SAFETY4RAILS

ETHICAL COMPLIANCE FRAMEWORK (ECF) -UPDATE

Deliverable 9.2

Lead Authors:UREAD, LAU

Contributors: Fraunhofer, MdM

Dissemination level: Public

Security Assessment Control: Passed

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

D9.2 Update of SAFETY4RAILS Ethical Compliance Framework (ECF)		
Deliverable number:	D9.2	
Version:	1.0	
Delivery date:	20/10/2022	
Dissemination level:	Public	
Nature:	Report	
Main author(s)	Atta Badii	UREAD
Contributor(s)	Tuomas Tammilehto	LAU
Internal reviewer(s)	Stephen Crabbe, Antonio De Santiago	Fraunhofer, MdM
External reviewer(s)	Marco Tiemann	INNO

Document control			
Version	Date	Author(s)	Change(s)
0.1	02/05/22	Atta Badii	Initial Structuring
0.1	01/06/22	Tuomas Tammilehto	Questionniare Design
0.2	14/06/22	Atta Badii, Tuomas Tammilehto	SIA-2 Framework
0.2	03/07/22	Atta Badii	use-cases to pilots to privacy /misuse risks check
0.3	13/09/22	Tuomas Tammilehto	SIA first draft
0.3	14/09/22	Atta Badii	SIA edits and additions
0.4	26/09/22	Tuomas Tammilehto	SIA 2nd draft compiled
0.4	10/10/22	Stephen Crabbe	Advice on the confidential research docs security
0.5	14/10/22	Antonio De Santiago	Advice on privacy risks
	17/10/22	Atta Badii	Compiled in SIA-2
	20/10/22	Atta Badii	Submitted full version
1.0	20/10/2022	Stephen Crabbe	Creation of version 1.0 from V0.5. Security Assesment decision. Update of front cover, this table, footer, disclaimer, abstract. Chapter 2 addition of UIC regarding mailing lists. Addition of footnotes on pages 22 and 24.

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 have to ensure that mitigation steps are taken and communicated to travellers and other users. **SAFETY4RAILS will improve the handling of such events through a holistic approach.** It will analyse the cyber-physical resilience of metro and railway systems and deliver mitigation strategies for an efficient response, and, in order to remain secure given everchanging novel emerging risks, it will facilitate the continuous adaptation of the SAFETY4RAILS solution; this is validated by two rail transport operators and the results supporting the re-design of the final prototype.

TABLE OF CONTENTS

List of tables

List of figures

Executive summary

This document, deliverable D9.2, presents the update on extensions and operationalisation support for ongoing ethical and data protection monitoring and compliance assurance. The deliverable also addresses the user acceptance-social acceptability of SAFETY4RAILS integrated Tools Environment with an extensive post-experience Social Impact Analysis. Finally the deliverable sets out the research finding risk assessment and concludes with a general and use-case-specific ethical and privacy risk assessment of SAFETY4RAILS as presented in respective tables.

The Deliverable structure is as follows:

- **Chapter 1:** Introduction
- **Chapter 2:** Social Impact Analysis
- **Chapter 3:** SAFETY4RAILS Ethical Compliance Framework: Extensions and Implementation Support
- **Chapter 4:** Information Security and Ethical Risks Analysis
- **Chapter 5:** Conclusion

Annexes: I – Ethical Compliance Data Protection Operational Manual, II – Ethical Guidelines for Crisis Communication Management

1. Introduction

Both the above objectives have been delivered through ongoing engagement with the Consortium, in particular, with the Project Ethical and Advisory Boards. Above all operational guidelines to support the implementation of the ethical framework and streamline the adherence of ethical and data protection at the frontline has been the mainstay of our approach in this Project – the results have supported this commitment to combining the framework with the manual level implementation support to facilitate the delivery of compliance. Accordingly this deliverable, D9.2, sets out the results of the seven streams of effort that form part of the above approach. In so doing it provides an update on the in-field support provided by way of follow-on documents and ad hoc online tutorials on the "how-to"s of data protection. As well as ethically guided crisis communications as examples of responsive and timely support for ethical compliance by design.

2. The Societal Impact Assessment of SAFETY4RAILS: Part II (SIA-II)

This second stage of the Social Impact Analysis (SIA-II) is based on an online survey circulated via email among the Consortium members, members of the advisory groups, and other stakeholders who have been involved in various ways with the SAFETY4RAILS project. The invitation (and one reminder) for the survey was sent using the email lists that were created by the Coordinator/UIC during the project: the recipients were thus the Consortium members or others who had given their consent to participate in various SAFETY4RAILS activities. No monetary or other incentives were offered – all answers were given voluntarily and anonymously. The respondents were asked for their consent to participate in this survey and were supplied with all the relevant detail about the purpose and context of this survey (Information Sheet) including how the answers were to be used and how their provided data would be protected. The information included links to the project website (https://safety4rails.eu/), a description of the EU Survey-tool[i] and a link to a form to contact the organisers of the survey for further details. The questionnaire also contained a link to a short video of the SAFETY4RAILS project and its developed solutions (https://youtu.be/Za0LJH87aeM).

3. SIA Implementation

3.1 Methodology – Questionnaire Instrument Design

Often, the quality of data from a survey depends on the size of the sample. However, the representativeness of the sample from which the data is collected is even more pivotal (Fowler, 1998). Altogether 23 respondents gave their answers to this survey, hence presumably nearly 80% of the Partner organisations expressed their views. The respondents were selected (i.e., the invitation link was sent to the recipients) based on their involvement as well as knowledge on the SAFETY4RAILS project and its results. The respondents were probably those who had knowledge on the developed solutions and thus had a motive in sharing their thoughts and giving their comments.

The questionnaire included a managed mix of questions to best enable the respondent's expression of their opinions; this included a seven-point Likert scale (from one to seven stars, seven stars being the highest). The Likert scale has the advantage that it does not seek a simple dichotomic yes / no -answer from the respondent but enables a range of opinions. Thus, quantitative data was obtained which could be analysed with relative ease. The questionnaire was anonymous, thus reducing possible social pressure to respond in any particular way which could have introduced social desirability bias; for example, leading to an overly positive or otherwise expected outcome. Open-ended questions followed the Likert scale questions. Their aim was to enable the elaboration of the answers and/or give concrete examples to endorse the questions/statements. The open-ended questions aimed to generate knowledge about the contingent relationships between the phenomena and their attributes, but more so to produce knowledge about actions that should be taken. Therefore, the questions were both explanatory and normative in nature (Alversson & Sandberg, 2013).

The Likert scale questions, and the open-ended questions were clustered under four themes/sections; as follows:

1. Threat assessment,
2. Risk and crisis management improvement,
3. Improvement of resilience and security, and
4. Practitioners and exploitation.

For a fifth theme/section, an additional method was used: a closed question on the most potential efficiency gains. Lastly, open-ended commenting was invited on any possible issues related to SAFETY4RAILS and its possible outcomes.

In this SIA, the focus was on the future use of SAFETY4RAILS solutions in the above-mentioned contexts and how they would and could impact societies in which SAFETY4RAILS solutions would be in operational use. SIA is very much a future-oriented assessment. It is based on the users' views and is thus very much subjective. However, behind the views is often hundreds of years of experience – the cumulative knowledge of the respondents: this gives credibility. The answers are analysed in this SIA both independently as well as in relation to each other, for example in the following way: the average of the responses was greater on Qx than on Qz, thus indicating that impacts on Qx were seen to be potentially more pivotal than Qz.

First, the mean is considered, as a simple mathematical average of the set of numbers, and then the mode, the value that appears most frequently in a data set, is considered; both tell something about the issues in question. The average weighs every item equally, diminishing the importance of more impactful data points. The advantage of the mode is that it is not affected by extreme values, thus maybe better reflecting the overall consensus.

Following the numerical analysis, the answers to the open-ended questions were examined, and the information that they held informed the analysis re how the respondents saw the possible societal and other impacts. At this stage, we can set out the actual questions as well as the analysis of the answers in detail.

3.2 Facets of the SIA Study

Following discussions with the Partners and considering the questionnaire responses, the following facets constituted the focus of the SIA.

3.2.1 Threat Assessment

This theme/section contained two questions, thus two Likert scale questions and related open-ended questions.

The first question was: How well is SAFETY4RAILS going to benefit the society with enhanced capabilities on identifying new threats?

And the follow-on question was: Please elaborate how? Please give concrete examples.

The respondents gave an average of 5.40 out of 7, and the mode was 5. The average was slightly lower than the overall average of all the questions. Thus, one could argue, that despite the high appraisal, the SAFETY4RAILS solution benefits in identifying new threats were relatively less valued than other elements of future impacts to society.

The answers to the follow-up question revealed the following.

SAFETY4RAILS provided several deliverables for metro and rail operators with an updated overview of threats faced by rail and metro operators in the preceding years. Furthermore, there are also tools for analysing risks which can identify threats which can be considered as being new to the specific metro and rail operators. The tools will enable early assessment of potential threats to systems and operational safety. These may be known types of threat previously experienced or new types of threat, particularly cyber. This information together with the assessed potential impact supports the possible redesign of systems to meet the challenge faced.

According to the respondent, SAFETY4RAILS is going to thus benefit society with enhanced capabilities on identifying new threats, for example through modelling the threats and using tools to identify new threats and plan mitigation against cyber-physical threats. The respondents maintained that the platform works with state-of-the-art systems and data extracted from the latest databases, so that data threats can be identified as promptly and accurately as possible. Furthermore, the fact that SAFETY4RAILS is capable of handling and identifying a multitude of incidents through a single interface, as well as issuing appropriate remedial measures in a timely manner is a great help. In particular, assists in identifying possible threats so the operators may consider them before the threats occur.

The respondents acknowledged that there are already existing systems that aim to identify risks in railway and metro systems, but SAFETY4RAILS brings new tools together and can combine new information to identify risks faster. For example, in modelling the passenger load at a certain station and to identify abnormally high passenger loads. This is important since, not only do growing urban population increases the demand on transportation, but also various societal activities (e.g., mass- events lead to load spikes). This combined with malicious threats may pose extreme challenges, which can be handled with prior preparation based on simulated exercises, including low probability and/or high impact situations both from a technological as well as from an efficient crowd control approach.

Another benefit to society is related to the fact that SAFETY4RAILS includes diverse monitoring tools, which cover most of railway systems potential physical and cyber threats. Some tools developed during the project specifically address this threat topic (e.g., TISAIL and Curix). Furthermore, the SAFETY4RAILS platform is not only capable of identifying emerging threats but also communicating them immediately to the operator. Thus, it enables both the identification of new threats and keeping the crisis managers more informed. Although, for some respondents, more critical than identifying threats, as most are already known, is mitigating those threats and risks.

To sum up, the capability to identify new threats against train and metro transport infrastructure and operational frontline systems, will lead to safer means of transport. By identifying new threats, it is possible to take action against them and therefore the safety of the system can be maintained. The SAFETY4RAILS Tools can provide significant benefits to citizens, businesses, and end-users, such as reducing recovery costs and improving the quality and efficiency of railway/subway services in the detection phase and prevention process and improving network transportation safety and reliability. Also one critical point was that, since the SAFETY4RAILS system will enable the end- user to take decisions mainly on the basis of data and less on the basis of experience or expert judgement, this will strengthen data-driven decision making. Abnormal behaviour detection based on AI, improved interoperability with consideration for improved security, safety and privacy, and an integrated approach linking multiple types of solutions into a single framework are all ways to tackle the threats. Perhaps, a possible integration

with the MISP platform[1] would help to keep technical responsible individuals even more up to date with vulnerabilities.

As a result of the successful completion of the project, the full range of risks faced by railways in general have been addressed. The project has examined the relationship between risks and the impact that they could have on the strategic goals of an infrastructure organisation – this was also a key in dividing strategies and tools for tackling threats.

The second question on threats was the following: How well is SAFETY4RAILS going to benefit the society with enhanced capabilities on detection of new threats? and the follow-up was Please elaborate how? Please give concrete examples.

The respondents gave an average of 5.70 out of 7, and the mode was 5. The average was higher than the overall average of all the questions (5.56). Therefore, indicating enhanced capabilities on detecting new threats was of relatively more value than other elements of future impacts on society.

The responses to the follow-up question re the concrete examples, adopted much the same lines as those for the first question. Some statements were almost identical. For example, stressing less on detecting than on mitigating.

Overall, it was stated that SAFETY4RAILS helped to detect the threats (ranging from cyber threats to natural hazards) so the operators could take precautions before the threats occurred. The more types of threats that could be managed, the more protection for commuters. This is supported by complex data analytics, with continuous monitoring of various sensor data capable of identifying combinations of circumstances, which are not easily anticipated from singular observations. Monitoring the dynamic/temporal behaviour of the interconnected systems in various traffic conditions can reveal additional dependences of individual factors, not accounted for in previous design/operational stages of the railway systems, thus providing potential alerts re anomalous behaviours.

SAFETY4RAILS includes diverse (monitoring) tools, some specifically addressing this topic (RAM2) and d covering most potential physical and cyber threats to railway systems. Furthermore, there are tools for detecting threats during operations, for example, anomaly detection. The main decision support platform also enables the correlation of alarms from different tools leading to a higher level of insight and connected detection. However, the users will need to gain experience in use of the tools to benefit in terms of detecting new types of threat as opposed to known types of threat.

It is also through the above threat handling capabilities use that the network transportation safety and reliability are improved, as well as the understanding of the detection phase and prevention process. There is no doubt that all threat detection tools, such as Configuration, Modelling, Indicator, and Threat Behaviour, provide significant benefits for citizens, businesses, and users alike. A variety of approaches and requirements can be found for each of these categories, depending on the railway infrastructure in the area. The integration of these capabilities within a single platform supports generalisable threat detection approaches and thus flexibility in detecting a variety of threats including possibly ones that have not been seen before. As a result of these efforts, railways and subways operators would be able to reduce their incident recovery costs and improve service quality.

Targeting public transport services will surely improve a general feeling of safety and security in the public, especially in the context of preventing and protecting against the risk to citizen's life. However, this needs to be communicated to the public, so that they are aware of the existence of such safety protection measures and remain vigilant to the ever-present likelihood of threats translating to attacks.

[1] www.misp-project.org/

3.2.2 Risk and Crisis Management Improvement

Moving on from threat assessment the next questions were on Risk and Crisis management. This theme/section contained three questions. **The first question** was: *How well is SAFETY4RAILS going to benefit the society with enhanced capabilities on forecasting and management of new threats?*

And the follow-up question was again: *Please elaborate how? Please give concrete examples.*

The respondents gave an average of 5.32 out of 7, and the mode was 6. The average was second lowest of all the questions, however, the mode was quite high, indicating that some respondents were not very optimistic giving low ratings.

The answers to the open-ended follow-up question led to the observations as set out below:

Again, a reminder had been given that there did exist other systems to forecast new threats in railway and metro systems. Also highlighted was that SAFETY4RAILS included relevant data analysis tools to provide insights and forecasts from existing events detected - as demonstrated using RAM2 system, and some tools developed during the project are specifically addressing this topic, for example, TISAIL & Curix identify threats.

The benefit of SAFETY4RAILS arises from integration of domain modelling, data fusion and situation assessment techniques and tools. There are tools that contribute to all phases of a resilience cycle as represented by: identification, prevention, detection, response, and recovery. These include simulation tools to model what-if scenarios. All these tools can support forecasting and management. Starting from one threat, the system can compute the effect that it could have on the network taking also into account the people who are in the stations, for example. The AI-based threat and risk prediction is still in its infancy, mainly focusing on abnormality detection. A comprehensive vulnerability analysis of such complicated infrastructure inter-linked with other inter-dependent infrastructures is still not yet realistic and was beyond the scope of this project. However, in recent years, technology forecasting has relied heavily on data, and data has had a positive impact on manufacturing and infrastructure in many ways. To prevent infrastructure disruptions and to ensure the resilience of infrastructure services to society, a powerful platform has been provided that includes 31 participants and 18 smart tools for predictive analysis. Accordingly, it is expected that forecasting accuracy and reliability for those who use the transportation network will improve because of the tools available within the SAFETY4RAILS platform. In the future, to benefit society in the forecasting and management of new threats, AI will be needed, but also data for model building and refinement as well as proper training and implementation for the end-users.

Data privacy remains the main challenge that needs to be addressed for the solutions to be successful. Some saw significant challenges arising from lack of a centralised system to manage new threats and risk in the railway or metro eco system and having to maintain preparedness for adverse situations under extreme transportation load and/or weather conditions; this calls for improvement in the training of personnel, as well as testing the interoperability of various technology solutions - SAFETY4RAILS tools can support these objectives.

The respondents commented that AI-based approaches including heuristic and abnormality detection still lack sufficient reliability and require human intervention. However, they should offer the capability to reduce the number of false alerts and attract the attention of human operators to possible threats and this is supported by the integrative tools framework of SAFETY4RAILS.

The second question of this section was: How well is SAFETY4RAILS going to benefit society with enhanced capabilities on knowledge sharing with stakeholders?

And the follow-up question was again: Please elaborate how? Please give concrete examples.

The respondents gave an average of 5.00 out of 7, and the mode was 4. The average and the mode were the lowest of all the questions indicating that enhancements in knowledge sharing are not seen as having a major impact on society.

The answers to the open-ended follow-up question led to the observations as set out below:

The benefits to the society, i.e., the positive impact, will obtain through the framework for crisis communications management and knowledge sharing between the frontline incident management and other stakeholders. The

SAFETY4RAILS platform is designed to obtain and correlate information. A stakeholder with this information can share it with all relevant stakeholders. For example, one deliverable focussed specifically on crisis management, identifying an "ideal" tool for crisis management with multiple stakeholders. Thus, the SAFETY4RAILS platform could in principle be implemented relatively easily to share information between different stakeholders. Operators and authorities could fine tune response plans for challenging situations with multichannel communications as well as standardised data sharing interfaces between personnel and digital equipment alike.

In short, SAFETY4RAILS has some tools capable of knowledge sharing. Likewise, it is obvious that the sharing of knowledge will lead to an overall safer system since it enables parties to benefit from the experiences and knowledge of other parties. However, the project inter-operational capabilities were mainly offered via the message broker and JSON message exchange, and they showed some limitations. For example, they could introduce latencies in case of a complex even scenario and overloaded message cues, especially in the case of emergencies with many sub-systems pushing their own alerts to the system.

Nevertheless, through sharing of knowledge, stakeholders will be able to make better decisions during emergency or crisis situations, build a safer community and learn from historical incidents, reduce the stress experienced when facing hybrid physical and cyber incidents, retain knowledge for end-user staff, and improve the overall experience of end-users: a significant role in crisis management. However, the current SAFETY4RAILS capability in this regard is at a proof-of-concept level, although offering potential for the future improvement of knowledge sharing -for example, better ways of collaborating and building collective knowledge, supporting a learning system-of-systems to support improved customer experiences.

Some respondents felt that although the involvement of UIC, EOS and end-users from the railway and metro sectors was seen as highly beneficial to share knowledge with stakeholders, there was still more potential for knowledge sharing with the users to be realised. In future, more attention must be paid to this, and the goal should be to widen and deepen the sharing and retaining (organisational memory) of knowledge to support safety, security and efficiency at all levels of infrastructural resilience engineering and the operational frontline.

The third and final question of this section was: How well is SAFETY4RAILS going to benefit society by enhanced capabilities on reacting to/impacting on evolving threats?

And the follow-up question was again: Please elaborate how? Please give concrete examples.

The respondents gave an average of 5.53 out of 7, and the mode was 5. The average was lower than the overall average, thus indicating that the issues raised in the question was not deemed as having a relatively very high impact on society.

The answers to the open-ended follow question revealed led to the following observations:

The respondents remarked that the SAFETY4RAILS framework supports the operators in better decision making and an improved ability to evaluate the outcomes of their actions when facing potential attacks and incidents. To achieve the most efficient results, SAFETY4RAILS tools support efficient and rapid situation assessment. This is supported through context-aware semantic threat-severity-based risk assessment and responsive crisis management improvement. Again, there are already systems which react to evolving threats in railway and metro systems, but SAFETY4RAILS integrative approach combines new information to react to threats faster. Many of the tools are AI-based, thus they will be able to filter out evolving threats in the system. With state-of-the-art administrative and technical controls in place, predictive estimates of actual impacts of threats could be made, as well as fast analysis of applicable variations of response/mitigation measures, thus allowing optimisation of these activities, assisting high-level dynamic decision making.

The SAFETY4RAILS platform was seen to be capable of computing from an early threat the correlated ones that could affect elements of the system. This is related to resilience and predictive modelling capabilities. It was emphasised that such capabilities could only be tackled using abnormality analysis (involving challenges in distinguishing harmless changes that might be genuine from actual threats) as well as with heuristic methods that unfortunately still cannot reliably accommodate the prediction of new types of risks. Although the social effect might be to offer higher levels of safety, the realities might be quite different. In the case that the system fails to respond correctly, social disillusion might result in a high level of distrust.

To sum up, the SAFETY4RAILS framework deploys an integrated solution stack of tools to improve operational safety and security in many ways, including better monitoring of attacks, reducing physical dangers, and keeping people safe. This will ultimately enhance the safety of the public and security of data that it depends on, thus reducing risks of critical events.

3.2.3 Improvements in Resilience and Security

Improvements in resilience and security are obviously very important for projects such as SAFETY4RAILS. Therefore, this section contained four main questions related to these twin objectives; each of which was followed by the subsidiary questions.

This first question was: *How well is SAFETY4RAILS going to benefit the society in relation to the goal of reduction of incident response time with decision support?*

And the follow-up question was again: *Please elaborate how? Please give concrete examples.*

The respondents gave an average of 5.67 out of 7, and the mode was 6. The average was higher than the overall average, thus indicating that the security question, particularly reducing response time, were seen as important operationally but also could have a real impact on society.

The answers to the open-ended follow-up question led to the observations as set out below:

User-friendliness of the platform and its tools was highlighted to be one of the key elements in reducing the response time along with the ability to display all (near real-time) relevant information, as well as decision recommendations. Clearly, the enhanced decision support may (and should) lead to response time efficiency. However, the quantification of any efficiency gains depends on individual operators and the overall architecture and processes implemented, thus a direct estimation is difficult to arrive at. Shorter response time also means a better chance of mitigating cascading effects and therefore a safer system altogether.

SAFETY4RAILS involved simulation exercises that improved end-user confidence, peer acceptance, staff skills, and empathy. The end-users benefitted from smart tools to be used during realistic activities based on four simulation exercises with various scenarios. It is expected that the simulation exercises, which show-cased how the capabilities of the SAFETY4RAILS could be exploited, would enable the end-users to see how they could best exploit the platform to support safety and availability of non-stop transportation services, as well as reduce recovery time after any kind of incident by using these tools. In this way by supporting the operators to maintain safe, reliable and efficient transportation services, SAFETY4RAILS, contributes to socioeconomic improvement.

Lastly, in reply to this question one respondent openly admitted that s/he was not sure. And how could s/he be when SIA is about future expectations? Nonetheless, broad agreement was evident about the positive impact that could be achieved through integration of domain modelling, data fusion and situation assessment techniques and tools to support higher quality decision making to support the operational frontline.

The second question was: *How well is SAFETY4RAILS going to benefit the society with cos- effective technological measures?*

And the follow-up question was again: *Please elaborate how? Please give concrete examples.*

The respondents gave an average of 5.65 out of 7, and the mode was 5. The average was slightly higher than the overall average (5.65), thus indicating cost effectiveness is an issue that could have a real and meaningful impact on society.

Here are some observations could be made based on the answers to the open-ended question that followed:

Again, the respondent pointed out that there are already systems for cost-effective technological measures in railway and metro systems. However, SAFETY4RAILS integrates all relevant tools that could be needed to evaluate cost-effective measures faster, e.g., in predicting high passenger loads before and after a large event such as a

football game (at a particular station), and how to re-direct passengers to the surrounding stations providing support to evaluate which further transport modes (bus, trams etc.) as needed.

Further, some of the tools can assess asset status and the financial impact of events as well as a variety of response measures (both immediate and longer term). Also, more fundamentally, the combination of advanced pre-matured tools from different vendors, together with COTS technologies can create a cost-effective solution for fast deployment.

Technological measures for monitoring cyber related incidents and cyber-physical incidents have been investigated and demonstrated in the project and can be used in the railway eco-system. An obvious aspect is that if one stakeholder is faced with an issue, others will gain information about similar issues. This will reduce costs.

It was highlighted that, since most of the end-users are funded from public sources, they are responsible to ensure that they operate in a cost- effective manner. The respondents pointed out that a smart tool is widely accepted as the key driver of infrastructure budget planning. SAFETY4RAILS budget planning support is targeted on fixing vulnerabilities to specific railway incidents, this would support the objectives of safety, security and operational continuity through optimising maintenance planning and preparedness and resilience investment planning.

The third question was: *How well is SAFETY4RAILS going to benefit the society with real-time management resilience?*

And the follow-up question was again: *Please elaborate how? Please give concrete examples.*

The respondents gave an average of 5.41 out of 7, and the mode was 6. The average was lower than the overall average (5.65), thus indicating that the impact of real-time management was deemed relatively less significant. However, the mode being quite high indicates that there might be a high level of variation, i.e., a few respondents scored this question very low.

The answers to the open-ended follow-up question led to the observations as set out below:

The respondents pointed out that since all circumstances in life are continuously evolving, all systems need to be responsively adaptive to provide the appropriate support for the users. SAFETY4RAILS aims to do this closer to real-time. Real-time collection and integration of data on operational systems and passenger involvement in any situation supports decision making to prevent further escalation and minimise damage in human and/or equipment costs. Many respondents pointed out the capabilities of the SAFETY4RAILS tools for real-time threats assessment. Some tools contribute to all phases of a resilience cycle (identification, prevention, detection, response, and recovery). The identification of threats can lead to the preparation of mitigation steps to be implemented in the response phase. The near real-time detection of threats will support near real-time management of resilience. In addition, in the response phase, specific mitigation measures can be modelled for their contribution to resilience; thus, supporting the optimisation of resilience planning.

Further remarks were that with the SAFETY4RAILS platform, the different stakeholders could leverage shared learnings to support the timely deployment of optimal safeguarding measures proactively instead of simply reacting to an incident or attack. Also highlighted was the fact that there exists a growing trend for the selection and prioritisation of safeguarding measures to be undertaken in a decision support environment that could deploy various models beyond the use of the tools integrated within any particular platform; for example, using modelling informed by behavioural science, applied ethics, and cultural and organisational theory - SAFETY4RAILS would provide an effective integrative support to policy and decision environment.

The fourth and final question of this section was: *How well is SAFETY4RAILS going to benefit society with its multi-modal infrastructure approach?*

And the follow-up question was again: *Please elaborate how? Please give concrete examples.*

The respondents gave an average of 5.44 out of 7, and the mode was 5. The average was lower than the overall average (5.65), thus indicating that the contribution of multi-modal infrastructure to any social impacts of SAFETY4RALS was relatively insignificant. The mode was also within general average line which supported the low impact thesis.

The answers to the open-ended follow-up question led to the observations as set out below:

The multi-modal infrastructure approach in railway and metro systems is not a novelty as such, however, SAFETY4RAILS integrates the relevant tools to enable operators to be more effectively prepared. A multi-modal infrastructure was deemed as integral to the solution stack as specified to support the operational frontline of railways and metro systems. Specifically, this would support the assessment of the impact of threats and determination of the potential mitigation measure(s) which could be modelled and analysed in the identification and response phases of the resilience engineering pipeline.

A layered architecture of tools as the enabling building blocks of X-as-a-Service can be composed as a customised configuration of use-cases available through the SAFETY4RAILS framework responsive to the decision-making needs of particular teams within the railway systems. This was a necessity when aiming for optimal deployment of safeguarding measures since transport systems are inter-linked and react to and on each other. Otherwise, solutions will be sub-optimal and possibly have a detrimental effect on each other. Further, managing different transport modes within a unified framework enables the sourcing of temporary alternatives, enables reduction of load spikes (e.g., via optimal activation of reserve capacities combined with a reduction of access at critical crossing/transfer locations, etc.).

The project addressed a multi-modal infrastructure approach in a very effective manner, since it was highly focused on the demonstration of a Partner's tool in their multi-modal transport system, although the SAFETY4RAILS system mainly targets railroads, and transport multimodality aspects have not been fully addressed.

Nevertheless, with the SAFETY4RAILS platform, multimodal transportation can be enhanced in a number of ways; advantages include:

- saving time and effort,
- reducing costs,
- enhancing handling and delivery efficiency,
- increasing transport security,
- keeping track of one contract,
- responsiveness to cyber-physical and cyber-attacks.
- Integrated solution stack for critical infrastructures protection.

3.2.4 Practitioners and Exploitation

The SIA questionnaire also addressed the practitioners and exploitation with a set of three questions.

The first question of this section was: *How important is the user training with respect to SAFETY4RAILS components?*

And the follow-up question was again: *Please elaborate how? Please give concrete examples.*

The respondents gave an average of 6.00 out of 7, and the mode was 7. Both ratings were the highest, thus indicating that the impact of training was deemed to be critical.

The answers to the open-ended follow-up questions led to a widely shared view emerging- as set out below:

It was made very clear that the SAFETY4RAILS system only works effectively if it is used correctly. Words such as must, critical, very important, necessary were used in the responses. Thus, the training courses for mastering the system are vital, because otherwise the platform would not be fully or properly deployed. Furthermore, many of the tools are new, and practitioners could use them only after they are familiar with them, therefore training is essential for using the tool and also for user's acceptance of the system. Some said that rehearsal and/or simulation exercises should be mandatory - only after gaining knowledge as to how the components of the platform work, can the operator use the platform in the most efficient way.

Thus, to support the efficient and effective deployment of the SAFETY4RAILS system, as cloud services online, user training content must be available as a sort of a digital user manual.

Training and deployment of the SAFETY4RAILS platform helps railway end-users gain and retain skilled staff, supports preparedness training to dealing with incidents and improves productivity. Additionally, infrastructures with assets that are actively engaged and dedicated have a higher productivity rate.

It must be noted too that, thus far, there is a limited SAFETY4RAILS training capability online and more hands-on sessions offering customers an opportunity to "play" with technologies is needed.

The purpose of security awareness training is to minimise risk, and prevent and mitigate threats to public safety, financial loss and brand reputation due to a failure to ensure security.

The second question of this section was: *How important is demonstrating SAFETY4RAILS operational performance?*

And the follow-up question was again: *Please elaborate how? Please give concrete examples.*

The respondents gave an average of 5.60 out of 7, and the mode was 7. Both ratings were high, especially for the mode, thus indicating that demonstrating the operational performance is indeed important and has an impact on society.

The answers to the open-ended follow-up questions led to the observations as set out below:

The demonstration: use-cases from the real-world railway systems operational frontline show-casing the functionalities of the system and its performance assessment. These are very important, since many of the tools are new and practitioners will be using them while being unfamiliar with the new technologies. Demonstrations are key in enhancing the user's acceptance of these new technology components. The demonstrations are important from another point-of-view: they will motivate specific tool providers to address the specific problems of end-users in their existing operational and technological environment. This is essential for solution providers, as the railways and metro systems require specific solutions, compliant with specific safety standards and interoperability requirements.

With the demonstrations the various benefits and opportunities can also be shown to potential customers.

During the project several live demonstrations on different scenarios at railway sites were held, which was an impressive achievement according to one respondent. The feedback from each simulation exercise was that the potential value of the S4RIS platform with its tools based on end-user need/choice in actual daily operational implementation was recognised. More physical interaction would have been even more productive, but the COVID-19 restrictions made it difficult to hold physical meetings.

Demonstrating operational performance is essential in convincing customers to use such technologies in a security critical operational context.

The third and final question of this section was: *How important is exploiting SAFETY4RAILS results?*

And the follow-up question was again: *Please elaborate how? Please give concrete examples.*

The respondents gave an average of 6.00 out of 7, and the mode was 7. Both ratings were the highest, thus indicating that exploitation should be central to societal impact.

The answers to the open-ended follow question led to the observations as set out below:

Exploitation of the results would help realise the business and societal benefits of deployment of the SAFETY4RAILS Project as well as enable the evolutionary enhancement of the system through usability evaluation and responsive future refinements -in short: exploitation helps ensure that this platform works well in every situation.

Thus, exploitation was seen as being very important, as one respondent pointed out: an R&D project must be closely linked to the market needs and be exploitable by the real customers, clients, and end-users. The exploitation routes are evolving, but steps are in place.

Added value plays a critical role here. Demonstrations, exploitation and training exercises such as those in the SAFETY4RAILS project all serve to provide information about use-scenario, end-user's objectives and needs and the effectiveness of the training tool in real-world situations. Most tools in SAFETY4RAILS were prototypes and/or results of applied R&D, and their further development could benefit from end-user feedback arising from any exploitation/demonstration/training opportunity in the operational context of the transport services.

3.2.5 Potential Efficiency Gains

Regarding this section/theme, the respondents were asked to tick a box in order to reply to the following questions: Which one of the following types of potential efficiency gains that may arise from deployment of SAFETY4RAILS do you think to be the most important? (You can select one or more answers).

And the possible answers were:

- Time to Decision
- Time to Response
- Operation Maintenance Planning & Resilience Engineering
- Operational Safety Maintenance Costs
- Operational Carbon Efficiency
- Any other Efficiencies as may be also relevant from your perspective. (For this last item, a space to add ones' own answer was given.)

The answers formed the following table:

TABLE 1: RANKING POTENTIAL AREAS OF EFFICIENCY GAINS PERCEIVED BY STAKEHOLDERS AS ARISING FROM SAFETY4RAILS DEPLOYMENT

List of Importance of Potential Efficiency Gains	1st place	2nd place	3rd place	4th place
Time to Decision	82 %	0 %	0 %	0 %
Time to Response	18 %	78 %	0%	0 %
Operation Maintenance Planning & Resilience Engineering	0 %	17 %	62 %	0 %
Operational Safety Maintenance Costs	0 %	6 %	38 %	100 %

Based on the answers, it is evident that the efficiency gain area with the most potential arising from deployment of SAFETY4RAILS is the *Time to Decision*. Over 80 per cent of the respondents ticked this as being the most important. The order of the rest also transpired to be very evident: the second place went to *Time to Response*, as 18 per cent of the respondents gave it first place and 78 per cent second. The *Operation Maintenance Planning & Resilience Engineering* were in third place, equally clearly and *Operational Safety Maintenance Costs* was ranked as the fourth. None of the other answers, i.e., *Operational Carbon Efficiency* or respondents' own suggestions were given any mention.

Thus, it can be stated that efficiency related to time function is what the respondents hope and/or anticipate from SAFETY4RAILS, i.e., faster, quicker etc. decisions and responses.

An illustration of all the answers can be seen here below in a form of a word cloud:

FIGURE 1: THE QUESTIONNAIRE RESPONSES WORD CLOUD

3.3 SAFETY4RAILS SIA–RRR AXIS

SAFETY4RAILS, as a publicly funded project, was implemented by a Consortium that enabled teamwork between the end-users and technology developers as well as researchers from domains of social sciences and humanities (SSH). The inputs of SSH were specifically needed in ensuring research toward both ethical and societally acceptable solutions and in highlighting the societal impacts of the developed technologies as per the stakeholder-centred Social Impact Analysis studies conducted in Period 1 and Period 2 and presented in deliverables D9.1 and here in D9.2 respectively. This work has been consistent with and supportive of the *Responsible Research and Innovation* (RRI) approach. RRI can be seen as part of the innovation and development process as an approach to ensure that the innovation outcomes are ethically sustainable and societally acceptable. Consequently, the analysis of societal impacts is very much intertwined with the RRI, since Societal Impact Assessment examines not only the ethically acceptable and societally desirable outcomes but also the possible effects of the developed solutions on the society.

It has been said that there are four main characteristics in the RRI approach/process for a project (Aidinlis & Gurzawska, 2021):

1. Inclusion (this was present in SAFETY4RAILS with the substantial participation of the practitioners and end-users);
2. Anticipation, i.e., the project assesses continuously the benefits and risks of its outcomes (see, D9.1 and the first round of the Societal Impact Analysis);
3. Reflexivity, i.e., reflecting on values and beliefs during the research process (also taken into account during SAFETY4RAILS, e.g., the first round of SIA but also in following research ethics principles); and
4. Responsiveness, i.e., the capability to change practices, processes, customs, structures, and systems (this was present in SAFETY4RAILS, since the project has been taking the practitioners feedback into account during the development work).

To capture the essence of the above-mentioned elements, a research project such as SAFETY4RAILS would require a range of different assessment methods: this SIA being one.

SIA concerns the clarification, as far as possible, of the future consequences of a current or proposed action, in our case, this was the deployment of the SAFETY4RAILS tools, and the associated societal impacts - environment, health, human rights, although all important, constituted the secondary tier of concerns within the scope of this study.

The first Societal Impact Analysis (results published in the early stage of the project in D9.1) was based on the perceived impacts as viewed prior to the development of integrated SAFETY4RAILS tools development, whereas this second analysis is based on actual assessment of the stakeholders' views after the realisation and piloting of the SAFETY4RAILS tools, and as such is expected to provide a more realistic, reflective and reliable analysis of the SAFETY4RAILS' Societal Impacts.

However, SIA is predicated on the projection of future effects and as such is fraught with uncertainty. The famous physicist, Niels Bohr, a Nobel Laureate, has said (allegedly) that "predicting is difficult, especially predicting future". Much of the analysis of possible societal impacts is about predicting future. Furthermore, as Sören Kierkegaard so eloquently puts it – "one cannot seek for what he knows, and it seems equally impossible for him to seek for what he does not know. For what a man knows he cannot seek, since he knows it; and what he does not know he cannot seek, since he does not even know for what to seek" – we too have only touched aspects and areas that our imagination can capture. SAFETY4RAILS could have impacts, and most probably will have, that are not emerged through this analysis and the impacts elicited may turn out to be more, or, less significant than anticipated.

3.4 SAFETY4RAILS SIA -Summing UP

In conclusion, the impacts indicated through our SIA study as being the most likely to arise from the deployment of SAFETY4RAILS can be summarised as follows:

Threat assessment

SAFETY4RAILS Threat assessment could have a beneficial social impact with enhanced capabilities for identifying new threats and mitigation against cyber-physical threats.

The tools can provide significant advantages for citizens, businesses, and end-users, such as reduced recovery costs and improved quality of railway and/or subway services, energy and time efficiency gains, increasing knowledge in the detection phase and prevention process, and improving network transportation safety and reliability.

Risk and crisis management improvement

The benefits of SAFETY4RAILS in risk and crisis management improvements arise from integration of domain modelling, data fusion and situation assessment techniques and tools. The positive impact is expected to materialise through the framework for crisis communications management and knowledge sharing between the frontline incident management and other stakeholders.

Through sharing of knowledge, stakeholders will be able to make more effective decisions during emergency or crisis situations, build a safe community and learn from historical incidents, reduce stress experienced in case of more sever incidents such as combined physical and cyber-attacks; retain knowledge for end-user staff, and improve the overall experience of end-users. Accordingly, SAFETY4RAILS can provide organisations with enhanced decision making, responsive actions and improved ability to evaluate the outcomes of their actions in countering potential attacks and incidents.

Improvement of resilience and security:

SAFETY4RAILS integrated multi-modal infrastructure can support its end-users in reducing the Time-to-Respond as well as dynamic responsive action supported by the display of near real-time information on the operational and incident management frontline as well as decision recommendations.

Practitioners and exploitation:

Training courses for mastering the system will enable the practitioners to best use the SAFETY4RAILS tools once they are familiar with the capability of the tools as well as their functionalities. Also, pivotal is this R&D project has remained closely linked to the Railways stakeholders as operators and, through them, to their customers (passengers/citizens).

Potential Efficiency Gains:

The respondents hope and/or anticipate from SAFETY4RAILS: faster, quicker etc. decisions and responses.

The impacts of SAFETY4RAILS are scientific, economic, societal, and democratic benefits and/or enhancements – support for enhanced performance capabilities being the cross-cutting theme. SAFETY4RAILS innovation has contributed new insights, made the science behind the solutions known and thus increased trust. The tools also could support societies toward a better alignment of research with societal needs given that secure and safe transportation and (carbon) efficient mobility is very much a current and strategic objective of European societies.

The range of SAFETY4RAILS tools would also lead to some democratic benefits, since they contribute to better informed data-driven and thus evidence-based decision-making and as such support Accountability.

Considering all the potential direct impacts and possible secondary effects (multiplier/side-effects), it can be argued, with some certainty, that overall, the SAFETY4RAILS possible impact, including its multiplier/side-effects, will be positive to the society. However, various ethical issues (starting from respecting fundamental human rights) need to be taken seriously in the future use of SAFETY4RAILS solutions (as much as they have been during the project): ethically sustainable and societally acceptable solutions are the only way the outcomes will positive. This is yet another key for success.

4. SAFETY4RAILS Ethical Compliance Framework: Extensions and Implementation Support

To ensure full compliance, at the operational frontline, with respect to the European Data Protection (EU) 2016/679 (GDPR), within Task9.1, the SAFETY4RAILS Ethical Compliance Framework was developed and presented in D9.1 as a set of purposes, contexts and data typology check tables derived from the collective analysis of all the Task Teams' the planned activities within the project and the extent to which these would involve any personal data processing. The resulting Framework included explicitly actionable sequences of steps to be taken by the Data controller to determine whether any proposed form of data processing given its scale, purpose, context, could be permitted under the applicable legal directives and if so any whether any modifications had to be enforced and accordingly the legal basis on which any data processing could proceed compliant with the requirements both of GDPR and any other jurisdictions involved as the case may be.

Any such framework would need to remain responsive to the evolution of stakeholders' requirements in particular any changes in proposed data processing plans as well as the evolving needs of the participants for extensions and clarification to support continuous compliance assurance. Accordingly in period 2 further elaborations of the Safety4Rails Ethical Compliance Framework have been provided to ensure that there exists an integrated support environment for the implementation of the framework by way of what essentially amounts to an operational manual for SAFETY4RAILS Ethical Compliance including cross-jurisdictional harmonisation of compliance management across EC - non EC Partner organisations. As such the framework has ensured streamlined and continuous ethical compliance support through the results of the seven streams of effort for ethical compliance management as follows:

1. **Ethical Compliance Framework Console**

- In summary the framework including check and decision tables (Data Controller's Ethical Console) has evolved through further analysis so that the socio-ethical and legal compliance within the project could be maintained starting with D9.1, it addressed the following key aspects of such compliance as follows:
- The Data Controller's Ethical Compliance Framework Console tabularised the ethical compliance decision pipeline as a look-up table starting with each proposed data processing, its Context-Purpose (Ps & Cs) and setting out the respective categoric data protection safeguarding measures and Ps-&-Cs-specific legal permission and if so the approved legal basis and conditions under which the data processing could be allowed to proceed. The Ethical Console, as such, was to be updated in light of any new unforeseen data processing that may be proposed.
- The Requirement for Explicit "Healthy Consent" as part of the legal basis for processing essential personal data as necessary; ensuring that any consent seeking process is conducted appropriately, meaningfully and where it is necessary, practicable and meaningful to do so.
- Compliance with Healthy Consent was supported by the Ethical Compliance Framework shortly after the commencement of the project, with the "SAFETY4RAILS GDPR Consent Form Constructor Template for prospective data-subjects as respondents/participants to questionnaire/interviews/stakeholder-workshops". This was designed to cover both consent for research participation and the processing of personal data (as relevant). It includes informed consent/assent procedures to be followed and the content options to be included in consent forms. A SAFETY4RAILS project information sheet and a volunteer consent form were included and the entire package translated into the relevant local native languages and made available to data subjects a priori as required. It included full, clear and explicit information about the boundaries, scale, scope, modalities and safeguards appertaining to each of the facets and phases of the data operations end-to-end throughout the lifecycle of the data each data proposed to be acquired.
- Typology of data types processed with SAFETY4RAILS and the respective Purpose(s) and Context(s) of their usage. to fulfil the GDR requirements as applicable e.g. in relation to the principles such as Purpose Limitation, Data Minimisation etc and the requisite procedures
- This set out data modalities and respective privacy-sensitivity-specific approaches to de-identification of any personal and otherwise linkable data to be processed.

- Localisation of sub-system development (e.g. model training and testing) to avoid transfer (to non-EC countries) of any mistakenly included and identifiable personal or linkable data of real persons. Notwithstanding these data transfer avoidance measures, any unavoidable data transfers must fully comply with GDR as well as the local data protection regulations of all countries involved.
- As for any data transfers involving Partner organisations located within non-EU countries; the following guidelines were applied re data transfer, particularly regarding minimisation and de-identification. In all Data Processing within a collaborative project involving both EU and non-EU countries, it is mandatory that the legal and data protection regulations of all jurisdictions involved are complied with. Accordingly, SAFETY4RAILS Partners from Non-EU countries had to ensure that any data processing conducted by them remained compliant with the data protection requirements of their country which in almost all cases should was consistent with GDPR requirements.
- Socio-technical, user-centred and social acceptability analysis for responsible and responsive innovation (Pre-experience Users' SAFET4RAILS Potential Impacts Analysis)
- Risk-aversive approaches to prevention and mitigation against the risks of information security breach and misuse.

2. Guided operational Protocol for implementation of Ethical Safeguards to Ensure operational compliance as included in D11.3 and Annex 1 of this document for ease of reference.
3. Data protection ethical compliance essential precautionary and safeguarding steps in crisis communications, as included in D9.3 (Guidelines for Ethically Sustainable Crisis Communications and Information Sharing) and Annex II of this document for ease of reference.
4. Pre-and-Post-experience Social Impact Analysis of SAFETY4RAILS Integrated Tools Platform (S4RIS) as presented in D9.7 (Chapter 7) and extended in this deliverable which provides an account of the results arising from the work done for the second stage Social Impact Analysis (SIA-II) (Chapter 2).
5. Ethical Situation Assessment through the ongoing Data Protection engagement within the SAFETY4RAILS consortium, as part of the SAFETY4RAILS Ethical Board Operational Ethical Compliance Monitoring with the close collaboration of the Coordinator and the Data Controller and reporting to and seeking opinion from the Ethical Advisory Board.
6. Review of all the deliverable involving any ethical aspects to ensure ethically consistent and compliant analysis
7. Support for work package 11 Ethical Requirements Deliverables (D11.1 – D11.4) in particular to conclude the consideration of possible privacy, misuse and information security risks as presented in the next chapter.

5. Information Security and Ethical Risks

By virtue of its activities, SAFETY4RAILS involved the collection, processing and generation of some sensitive security data and the creation of IPR both of which would require security safeguards to be addressed. The deliverables are the containers of the above two sensitive types of information as they are by definition to elaborate on the technology and models deployed and detail the implementation in the context of (privileged) data made available as confidential data. Accordingly, some of the deliverables had been designated with restricted dissemination and these have been included in the research findings risk assessment table as the exponent of the Knowhow and use-cases enabler IPRs and privileged information to be protected.

Additionally, other deliverables that would normally include consortium and partner information have also been included in this impact assessment with safeguarding measures indicated to be secure storage, multi-level role bases access control password and encryption when stored/transferred (at-rest and in-transit). These SAFETY4RAILS information security safeguarding guidelines have been and will continue to be adhered to, particularly for sensitive data that may be likely to expose a Nation State to any security risks – all access to such information will have to be based on national security clearance and for specific legitimate security purpose.[2]

All the National Security, IPR and Business Confidentiality and Privacy safeguarding commitments on the part of the Consortium equally extend to dissemination material, hence the established process for dissemination approval to ensure not only that no restructured information is inadvertently or indirectly divulged but also that no images or other material, whether as primary/secondary usage, is included in any deliverable that may expose the privacy and confidentiality of information belonging to any data subjects or organisations.

5.1 Ethical, Privacy and Misuse Risks Minimisation

Notwithstanding the fact that scope of the Consortium's responsibility from a GDPR viewpoint, was limited to the data processing actions taken for innovation purposes within the project and not extending to the legal basis of any future data processing actions that users of the SAFETY4RAILS Tools may perform, the social acceptability of the resulting innovation has to be examined and, as far as possible, measures proposed to address possible ethical risks in light of the Social Impact Analysis that has already been performed as (per D9.1 and this deliverable) but that is indeed a dynamically evolving artefact and would need to be re-examined in the future.

As has been established in D9.1 and D11 ethically-focused deliverables, within the SAFETY4RAILS lifecycle, processing of any personal data has been on a limited scale and subjected to strict privacy protection at source /at-capture. However the listing of such data processing and the safeguarding measures as presented in the table below are from the perspective of possible exposure to some future misuse by persons or organisations with ill intent.

Accordingly in the following tables indicative potential Ethical Risks Table 1 sets out the general risks and table 2 shows the risks associated with the context of specific uses-case as may be deployed by future users of the SAFETY4RAILS whether intrinsic or extrinsic to it.

[2] Project co-ordinator comment: we have to no deliverables or results above the H2020 dissemination level CO – Confidential i.e. we have nothing requiring national security clearance. No further results will be generated in the project.

TABLE 2: SAFETY4RAILS OBJECTIVES, USE-CASES AND COMMON USE SCENARIOS

SAFETY4RAIL Objectives	SAFETY4RAILS Use Cases	SAFETY4RAILS Common Use Scenarios in Pilots
01: IDENTIFYING new threats **02:** DETECTING new threats **03:** AUTOMATING forecast & management of new threats **04:** KNOWLEDGE sharing with stakeholders **05:** MEASURING impact of evolving cyber-physical threats **06:** SAVING response time 07: INNOVATING and making response measures cost effective **08:** IMPROVING resilience of real-time crisis and security management **010:** TRAINING of users associated to different components of SAFETY4RAILS **011:** DEMONSTRATING the S4RIS operational performance and security effectiveness	UC-001 Natural disaster flooding UC-002 Track interception due to a landslide that causes an immobilisation of a train UC-003 Physical attack, terrorist attack using firearms inside a railway station UC-004 Physical attack, potential terrorist attack via IED carried in luggage UC-005 Train failure inside a tunnel without possibility to communicate With the train driver UC-006 Physical attack, intrusion and bomb planted UC-007 Physical attack, intrusion in sensitive place UC-008 Physical attack, spoofing attack on existing sensors UC-009 Cyber-attack on data transferred to operating systems UC-010 Cyber-attack on system causing accidents UC-011 Combined Cyber-physical attack	**S4RIS** • Integrating Real-Time Monitoring Tools • Simulation Tools • Risk Assessment and Decision Support Tools To support advanced capabilities for: • Threat-Attack Prevention • Threat-Attack Detection • Threat-Attack Response • Threat-Attack Recovery • Validated through the Safety4Rails Pilots, deploying various user scenarios with a range of data processing contexts for which potential future misuse risks could be examined

TABLE 3: RESEARCH FINDINGS SECURITY RISK ASSESSMENT

Deliverable no.	Deliverable Title	Measures to prevent misuse including observations[3]	Likelihood of misuse	Potential impact of misuse	Overall Risk Score
D1.1	Project Management Manual	Passwording and Encryption	1	3	3
D1.2	Mid-term Report	Passwording and Encryption	1	3	3
D1.3	Final Report	Passwording and Encryption	1	3	3
D1.4	Specification of the overall technical architecture	Passwording and Encryption	2	2	4
D1.5	Quality Assurance Plan	Passwording and Encryption	1	2	2
D1.6	Data Control and Management Plan	Passwording and Encryption	2	2	4
D2.1	Grid Analysis of End-users needs and workshop minutes	Passwording and Encryption	2	4	8
D2.5	Specific Requirements for Multi-modal Transport Systems	Passwording and Encryption	2	3	6
D3.1	Identification and Characterisation of Cyber physical systems and threats in a railway environment	Passwording and Encryption	2	5	10
D3.2	Description of S4RAILS Tool Functionalities	Passwording and Encryption	2	5	10
D3.5	Risk Assessment and Resilience Strategies Simulation	Passwording and Encryption	2	4	8
D4.1	Incident detection methods and capabilities	Passwording and Encryption	2	5	10
D4.4	Blockchain Technology and Cyber-physical threats	Passwording and Encryption	2	3	6
D4.5	Model of cascading effects	Passwording and Encryption	2	4	8
D4.6	Implementation of Real-time Monitoring components to S4RIS	Passwording and Encryption	2	5	10
D5.1	Taxonomy of Risks and Vulnerabilities for Railroad Infrastructure and a Toolkit of Measures and Strategies to Effectively Identify and Respond to Incidents	Passwording and Encryption	2	5	10
D5.3	Predictive Risk Assessment Plan and Mitigation Strategies	Passwording and Encryption	2	5	10
D5.7	Decision Support Platform including Infrastructure Analytics Engine and UI	Passwording and Encryption	2	5	10
D6.2	S4RIS System with an Online Platform Dedicated Training and What-if Scenarios	Passwording and Encryption	2	4	8
D11.1	H-Ethical Requirements No.1	Passwording and Encryption	1	3	3

[3] Project coordinator comment: To date deliverables accessible to authorised users of Fraunhofer data storage and sharing platform. None of these deliverables individually password protected for access or encrypted to date.

D11.2	H-Ethical Requirements No.2	Passwording and Encryption	1	3	3
D11.3	POPD-Ethical Requirements No.3	Passwording and Encryption	1	3	3
D11.4	M-Ethical Requirements No.4	Passwording and Encryption	1	3	3

TABLE 4: EXAMPLES OF SAFETY4RAILS POTENTIAL SYSTEMIC ETHICAL AND MISUSE RISKS AND MITIGATION APPROACHES

Misuse Risk Type	Measures/Observations re Minimisation of Risk
Misuse of discovered unseen patterns of correlation of data relating to natural persons' transaction behaviours or national security sensitive data/processes.	The use of synthetised data would eliminate or at least minimise the discovery of any identifiable-person-specific patterns of data which may in turn give rise to risk of potential misuse of such findings.
Misuse of any algorithmically derived patterns of data related to possible sources of attack	It is at least theoretically possible that even in the context of machine models based on synthetic data, some inferences could be drawn by malicious persons exploiting the necessary prototypicality/high-fidelity of the relationships that may become evident through some correlation and which could expose real persons /organisations to the risk of misuse. However one can rely on the dynamic evolution of the real data and operational workflows to somewhat mitigate this risk
Misuse of stored profile data, platform registration and collected social network data of clients	Encryption/deleting of personal information would help reduce the risk of misuse but it has to be acknowledged that wherever there may be the opportunity of somehow accessing profile information and pooling linked data., there will be the risk of misappropriation of the technology and misuse by some insider/hacker or other and this has to be factored into reflective design to minimise the use of technologies that can be fraught with misuse risks.

Misuse Risk Type	Measures/Observations re Minimisation of Risk
Misuse of algorithms through adversarial attacks or other means to lead to incorrect, unfair or biased results	Care has to be taken to design inherently bias-aware and self-audit capable models that can resist adversarial attacks as well as multi-model approaches that could periodically cross-verify results across models so as to detect any models that have been compromised; as such the variety of tools integrated within SAFETY4RAILS could offer an intrinsic means of reducing the risks of adversarial attacks.

TABLE 5: SAFETY4RAILS PRIVACY AND DATA PROTECTION RISK ASSESSMENT ISSUES

Issue #	Privacy Issue potentially arising from	Risk to Individuals	Measures which if lacking would cause Compliance Risk	Associated organisation or corporate risk
1	Participant's name and particulars	Linked data privacy risk through malicious pooling	Can be minimised through to de-identification at source	Arising from Data Controller's inadequate monitoring and enforcement of de-identification implementation encrypted storage of the delinked data, access control
2	Video, photos, recordings of participants during demonstration exercises comprising audio image video	Incidental image and audio capture of citizens' potential privacy protection risk including through other linked data, place-ability/locate-ability	Selective or total privacy masking (irreversible; scrambling, blurring or total) as required to ensure personal data protection	Arising from Data Controller's inadequate monitoring and enforcement of: De-identification through irreversible marking and encrypted storage of all images at-source/at-the-point-of-capture as possible
3	Network traffic metadata of the client device IP or MAC address	Potential linkage from device IP and MAC address particulars to device owner's identity and possibly other personal data	Encrypted storage of access logs, de identification by masking computer data in the meta0data to obfuscate the device ID and prevent potential linkage to the device owner's identity as well as categorisation risk	Arising from Data Controller's inadequate monitoring and enforcement of access logs encryption, obfuscation/de—linking of device ID in the metadata and access control to logs data
4	Train station CCTV camera stream /frames acquisition for crowd monitoring.	Incidental image and audio capture of citizens'; hence potential privacy protection risk including through other linked data. No sound monitoring	Selective or total privacy masking (irreversible; scrambling, blurring or total) as required to ensure personal data protection wide-area /aerial shot, rendering faces/bodies undistinguishable and/or irreversible blurring for only size/movement of crowd alerting to unsafe situations	Arising from Data Controller's inadequate monitoring and enforcement of: Camera shots control, implementation of de-identification through irreversible marking and encrypted storage of all masked images; lack of adequate Fair Processing Notices.

Issue #	Privacy Issue potentially arising from	Risk to Individuals	Measures which if lacking would cause Compliance Risk	Associated organisation or corporate risk
5	Train station public area audio stream recording for ambient sounds modelling and anomalous sounds detection	Only sound monitoring for ambient noise modelling, but a misappropriation to possibly eavesdrop on conversation risks personal info including placeability/locateability information	Ensuring high resolution directional capability of all the microphones in the array is disabled	Arising from Data Controller's inadequate monitoring and enforcement of switched off capture modes of the microphones array and access control to the ambient monitoring network control
6	Access Control Data	Personal data including password and accounts data and potentially other linked personal data at possible privacy risk through malicious pooling	Encryption of access data and online authentication data	Arising from Data Controller's inadequate monitoring and enforcement of de-identification of access control data and encrypted storage of such data.
7	Social network data	Privacy risks to personal and lifestyle data plus other linked data.	Data to be rendered de-identified through -pseudonymisation, anonymisation, scrambling the order of records, and generalisation through aggregation plus encrypted storage, including audio/video data masking using appropriate techniques such as scrambling, blurring, pixelization etc as appropriate.	Arising from Data Controller's inadequate monitoring and scrutiny of the purpose, context, and scale of data capture, limitation of such data capture and its use to only specific strictly controlled purpose; de-identification at-the-point-of-capture

6. Conclusion

This deliverable has set out the description of additional work as continued in period 2 of the project by way of the second stage of Social Impact Analysis (SIA-2) as well as the extensions to the Ethical Compliance Framework. Accordingly our ethical discourse in this deliverable is centred around the results of seven streams of effort to support ethical compliance and socially responsible and reflective innovation as follows.

1. Ethical Compliance Framework Console
2. Guided operational Protocol for implementation of Ethical Safeguards Data protection ethical.
3. Pre-and-Post-experience Social Impact Analysis of SAFETY4RAILS Integrated Tools Platform (S4RIS)
4. Ethical Situation Assessment Through the ongoing Data Protection Engagement
5. Review of all ethically involved deliverable to ensure ethically consistent and compliant analysis
6. Support for work package 11 Ethical Requirements Deliverables (D11.1 – D11.4)
7. particular to conclude the consideration of possible privacy, misuse and information security risks as presented in the next chapter.

Accordingly, this deliverable has provided a systematic analysis of stakeholder centred perceptions of the social impact of the deployment of the tools framework that has been developed and validated by the SAFETY4RAILS Project and has thereby concluded its work.

****

7. Bibliography

Aidinlis, S and Gurzawska, A. (2021). *Responsible innovation in Multidisciplinary Research and Innovation Projects: Moving from Principle to Practice*. Paper presented at The ISPIM Innovation Conference – Innovating Our Common Future, Berlin, Germany on 20–23 June 2021. Online. Available at https://www.darleneproject.eu/wp-content/uploads/2022/04/Responsible_innovation_in_Mult.pdf

Alvesson, M., & Sandberg, J. (2013). *Constructing research questions: Doing interesting research*. SAGE publications: London.

Fowler, Floyd J. Jr. (1998). Design and Evaluation of Survey Questions. In Bickman L. & Rog, D.J. (eds) *Handbook of Applied Social Research Methods*, SAGE Publications: London, pp.343—374.

ANNEXES

8. ANNEX I. SAFETY4RAILS Operational Ethical Compliance Manual

This Annex sets out the Safety4RAILS Ethical Compliance Framework (ECF) Guided Operational Protocol for Implementation of Ethical Safeguards to Ensure Operational Compliance

The following lists the operational procedures to be followed within the SAFETY4RAILS implementation in respect of any Personal Data Acquisition and Data Processing pipelines. This is to ensure full compliance, at the operational frontline, with respect to the European Data Protection (EU) 2016/679 (GDPR); in so far as this Directive appertains to the various lifecycle facets and phases of operations on any personal data that may be performed within the project, and that accordingly would need to be subjected to GDPR Requirements.

1) **Determination as to whether and to what extent any Personal Data is included in the Processing Pipeline**

   a. With Reference to the criteria established as part of the SAFETY4RAILS Ethical Compliance Framework (ECF) as described in deliverable D9.1, the local Project Manager is responsible to ensure that the nature of any proposed data acquisition and processing is examined in terms of the Purpose and Context of any such Data Processing and if in any doubt as to whether any proposed data processing may involve any *Personal Data Processing* then the procedure set out in D9.1 shall be followed to determine the sequence of steps to be actioned in relation to various aspects of compliance assurance to fulfil the GDR requirements as applicable e.g. in relation to the principles such as Purpose Limitation, Data Minimisation etc and the requisite procedures such as establishing the legal basis of the proposed processing under GDPR, consent seeking and anonymisation etc. These steps are to be taken in consultation with and the Data Protection Officer and with the knowledge and approval of the SAFETY4RAILS Data Controller (as set out in D9.1 Chapters 2 & 3).

   b. Should it be the case that the proposed data processing does include an element of *Personal Data Processing* then the following protocols shall be strictly observed, overseen by the Data Controller, in accordance with the SAFETY4RAILS Compliance Assurance Governance Structure as set out in D9.1.

2) **Primary Data Acquisition Under Controlled Conditions**

   No data acquisition will take place unless it is explicitly permitted under the *formal prior consent* of all the data-subjects involved and only if the process can adhere to all the conditions stipulated by the data-subjects involved -in respect of each of the lifecycle facets and phases of data processing.

3) **Knowledge-ful, Formal and Explicit, Positive Consent Seeking**

   In all cases consent is taken to mean positive knowledge-fully given written statement of agreement by a data-subject with respect to an explicitly and clearly stated protocol to be adhered to in dealing with the data-subjects' personal data. This also implies making available, a priori, to the data-subjects concerned, the full range of *The Requisite Information for Consideration of Consent* in seeking the formal expression of consent with respect to any aspect of the operations involving their personal data.

   This includes full, clear and explicit information about the boundaries, scale, scope, modalities and safeguards appertaining to each of the facets and phases of the data operations end-to-end throughout the lifecycle of the data that is proposed to be acquired.

   This should follow the relevant process and respective reference templates provided in D9.1 including the Generic Consent Form and the Project Information Documentation.

4) **Secondary Data Acquisition**

   This includes data from primary sources that may have acquired their data under uncontrolled conditions. Whenever data are acquired from publicly available sources as secondary data and/or through sources with uncontrolled conditions or from settings where it cannot be anticipated whose data may be inadvertently

included in the process of data acquisition and where all people involved are by definition anonymous (e.g. as in aerial imaging or other public imaging for performed for a legitimate approved purpose), the continued anonymity of the people whose data may be included in the data acquisition process shall be maintained. Additionally, where practicable the following Fair Notice process can be disseminated.

FAIR PROCESSING NOTICE

What are we doing?

Here we are to describe what data acquisition steps we wish to take e.g. type of data gathering for which it is not normally practical to have obtained consent for various reasons, but which may indirectly impact the inhabitants of a city e.g. aerial imaging of flood damaged districts to locate and rescue victims or plan repairs.

How might this affect you?

The activity may become relevant to you in terms of your personal data if you work or move around in or adjacent to the area which is to be observed. While data will be anonymised there is a limited possibility that you may still be identifiable by certain people depending on the extent of other personal information that they may have about you.

Who can you contact?

If you feel that some information about you may feature in the data planned to be acquired and you would like to ascertain whether this is the case and if so, have the data deleted then please contact the Project Data Controller (<here we are to provide the data controller's contact details including affiliation, email and telephone number>).

5) **Data Processing**

No data processing will take place unless the legal basis and accordingly the requisite safeguarding steps have been determined and approved by the Data Controller in accordance with the procedure as stipulated in D9.1. This includes the required level of anonymisation to maintain personal data protection prior to any such processing. Section 4 of D9.1 sets out the anonymisation techniques that can be deployed as required by the Data Controller and as applicable to particular types of multimedia which may be included with the datasets to be processed. In cases where the data has to be pseudonymised, appropriate K-anonymity levels need to be assured with reference to Section 4 of D 9.1.

6) **Secure Data Storage**

After the data has been subjected to the minimum guaranteed levels of anonymisation ("anonymisation at rest"), as set out under 3 above, it will be stored in secure data bases. This may involve a further security protection measure by way of *data encryption* where appropriate or as may have been stipulated per the consent given by the data-subjects concerned.

7) **Access Control Policy**

Any data as may be stored in secure data bases will be subjected to strict access control policy involving *mandatory access logging* including:

- The identity of any persons accessing the data
- The identity of data to be accessed

- The role of each person accessing the data per their rights of access
- The reason for any access by the person wishing to access the data

8) Exchange of Data with Project Partners

Under the requirements of the collaborative research efforts within the framework of the project, it is possible that data exchanges may be required between project Partners for research and innovation purposes, e.g. testing and evaluation of algorithms. However, no data shall be exchanged with Partner organisations unless the data set is fully compliant with at least the guaranteed levels of anonymisation ("anonymisation in transit"), as set out under (4) above.**)**

9) Data Analytics including Data Mining and/or Modelling

Such operations would be performed only on anonymised data or such data from the open sources which would have been either pre-anonymised or where any processing would not amount to violation of any privacy protection undertakings.

10) Prevention of Pooling of Personal Data

At no time will any data pooling be performed in such a way as to compromise the anonymity of any data belonging to ordinary citizens or any government (particularly involving sensitive data that may be likely to expose a Nation State to any security risks).

11) Acquisition of Secondary Data

All secondary data acquisition will comply with all the ethical and data protection requirements appertaining to such data as per commitments given by the Primary Source Owner(s) including partial or complete prohibition of usage of such data.

12) Parsimony in Data Acquisition

In general, all possible endeavours will be made by all Partners to use available pre-anonymised data from public sources as may be accessible for research purposes and in particular for testing and benchmarking the performances of algorithms.

13) National Security Protection

In All Facets and Phases of the Data Operations Lifecycle:

a. The project will not concern the acquisition of and/or indeed any data operations on any images that may be classified or reasonably deemed classifiable (i.e. may be security sensitive and/or confidential and/or in any way whatsoever be covered under any of the provisions of *any Official Secrets Legislation of any Nation; particularly* within the jurisdiction of any European Country including the Partner countries

b. This includes an unconditional undertaking that at no time will the Partners knowingly allow circumstances where any wilful and unauthorised access to any national security sensitive data may occur by any Partner organisation staff unless such staff were to be explicitly and formally authorised by the relevant authorities to access such data, clearly under fully protected conditions, for the express purpose of research and technology development per approved planned effort within the project; including testing and validation of algorithms.

14) Dissemination of the Resulting Deliverables of the Project:

a. All the undertakings as given above in respect of data protection, national security protection and ethical compliance assurance, during acquisition and subsequent data operation facets and phases, also apply to our dissemination of the results of our research; either by way of documents to be submitted to the EC Project Officer and/or to the Project Review Board members, and/or, by way of any *dissemination action* in any format and through any channels whatsoever. This means that we undertake that any images that may be used in our results publications shall be included *only if, for the clearly stated dissemination action,* we have previously acquired explicit formal consent from the data-subjects and/or relevant national security authorities involved, and/or, we are able to use full anonymisation of such images. Finally, under no circumstances will we publish any images which may be classified or could reasonably be deemed as being of sensitivity from the point of view of the National Security of any country including, in particular, the Partner countries,

15) Data Deletion

Any data that will be stored will basically comprise of two types of data: **i)** primary acquisitions, and **ii)** secondary acquisitions; as may be acquired, anonymised and protected within the framework of the above

protocols. Such anonymised data may be securely stored, as stipulated above, for a number of years[4] to allow testing for refinement of algorithms and benchmarking of results obtained with different algorithms in the normal course of research studies as may be conducted to optimise research results and advance the state-of-the-art in research and technology development.

16) Cross-Jurisdiction Harmonisation of the Minimum Guaranteed Standards of Data Protection Compliance Management across Partner Organisations to Ensure Maximum Policy Interoperability

The above policy framework sets out the minimum applicable protocols to be universally adhered to by all project Partners. This will be translated in various languages of the Partner countries involved and will constitute the D9.1 operational reference manual that specifies the minimum protocol to be universally adhered within the SAFETY4RAILS Ethical Compliance Framework (EFC) as set out in D9.1.

17) Implementation Audit

The Project Legal Board (the Coordinator, the Data Controller and the Ethical Manger), supported by the local project managers and Data Protection Officers of all Partner organisations shall remain responsible for ensuring full adherence to the above undertakings at all times; including, in particular, the strict enforcement of the minimum guaranteed anonymisation levels and the data access control policy enforcement.

Specifically the Partner organisations are responsible to ensure that:

Any attempted/accidental violation of access rights will be logged and shall be reported and acted on immediately to ensure that the effects are promptly mitigated and any unexpected security vulnerabilities that may be discovered as a result are remedied immediately.

18) The Data Protection Policy Framework Revision

The above data protection policy framework is subject to annual revision to ensure that it remains responsive to the evolving data protection requirements.

The Partners who by nature of their planned work within the project are expected to be involved in data handling shall be expected to make a periodic statement to confirm their adherence to the above protocols and any issues arising as applicable in respect of any personal data that may have been processed by the respective Partner. The Data Handling Protocols Implementation Declaration Form, included as Annex 3, of this document offers a suggested format for the Partners' periodic compliance statement.

****

[4] Maximum duration to be stated as part of the process of *formal prior consent* of all the data-subjects (point 2) in this list).

9. ANNEX II. Requirements for Crisis Communication from the Ethics Perspective

As per the analysis performed for the SAFETY4RAILS Ethical Compliance Framework in Deliverable D9.1, the considerations for compliance assurance operate at two levels namely:

i) Legal and data protection compliance

ii) Ethical compliance

LEGAL AND DATA PROTECTION COMPLIANCE

With regard to the first consideration which essentially is focussed on the responsibility for ensuring that all the requisite steps for data protection have been undertaken prior to processing any data, the privacy sensitivity of the data itself and the purpose and context of the data processing are the factors to be analysed in order to determine the legal requirements for GDPR compliant data protection. This must be conducted in a way that fully respects the rights and freedoms of the individual regarding how they would wish their personal data to be safeguarded including the right to refuse all access to the data for any purpose and in any context whatsoever.

Even where a citizen, through voluntary participation in any consent seeking process, elects, freely and knowledge-fully, to permit some element of their personal data to be included in any communication acts or in any related data processing for situation assessment, this must still be in accordance with the GDPR principles of data minimisation and purpose limitation.

Any use of the individual's data will have to be subjected to specific conditions to clearly delineate the purpose and context of such use as previously clarified to and permitted by the user through a formal consent seeking procedure. Thus, as far as data protection compliance assurance for crisis communication is concerned the management of all communication activities has to be based on the type of information elements contained in the communication acts and the various purposes and contexts for which any such communication acts are intended.

It should be noted that, in the context of a crisis scenario, the individual's data could still be shared to protect their interests (life, well-being etc) or because the responding body has a legal obligation to do, without the need of an explicit consent. In this sense, there would be several instances where individuals (perpetrators or victims) would not be able to consent.

Accordingly, it is important to distinguish the following aspects of the purpose and context of the communication acts.

A) Data Elements: The data elements contained within the communication could comprise of personal data which in turn could include sensitive personal data for example relating to the individual's health information, gender, religious or political affiliation and personal and financial information. It is important to note that such information, if it associates a person or category of persons with any incident as it most likely could, would directly or by implication divulge additional sensitive data including the co-location and placing of persons (temporally or spatially), particularly if the information contains video and/or audio content.

B) Purpose: The actual objective for the use of information is a key criterion for determining whether or not any personal data contained in any data processed amounts to personal data processing as specified within GDPR. For example if the information links to, or, contains, data on the particulars of people in general, such as an aerial view of a crowd of people in a location, even although facial or head images of persons might feature in the information frame to some extent, this does not necessarily amount to personal data processing as long as no specific individual could be recognisable in the images and video streams concerned.

C) Context: This specifies how the information is to be processed and communicated, starting from the point of consent seeking for its use and subsequently to the point of acquisition, ingestion and possible processing for crisis communication through various media with any proposed de-identification steps such as partial or full masking/blurring.

i) **Type of Information Act**

This could comprise of

- **Information Getting Acts (IGAs)** ,

  These are actions undertaken to obtain information from persons through various channels.

- **Information Reporting Acts (IRAs) ,**

  These are steps taken to inform persons regarding certain events or actions to be taken.

- **Information Integration Acts (IIA)**

  These are steps taken to aggregate information for example to inform situation assessment

ii) Channel Type

This specifies the particular medium i.e. channel of communication

iii) Communication Scope and Scale

These relate to the domain of information dissemination or acquisition for example multi-channel, broadcast (public) private and/or any managed mix of synchronous and asynchronous communication acts through mass media, social media, mailshots and post

iv) Interlocutory Types

These could include information acts involving authorities or citizens e.g. in News Interview Clips and live at the scene reporting, which could be periodic, or event- triggered. This comprises of the following information flows:

1. Authorities to Citizen(s)
2. Automated system as proxy authority to citizen

The following interlocutory types **fall outside** the analysis frame for Crisis Communications as addressed in this deliverable:

i) Operational incident response communications by the rescue and recovery teams such as fire, ambulance, police.

ii) Citizen-to-citizen information acts either in person or through Twitter and social media messaging and/or cityscape.

iii) Announcements by NGOs and Voluntary Organizations such as through Local Resilience Community Representatives, News Channel Editors etc all of whom will also have to comply with the data protection and ethical requirements for which the actors are directly and separately accountable. This is in consideration of the fact that crisis communication, as addressed within this deliverable, is focussed on the railway system operators' responsibilities rather than the emergency services responsibilities and although the similar considerations for communication acts appertain to the conduct of communication and the management of the emergency services, these are not applicable to the analysis of concern in this deliverable.

Targeted persons

The assumption has to be that the targeted persons for any information act are to be responsible adults, and this would exclude persons under the age of 18 or any other persons of any age who are in some way cognitively impaired and vulnerable or in any way disempowered to act of their own volition. Accordingly, the targeted persons can be as follows:

- Targeted persons for Information Giving Acts (IGAs)
- Targeted persons for Information Reporting Acts (IRAs)

ETHICAL COMPLIANCE CONSIDERATIONS

These relate to avoidance of harm and hurt, including avoidance of inequitable treatment, stigmatisation and any form of discrimination and/or disrespect on the grounds of any of the protected categories of personal attributes for example, sex, gender, age, disability and impairments of any sort including frailty, cognitive impairments and political and religious affiliation. Equally the dignity of all citizens under any circumstances must be preserved particularly the injured, emotionally distressed, anxious and expressing grief and particularly if unconscious and physically exposed or deceased.

DATA PROTECTION AND ETHICAL COMPLIANCE ESSENTIAL PRECAUTIONARY AND SAFEGUARDING STEPS

As the extent of responsibility of authorities in respect of the conduct of their crisis communications is critically dependent on the above parameters of purpose and context which determine the steps to be taken for legal compliance. It is important that the communication needs responsive to any incident are specified and carefully categorised with respect to the purpose and context of any planned communication acts. A framework of Legal and Ethical Compliance has to be in place in accordance with the SAFETY4RAILS Ethical Compliance Framework as described in D9.1 as well as the additional steps as set out in this chapter which mainly arise from:

i) The need to be mindful of the fact that in the **context of a crisis, it is impossible to have had the opportunity for any a priori consent seeking**. It is impossible to know the involvement of subjects, as the identity of data subjects, a priori to any incident, and therefore, the need for communication. As a result, other grounds for lawful data processing would need to be investigated and taken into consideration by the operational framework. The extent of the purpose and context of the data acquisition and processing that becomes necessary during the course of crisis management would include various consideration and reasons why it may be necessary to process a particular element of data in particular way; the circumstances at the time (in terms of specific purpose and context) would determine the extent to which any processing would amount to personal data processing and the legal basis for the necessary processing and the safeguards for it. This would determine the extent of any personal data that may be potentially involved in the communication acts.

ii) In the context of a crisis any **potential data subjects involved in the incident would be most vulnerable** as they may well be emotionally distressed, injured, unconscious, physically exposed or deceased.

Accordingly, as part of the preparatory plans, the following steps need to be taken:

1) An operational framework for crisis communications has to be established, consistent with the Ethical Compliance Framework as set out in D9.1 and the steps stipulated below. Such a Crisis Communications Operational Framework should be the basis of preparatory training for all staff likely to be involved in crisis communications. A chain of **operational ethical authority would need to be established** to provide rapid advice on any ethical issue and a clearance role for any crisis communications and related data processing likely to involve personal data. This includes a need for authorities to be trained to determine whether or not and to what extent any personal data would absolutely need to be used in any communication acts and applying anonymisation and masking with reference to the SAFETY4RAILS Compliance Framework as described in D9.1 as required.

2) For Ethical Compliance Assurance, the requirements set out in D9.1 and in this chapter must be followed in all contexts irrespective of the purpose for which the communication act is being undertaken.

3) For Legal Compliance Assurance, beyond following the principles of purpose limitation and data minimisation, the purpose and context for any given communication act have to be identified with respect to the specific determinants of purpose and context as outlined in this chapter and in D9.1

4) Ultimately in an evolving crisis setting the justification for the need for any processing of any data has to be clarified by the operational team and this would define the purpose and context of processing according to which it is possible to determine to what extent and in respect of what data elements any proposed data

processing amounts to any personal data processing as determined within GDPR. Once this is known the applicable legal basis and respective legally permitted processing and associated safeguards can be readily determined by reference to GDPR as set out in the Ethical Compliance Framework Console (D9.1) The Operational Data Controller would then be responsible for ensuring that the permitted data processing can be actioned within the framework of the respective legal basis and the safeguards to be actioned to ensure full compliance whilst proceeding with the data processing within the permitted limits.

5) accordingly responsive compliance steps would need to be taken as precautionary actions to safeguard the privacy, dignity and rights and freedoms of the citizens involved.

As in the context of a crisis communication the information acts are expected to be undertaken with persons involved in the emergency incident, comprising the following **Data Subject Groups**, either as **i) Operational Staff & Rescuers**, ii) **Witnesses**, **iii) Victims** or to ensure legal and ethical compliance the following safeguarding steps must be implemented with respect to the above three distinct potential data subject groups, defined as follows:

i) Operational Staff & Rescuers: public authority representatives and/or employees as part of the crisis response team and/or rescuers including managers on the scene or at the centre.
ii) Witnesses, including any members of the public.
iii) Victims and the Crowd, as distinct data subjects including any citizens affected whether injured/unconscious/deceased or not

The additional precautionary and safeguarding step for compliance assurance specifically in respect of each of the above distinct data subject groups are as follows:

6) **Crisis Communication Safeguards for Data Subject Group 1: Public Authority representatives and/or employees as part of the crisis response team**

All form of communications with the public including **any video /audio reporting/announcement and leaflets regarding the crisis must be screened** to prevent the publication of any content therein which in any way may render a person re-identifiable unless the person is a public employee or public authority representative who has, by virtue of the job position, a responsibility to provide information and who has consented to do so willingly including to be part of an audio/video clip or still images.

7) **Crisis Communication Safeguards for Data Subjects Group 2: Witnesses**

Any video/audio-clip and/or document featuring witnesses, **cannot be cleared for publication without the prior explicit permission of the witnesses** as to any of their personal information being included whether as part of a video/audio or still image or statement attributed to them as may be conveyed through any channel e.g. by mass media, social media, mailshots, post, public address system etc.

8) **Crisis Communication Safeguards for Data Subjects Group 3: Victims and any ither members of the public involved in the incident**

As there will have been no possibility of any consent seeking with any of the victims, video/audio-clip/still-images and/or document featuring personally re-identifiable information of any victims whether as individuals or within a crowd of people, cannot be published without using either a wide-area or aerial shot whereby no individual faces or bodies could be clearly distinguished or otherwise using masking techniques including blurring. pixelization audio/video scrambling.

9) No communication content should be included with any information, whether direct, quoted and/ or attributed, which in any way offends the dignity of a person, including in particular deceased, unconscious, injured and/or highly distressed persons or in any way stigmatises or treats any citizen or citizen groups inequitably or in a discriminatory fashion.

For clarity the information to be subjected to the above safeguarding steps includes all elements of the foreground as well as the background which could in any way feature any personally identifiable elements as well a personal place-ability and locate-ability information (as described in D9.1) of any particular witnesses or victims involved.

SAFETY4RAILS

Partners:

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

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