be further adapted progressively according to the progress of the next period when preparing the exercises. Furthermore, it will be adapted for the two last exercises (Rome and Milano) to take into account both the results of the evaluation of the 2 first exercises. The evaluation will continue in the coming exercises and complementary surveys, as well as group-based techniques, will be used for the evaluation.

The Madrid exercise represented the first simulation exercise, the analysis of the results of all simulation exercises will be done in the deliverable D8.5 – Final version of evaluation report – M22 (July 2022) after all the evaluation material is available. D8.5 will take into account all simulation exercises and the evaluation will contribute to the assessment of the Technology Readiness level, especially for TRL 6 (System/subsystem model or prototype demonstration in a relevant environment) and TRL 7 (System prototype demonstration in an operational environment). It will be used to assess whether the demonstrations/exercises have been performed successfully in a relevant environment. It will also be input into steps after the project to implement the results such as validation of products following also the UK FSR guidelines even more comprehensively.

Bibliography

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

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.

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

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

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

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

ANNEX 1 Glossary and Acronyms

TABLE 1 GLOSSARY AND ACRONYMS

Term	Definition/description
CDM	Comune di Milano
DoA	Description of the Action (Annex 1 to the Grant Agreement)
EGO	Ankara Metro
FGC	Ferrocarrils de la Generalitat de Catalunya
GUI	Graphical User Interface
MDM	Metro de Madrid
PRORAIL	Rail Infrastructure Manager in the Netherlands
RFI	Rail Infrastructure Manager in Italy
SE	Simulation Exercise
S4RIS	SAFETY4RAILS Information System
TCDD	State Railway in Turkey
TOC	Train Operating Company
UC	Use-Case
UIC	International union of railways
UR	User Requirement
WP	Work-Package
WS	Workshop

ANNEX II Metro De Madrid exercise schedule

14:00	**Opening ceremony including presentation of agenda and methodology**				MdM, FhG, ETRA
PREVENTION PHASE - WORKSHOPS/TRAINING					
14:30	BB3D - Bomb Blast Simulation with outdoor and indoor effects (Civil Construction Department)	RINA	14:30	iCrowd - Outdoor stampede due to bomb blast. Assessment CCTV configurations for detecting blind spots (Security Department)	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 second day				
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
11:35-11:50	CuriX – General Presentation (ALL)				IC
11:50-12:00	SAFETY4RAILS Information Systems (S4RIS) Graphical User Interface				UNEW
12:00	S4RIS platform (+all tools*) 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				

ANNEX III Example of debrief questionnaire for Prevention phase 1

SAFETY4RAILS MdM - PREVENTION phase 1 Wednesday 9th PM

Who: end-users: experts from the end-user company organising the exercise and end-users from the Consortium attending the exercise.

When: after the simulation for each resilience stage.

* Required

Part 1: General information

1. Your name *

2. Your organisation/Company *

3. Your position/job in your organisation *

4. Do you consent to the SAFETY4RAILS consortium/researchers contacting you, if required, as a follow-up interview to this research? *

- ◯ Yes
- ◯ No

3/30/2022

5. Do you consent to the SAFETY4RAILS consortium/researchers contacting you, if required, as a follow-up focus group discussion to this research? *

- ◯ Yes
- ◯ No

6. What is your email address or any other contact details (e.g. phone number) SAFETY4RAILS researchers may use to contact you? (if you did not consent, please write "NA") *

7. How would you define your contribution in this scenario exercise? *

- ◯ End-user representative organising the exercise (and therefore actively using the tool)
- ◯ End-user representative from the Consortium (and therefore observing the pilot case)
- ◯ End-user representative outside the Consortium and mainly from the Advisory Board (and therefore observing the pilot case)

3/30/2022

Part 2: BB3d

If you did not attend "BB3d - Bomb Blast Simulation with outdoor and indoor effects", please advance to the next page (part 3).

8. Questionnaire for scenario-based requirement; BB3d 01

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.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Not applicable
The objective was successfully met	○	○	○	○	○	○
The output will help for the prevention phase	○	○	○	○	○	○
The GUI of the individual tool is user-friendly	○	○	○	○	○	○

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

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

3/30/2022

Part 3: CAMS

If you did not attend "CAMS - Proactive asset management and preparedness", please advance to the next page (part 4).

11. Questionnaire for scenario-based requirement; CAMS 02

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.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Not applicable
The objective was successfully met	○	○	○	○	○	○
The output will help for the prevention phase	○	○	○	○	○	○
The GUI of the individual tool is user-friendly	○	○	○	○	○	○

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

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

3/30/2022

Part 4: SECURAIL

If you did not attend "SecuRail - Offline risk assessment (Security Department)" please advance to the next page (part 5).

14. Questionnaire for scenario-based requirement; SECURAIL 3

Enable off-line risk analysis of the metro infrastructure to understand the level of risk for each critical asset during a given hazardous event.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Not applicable
The objective was successfully met	○	○	○	○	○	○
The output will help for the prevention phase	○	○	○	○	○	○
The GUI of the individual tool is user-friendly	○	○	○	○	○	○

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

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

3/30/2022

Part 5: TISAIL/OSINT

17. Questionnaire for scenario-based requirement; TISAIL 2

Provide vulnerability and security gaps assessment, along with risk assessment for each of the operational units in the metro system.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Not applicable
The objective was successfully met	○	○	○	○	○	○
The output will help for the prevention phase	○	○	○	○	○	○
The GUI of the individual tool is user-friendly	○	○	○	○	○	○

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

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

3/30/2022

Part 6: iCrowd

If you did not attend "iCrowd - Outdoor stampede due to bomb blast. Assessment CCTV configurations for detecting blind spots" please advance to the next page (part 7).

20. Questionnaire for scenario-based requirement; iCrowd 02

Provide simulation capabilities to understand better the chances of detection during infiltration/escape per configuration (camera and guards locations) and infiltration/escape total times.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Not applicable
The objective was successfully met	○	○	○	○	○	○
The output will help for the prevention phase	○	○	○	○	○	○
The GUI of the individual tool is user-friendly	○	○	○	○	○	○

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

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

3/30/2022

23. Questionnaire for scenario-based requirement; iCrowd 04

Revealing blind spots and other related vulnerabilities in case of a threat actor trying to escape.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Not applicable
The objective was successfully met	○	○	○	○	○	○
The output will help for the prevention phase	○	○	○	○	○	○
The GUI of the individual tool is user-friendly	○	○	○	○	○	○

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

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

3/30/2022

Part 7: PRIGM

26. Questionnaire for scenario-based requirement; PRIGM 04

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.

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree	Not applicable
The objective was successfully met	○	○	○	○	○	○
The output will help for the prevention phase	○	○	○	○	○	○
The GUI of the individual tool is user-friendly	○	○	○	○	○	○

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

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

3/30/2022

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 1-4. 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"

TABLE 2 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	DATA FAN-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

TABLE 3 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
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

No	*Req.-ID - Need.-ID*	Short name	Objective for the MDM exercise	Integrated (Y/N)	Result of evaluation
MDM-DET-5	DATA FAN-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	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	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

TABLE 4 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	DATA FAN-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

TABLE 5 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

SAFETY4RAILS

Partners:

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