SAFETY4RAILS

GUIDELINES FOR ETHICALLY SUSTAINABLE CRISIS COMMUNICATIONS AND INFORMATION SHARING

Deliverable 9.3

Lead Authors: ETRA

Contributors: UIC, MTRS, LAU, UREAD, RMIT, CEIS, FGC, MDM, PRO, EGO, TCDD, EOS, UMH

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.

D9.3 GUIDELINES FOR ETHICALLY SUSTAINABLE CRISIS COMMUNICATIONS AND INFORMATION SHARING		
Deliverable number:	D9.3	
Version:	1.1	
Delivery date:	01/06/2022	
Dissemination level:	PU - Public	
Nature:	Report	
Main author(s)	Eduardo Villamor	ETRA
Contributor(s)	Laura Petersen Gilad Rafaeli Paul Abbott Eveliina Hytönen Atta Badii Karen Mathews Florence Ferrando Álvaro García Antonio de Santiago Laporte Jeroen van den Tweel Halil İbrahim Uluçinar Okan Topçu Juliette Vieillevigne Ignacio Díaz	UIC MTRS MTRS LAU UREAD RMIT CEIS FGC MDM PRO EGO TCDD EOS UMH
Internal reviewer(s)	Antonio de Santiago Laporte Atta Badii Andreas Georgakopulos Uli Siebold Stephen Crabbe	MDM UREAD WINGS IC Fraunhofer
External reviewer(s)	Yves Rougier	Ministère de la Transition écologique et solidaire

Document control			
Version	Date	Author(s)	Change(s)
0.1	22/12/2021	Eduardo Villamor	ToC release
0.2	25/02/2022	Laura Petersen	Chapter 2
0.3	12/04/2022	Laura Petersen	Updates Chapter 2 since it was put on Livelink
0.4	05/05/2022	Eduardo Villamor, Laura Petersen, Atta Badii, Gilad Rafaeli	Partner reviews integrated into new version. Chapter 2 is now finalised. Chapter 3 and 4 integrated
0.5	13/05/2022	Eduardo Villamor	Chapter 5 integrated
0.6	23/05/2022	Eduardo Villamor	Revisions from UIC, EOS, PRORAIL, UMH integrated. Chapter 1 and 6 finalised
0.7	24/05/2022	Eduardo Villamor	Executive Summary, Acronyms table and final edits
0.8	01/06/2022	Eduardo Villamor	Internal review comments addressed
1.0	01/06/2022	Eduardo Villamor	Version for submission. Yves Rougier review in process, feedback input to future work.
1.1	01/06/2022	Stephen Crabbe	Very minor edits and fromatting.

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 continuous adaptation of the SAFETY4RAILS solution; this will be validated by two rail transport operators and the results will support the re-design of the final prototype.

TABLE OF CONTENTS

List of tables

List of figures

Executive summary

SAFETY4RAILS develops a resilience-oriented framework including technical and non-technical tools to tackle combined cyber-physical threats to railway and metro infrastructure. In this document, the consortium presents the SAFETY4RAILS Crisis Communication and Information Sharing Guidelines. This is one of the project Key Exploitable Results and a non-technical tool that can be easily exploited by end-users after the project to improve communication mechanisms in the response and recovery phase of a crisis.

The foundation of the guidelines presented in this document was developed in Section 2, which provided an extensive State-of-the-Art review in the field of crisis communication. Specifically, a deep literature review was performed based on Crisis Communication Plans provided by the end-users in the consortium, a systematic literature review, cases studies review (from D2.2.) and the review of past projects. Qualitative interviews with railways and metro end-users were carried out and a final online Workshop was performed with all end-users, including those belonging to the Project Advisory Board.

In Section 3, a set of data protection and ethical compliance safeguarding steps are provided to define the ethical framework to be considered to prevent ethical-security risks on crisis communication. Section 4, on the other hand, presents the Crisis Communication Framework developed, including all relevant information streams, communication channels and sensitive information to be handled during and after a crisis.

Section 5 reports the SAFETY4RAILS Crisis Communication and Information Sharing Guidelines, considering the information elaborated in the rest of the document. The guidelines are formalised in a set of general recommendations, that can be applied to various types of threats, and context-based guidelines focusing on specific scenarios developed in WP8 – therefore addressing the crisis communication in the most relevant contexts of the project.

1. Introduction

1.1 Overview

A crisis is a situation, derived from natural or man-made threats, which has the potential to compromise the safety of individuals, group/s or the community, physical and logical assets; where the resources needed to respond, and recover are beyond the capacity of the system's owner and/or operator – definition provided in the course of the task. In T9.2: Crisis Communication, the task dealt with the complex problem of defining an applicable Crisis Communication Framework for railway and metro infrastructures including a set of recommendations to enable ethical guarantees in the communication process. The framework considered both internal and external stakeholders to the railway/metro infrastructure. This is formalised in a project exploitable result denominated **SAFETY4RAILS Crisis Communication and Information Sharing Guidelines** – this deliverable. The guidelines created have the goal of answering the following questions in the railways and metro sector:

- What information is susceptible to be sensitive?
- What information should be distributed?
- How should this be managed and by whom?

As part of such, various Security-Ethical risks are considered such as the leakage of terrorist modus operandi and infrastructure vulnerabilities, the communication of information that might create panic or concerns, the release of personal information of those involved in the crisis or information that might be manipulated through social media.

The formalisation of the guidelines was achieved through a comprehensive State-of-the-Art (SOTA) review and the engagement of the end-users at every step of the process. Such SOTA review was a key element in the process and revealed several gaps in crisis communication research, such as: 1) The lack of publicly available Crisis Communication Frameworks specifically tailored to rail and metro, 2) Cyber security elements, 3) Fake news not addressed, 4) Lack of understanding of ethical considerations. Those gaps have been successfully integrated in the development of this document.

1.2 Structure of the deliverable

The structure of this document is outlined as follows:

- Section 1: Introduction. This section provides a clear overview of what has been done to produce this deliverable, including its main goals, overall scope and structure.
- Section 2: Crisis Communication State-Of-The-Art. This section developed a State-of-The-Art review considering research literature, end-users Crisis Communication Plan, case-studies, past projects, end-users' questionnaires and a final workshop.
- Section 3: Requirements for Crisis Communication from the Ethics Perspective. A set of data protection and ethical compliance essential precautionary and safeguarding steps are included.
- Section 4: Crisis Communication Framework. The framework provides a general scheme of the relevant information streams, communication channels and sensitive information to be handled during and after a crisis.
- Section 5: SAFETY4RAILS Crisis Communication and Information Sharing Guidelines. This section combines the information produced in the rest of the document and supports railway/metro operators to build specific mechanisms for effective crisis communication.
- Section 6: Conclusion

The document also includes the following annexes:

- ANNEX I. GLOSSARY AND ACRONYMS
- ANNEX II. Crisis Communication & Information Sharing Message Map Template
- ANNEX III. Questionnaire
- ANNEX IV. Interview Guide

1.3 Relationship with other work packages

Crisis communication is a horizontal topic in SAFETY4RAILS falling under the umbrella of crisis management. In this sense, D9.3 work was connected to the following tasks:

- T3.5. Recommendations for crisis management and coordination of response teams
- T5.5. Implementation of simulation S4RIS tool as decision support system
- T10.3. Communication and engagement of citizens and (social) media

2. Crisis Communication State-Of-The-Art

2.1 Systematic literature review on crisis communication for transport operators

Research question: How does academic literature discuss crisis communication in the field of transportation?

The method used in this research was a systematic literature review. This is a qualitative study. Systematic literature reviews are useful in identifying knowledge gaps in current literature, and bring new insights to the respective field for further investigation[1].

2.1.1 Qualitative Research Design

According to Kitchenham, a systematic literature review is a thorough process that can help present evidence that showcases the effects of selected events as they are described in research literature, and which may not be conveyed in traditional non-systematic literature reviews. Systematic literature reviews may thus, be more extensive than traditional ones. To conduct this literature review searches were conducted to provide answers to the research question. This study was conducted in a series of four steps: 1) search, 2) inclusion criteria, 3) data extraction analysis, and 4) writing of results and conclusions.

2.1.2 Search, Inclusion criteria and data extraction analysis

The search for the articles was performed in March 2022. The search was conducted on three different databases: ProQuest, EBSCO and SCOPUS. A Boolean keyword search was used on each database combined with further search parameters depending on the database search features. The Boolean keyword search statement was the same on each database. The statement was as follows: crisis communication AND (railway OR rail OR metro OR tram OR aviation OR "air traffic" OR subway OR underground OR "light rail" OR "railway transportation" OR transportation OR transport OR "high speed rail" OR maritime OR sea OR "commuter rail" OR "suburban rail" OR "smart city" OR infrastructure OR port OR commuter OR passenger OR "urban mobility" OR Methodology.

2.1.3 Methodology

The initial searches on the three databases returned a total of 283 articles. The abstracts of these articles were examined against inclusion criteria: some form of transportation is mentioned, the article discusses the response or the recovery phase of the crisis management cycle, and it examines crisis communication towards external stakeholders e.g., the public, the authorities, emergency response, other operators. The final sample included six papers that correspond to the inclusion criteria.

Following the identification of the appropriate articles for the literature review all six articles were read and analysed by extracting relevant pieces of information to a data extraction table (DET) that was based on the research question. The next chapter discusses the findings of the sample articles.

[1] Kitchenham B. (2004). Procedures for Performing Systematic Reviews. Keele University 33:1-26.

TABLE 1 SEARCHED DATABASES AND THE SEARCH PARAMETERS

Database	Search parameters
ProQuest	Advanced search, 2017-2022 peer reviewed full text English anywhere except full text
EBSCO	Advanced search, 2017-2022 Full text peer reviewed smart text searching apply equivalent subjects
SCOPUS	2017-2022 English Peer reviewed

TABLE 2 SEARCH RESULTS

Database	Initial search results	Final sample
ProQuest	195	3
EBSCO	30	2
SCOPUS	58	1

2.1.4 Findings

The sample literature discussed crisis communication in the field of transportation in response and recovery phase of a crisis or a critical event. The transportation modes studied in the articles were railway, maritime and aviation. The following themes of academic discussion about crisis communication in the field of transportation emerged from the sample articles: emotions evoked by the crisis and crisis communication, crisis response strategies, communication strategy adaptation, and communication supporting crisis management, decision-making and creating shared understanding.

Crisis type is specified in five out of six articles. Four articles discuss one time crisis, that is train explosion, pandemic, and a maritime accident. One article, then again, focuses on more frequently occurring incidents and communication related to them, and one article discusses a wide variety of critical events in the cruise industry.

TABLE 3 SAMPLE ARTICLES

Authors	Article title	Transportation mode	Themes studied	Crisis type, if specified
Lonneke van Leeuwen, Jeroen Bommelé and Bart Hoogcarspel	Responsibly Communicating Delays After Suicides on Railways The Impact of Delay Announcements on Suicide-Related Associations and Emotions, and Announcement Appreciation	Railway	Emotions Message content	incident on railway
Marc D. David and Marie-Eve Carignan	Crisis communication adaptation strategies in the MM&A train explosion in Lac-Mégantic downtown	Railway	Crisis communication plan/strategy adaptation	train explosion fire
Dorota Chmielewska-Muciek, Jacek Jakubczak, Patrycja Marzec-Braun	Crisis Response Strategies and Themes during the COVID-19 Pandemic in EU Aviation, Airlines' Executives Communication with Shareholders: A Content Analysis	Aviation	Crisis response strategies Themes in crisis response communication	pandemic
Lara Penco, Giorgia Profumo, Marco Remondino and Carolina Bruzzi	Critical events in the tourism industry: factors affecting the future intention to take a cruise	Maritime	Emotions	

Yasuharu Tokuda, Tomoko Sakihama, Makoto Aoki, Kiyosu Taniguchi, Gautam A. Deshpande, Satoshi Suzuki, Sakon Uda, Kiyoshi Kurokawa	COVID-19 outbreak on the Diamond Princess Cruise Ship in February 2020	Maritime	organizational coordination and planning	disease
Carine Dominguez-Pèry, Rana Tassabehji, and Lakshmi Narasimha Raju Vuddaraju and Vikhram Kofi Duffour	Improving emergency response operations in maritime accidents using social media with big data analytics: a case study of the MV Wakashio disaster	Maritime	shared understanding decision making social media	Maritime accident environmental emergency

Two articles relate to emotions evoked by crisis communication.

Van Leeuwen, Bommelé and Hoogcarspel (2020)[2] have studied in a randomized online experiment the effect of the railway delay announcements about collision with a person, emergency services, and a control announcement (collision with an animal) on associations with suicide and on emotions of the passengers. The study showed that after the collision with a person announcement, participants were more likely to think that suicide was the most probable cause of the delay than after the emergency services announcement. Van Leeuwen, Bommelé and Hoogcarspel (2020) state that this result, alongside with results from other studies, "may encourage railway companies to communicate post-suicide delays to the public by broadcasting announcements that do not imply suicide by colliding with trains. Since these delay announcements are communicated through multiple channels besides railway companies, such as local news websites and radio broadcasts, they may stimulate responsible reporting about suicide on a larger scale too."

Although the emotional effect of collision with a person and emergency services announcements was low, the participants reported more anger toward the victim after collision with a person than after emergency services announcement. Furthermore, personal relevance of the delay did not affect associations with suicide. Regarding the announcement appreciation, the participants appreciated collision with a person significantly better than emergency services.

[2] van Leeuwen, L., Bommelé, J. and Hoogcarspel, B. (2020) 'Responsibly communicating delays after suicides on railways: The impact of delay announcements on suicide-related associations and emotions, and announcement appreciation', *Crisis: The Journal of Crisis Intervention and Suicide Prevention*, 41(4), pp. 280–287.

Penco et al. (2019)[3] have studied factors affecting the future intention to take a cruise. They have studied such factors, in particular the emotions related to the event, the prior corporate reputation and the use of social media in the corporate communication strategies followed during the crisis with an online questionnaire. They state, that "The analysis provides evidence that critical events may variously influence customers' intention to take a cruise in the future with the cruise company held responsible for the event depending on different factors. In particular, public emotions emerging from the event and from the communication strategy followed by the firm, seem to influence future cruising decision of potential customers."

Penco et al. (2019) state that "A high level of anger (ANG), that usually is related to a high corporate responsibility for the event, seems to increase the likelihood of the critical event influencing future cruise decisions of potential customers. On the other hand, emotions related to sadness (SAD) and empathy for the victims (SEM) do not seem to be associated with such likelihood. Moreover, the results provide evidence that a former good reputation of a cruise line may influence future cruising decisions by potential customers after a critical event. In particular, the cruise company's previous good reputation (REP) reduces the likelihood of the critical event impacting the intention to take future cruises with the same company and underlines the importance of building good relationships with customers over the years."

They did not find a magnifying negative effect of social media on the likelihood of a critical event influencing the intention to take a cruise in the future. They conclude, however, that it is important that the cruise line managers pay attention to the negative emotions of public emerging from the different types of media. Cruise companies should monitor public conversations about their brand during the crisis, searching for anger feelings, since social media spread the news fast, often deforming and expanding the facts out of control.

One of the sample articles addresses specifically the crisis response strategies and the themes communicated when responding to the crisis.

Chmielewska-Muciek, Jakubczak and Marzec-Braun (2021)[4] investigated European Union airlines top-level executives COVID-19 aviation crisis communication with their shareholders in terms of both crisis response strategies used and the themes addressed. They found that when communicating the crisis to key stakeholders and shareholders in particular, the airlines mainly played down the significance of the crisis i.e., used the diminish crisis response strategy. The airlines also attempted to build an image of a strong brand capable of surviving the crisis.

They also note, that since the crisis was universal and large in scale, and not depending on the companies' own actions, it was extremely difficult to maintain a good image and to convince shareholders of the safety of their investments. They further state that "within the diminish crisis response strategies the occurrence of causal statements related to justification strategy (19,47%) was more than twice of these related with excuse strategy (8,85%)". When communicating with shareholders, the airlines top-level executives seem to prefer minimizing the impact of COVID-19 crisis over admitting that they were not able to control the crisis.

The rebuild strategies were the least applied of primary crisis strategies in responding to the crisis. Chmielewska-Muciek, Jakubczak and Marzec-Braun (2021) state that "the executives were more eager to apply compensation strategy, rather than apology strategy taking responsibility for the crisis and asking for forgiveness. The only airline that included the causal statement related to apology strategy was SAS."

In their study they also found an observable difference between traditional and low-cost airlines regarding the themes in communication. They conclude that "Traditional airlines tend to include causal statements related to responsibility to the stakeholders and travel safety relatively more often than low-cost airlines. The general rate

---

[3] Penco, L., Profumo, G., Remondino, M. & Bruzzi, C. 2019, "Critical events in the tourism industry: factors affecting the future intention to take a cruise", *International Journal of Contemporary Hospitality Management,* vol. 31, no. 9, pp. 3547-3566.

[4] Chmielewska-Muciek, D., Jakubczak, J. & Marzec-Braun, P. 2021, "Crisis Response Strategies and Themes during the COVID-19 Pandemic in EU Aviation, Airlines' Executives Communication with Shareholders: A Content Analysis", *European Research Studies,* vol. 24, no. 4, pp. 276-299.

of occurrence of travel safety themes in airlines communication is the lowest of all themes for all the airlines with the exception of SAS. Surprisingly Lufthansa and Ryanair did not even include travel safety among their themes." Furthermore, they found that low-cost airlines communicate about themes such as new and adjusted services and future of aviation more often than traditional airlines to shareholders.

Crisis communication plan and crisis communication strategy adaptation to the crisis is discussed in one article.

David & Carignan (2017)[5] examined the adaptation of communication strategies set out in the pre-crisis plan implemented by the members of Quebec's public safety authorities in the specific case of the rail explosion and fire in Lac-Mégantic in July 2013.

They state that based on the examination of this crisis, formal planning and preparation of crisis management are essential, but they have to be adapted to the specific and evolving context of the crisis. They also say that it is important to have a dedicated, experienced communications team to properly understand the specific communication challenges of the crisis if and when events unfold on-site, like it happened in this specific case.

It is essential that in a crisis frontline responders do not rely exclusively on digital communications tools to disseminate messages to reach an entire population. Human to human communication strategies and community-based media are also of importance in reaching the target audiences. In addition, the examination of the crisis case showed that it is necessary to be present on-site to be able to assess the effectiveness of the communication strategies that are being used, e.g., how the communication is understood. David & Carignan (2017) also found major literacy and health literacy problems among certain disaster victims or at-risk populations, and hence they highlight the importance of including those dimensions in crisis management plans.

Two of the sample articles discuss communication supporting crisis management and decision making and creating shared understanding.

Tokuda et al. (2020)[6] analysed the COVID-19 outbreak on the Diamond Princess Cruise Ship in February 2020 identifying several salient issues regarding infection control measures, and they provide learning points formulated as recommendations for future control of infectious disease outbreak.

Regarding communications, they highlight the importance of adequate interorganizational coordination and communication. "Management of crisis events requires a substantial degree of organizational planning, which should be anticipated to the utmost degree possible, with simulation activities, such as drills, conducted for possible similar events in the future. It is important to appoint a central disaster/crisis commander, define the scope of responsibilities of this role, and to collect, prioritize, and effectively announce critical information to affected individuals, relevant participating organizations, and the public. A ship control center would not be a professional for outbreak/emergency response, nor for infectious diseases. The most important outbreak response is command and control structure, so that all players are kept informed of updated information of the situation inside and what activities would be made in that day."

Dominguez-Péry et al. (2021)[7] explored in a case study how social media with big data analytics could be used to improve emergency response operations in maritime accidents. They state that without adequate transmission of information, incorrect conclusions can be drawn, and without adequate processing on meaning,

---

[5] David, M. D. and Carignan, M.-E. (2017) 'Crisis communication adaptation strategies in the MM&A train explosion in Lac-Mégantic downtown', *Corporate Communications: An International Journal*, 22(3), pp. 369–382.

[6] Tokuda, Y., Sakihama, T., Aoki, M., Taniguchi, K., Deshpande, G.A., Suzuki, S., Uda, S. & Kurokawa, K. 2020, "COVID-19 outbreak on the Diamond Princess Cruise Ship in February 2020", *Journal of General and Family Medicine,* vol. 21, no. 4, pp. 95-97.

[7] Dominguez-Péry, C., Tassabehji, R., Vuddaraju, L.N.R. and Duffour, V.K. (2021), "Improving emergency response operations in maritime accidents using social media with big data analytics: a case study of the MV

there will be a lack of shared understanding. They also state that “In the MVW case, the ship’s organisation and formal institutions ignored the information from the informal institutions and the wider community and reached inaccurate conclusions about the causes of the MWV accident. Equally, in our case, there was also a clear lack of shared understanding between formal and informal institutions (wider community), thus leading to inadequate decision-making that ultimately escalated the disaster with catastrophic repercussions.”.

They also found that “Twitter has highly effective information transmission capabilities with large quantities of diverse and relevant information that needed to be disseminated rapidly in order to provide more detail of the situation and causes – just before and after the accident. Here, we have also demonstrated that BDA-facilitated Twitter also provides convergence, where the interpretation of a situation is iterative, with the objective of reaching a common understanding of the situation among stakeholders.”[8]

2.1.5 Conclusions

The purpose of this review was to view how academic literature discusses crisis communication in the field of transportation within the past five years. Six articles were included in the final sample. Consequently, it can be stated that discussion in the academic literature about crisis communication in the field of transportation is scarce. Hence, there clearly is a need to focus crisis communication research also on this field in the future.

The findings of this review point out the importance of planning crisis communication and crisis response strategies. Planned crisis communication is more likely to ensure creation of shared understanding, effective decision making and organizational coordination in the management of a crisis.

The findings in this review imply that certain content, message type and communication medium might cause negative emotions, which, in turn, might provoke negative associations. Public emotions emerging from the critical event and from the crisis communications might affect passengers’ purchasing decisions. Thus, planning crisis communication also from the point of view of emerging emotions may be of importance.

When applying crisis response strategies, planning the themes and the strategy itself beforehand, is essential. The crisis response strategy used in a specific crisis might affect stakeholders’ perceptions of the crisis, and of the company. It could be suggested that with an appropriate crisis response strategy, the company can attempt to maintain a good image and convince the key stakeholders and especially the shareholders of the safety of the investments.

Based on the findings in this literature review, it can be noted that while formal planning and preparation of crisis communication is required and essential, it is important to allow some deviation from the crisis management and communication strategies and plans, if needed. The specific communication challenges of the crisis need to properly analysed and understood on the scene of the crisis, and the unfolding events need to be taken into account when responding to a crisis.

To conclude, more research is required to gain a better understanding of crisis communication in the field of transportation. Some of the key topics in crisis communication in the field of transportation might have been identified in the sample articles of this review, but there is still a need for gaining deeper insights of the possible key topics.

2.2 Current Crisis Communication Frameworks (CCFs) for transport operators

SAFETY4RAILS has carried out research to find relevant external crisis communication frameworks for external crisis communication for transport operators. Crisis Communication Frameworks (CCFs) geared towards Law Enforcement Agencies (LEAs), other first responders or other authorities are excluded. This section showcases the relevant existing CCFs from three sources: past EU projects, relevant professional

[8] “Wakashio disaster", *International Journal of Operations & Production Management*, Vol. 41 No. 9, pp. 1544-1567.

associations, and the results of a questionnaire to SAFETY4RAILS end-users, including the advisory board end-users and selected UIC members.

2.2.1 Past EU funded projects

The method used to identify relevant past EU projects was twofold: i) based on consortium knowledge & experience in past projects and ii) a key word search performed on CORDIS. Table 4 lists the projects which came from the consortium knowledge, of which IMPROVER also appeared in the CORDIS search. Table 5 list the projects that came from the key word search. The key words used were “crisis communication” + the relevant sector keywords (“smart city”, “transport”, “infrastructure”, “metro”, “rail”, “tram”, “aviation”, “air”, “maritime” & “sea”). The CORDIS search took place on 21 January 2022. Those projects which provided a CCF are examined in detail in the following sections.

TABLE 4 PAST EU PROJECTS FROM THE CONSORTIUM KNOWLEDGE

Project from consortium knowledge	Published a CCF	Comments
COUNTERACT	No.	However the deliverable does describe some elements that would be required for a media relations plan. It further explains that a communication plan for passengers should be developed.
EU-HYBNET	No.	
FAIR Stations	No.	Crisis communication was not addressed by the project. However, the project concluded that information and signage posed the greatest difficulty when travelling through the rail system for passengers with reduced mobility (PRMs). As such, the project recommends an inclusive, well-designed information and signage system with audio, visual and touch solutions.
IMPACT	Yes.	The IMPACT Communication Guidelines
IMPROVER	Yes.	The IMPROVER AESOP guidelines
LETSCROWD	Yes.	The LETSCROWD Communication Toolkit (ICP).
RESILENS	No.	However, the RESILENS European Resilience Management Guidelines (ERMG) identifies key needs for external crisis communication of CI operators, produced below.
RESTRAIL	No.	The RESTRAIL project does not have any output of relevance to crisis communication, being primarily concerned with communications relating to the prevention of trespassing accidents, including suicides.
SECUR-ED	No.	The SECUR-ED Emergency & Crisis Preparedness Handbook does not provide a CCF. However it does list key issues related to crisis communication, produced below.
SECURESTATION	No.	The handbook entitled “Design Guidelines for Railway Station Security” does not have a chapter on dealing with crisis communications and indeed the term is not used at all. Implementing what the handbook identifies would provide the means for crisis communication.
SHERPA	Yes.	Railways’ Crisis Communication Guide Towards the Public for Terrorist Incidents.

TABLE 5 PAST EU PROJECTS FROM THE KEY WORD SEARCH ON CORDIS

Key word "crisis communication" +	Related projects on CORDIS (acronym)	Published a CCF
"Smart city"	ATHENA	Yes. "The development of a framework to manage various information sources and analysis services" However not publicly available and no replies to attempted contact.
"Transport"	SAFETY4RAILS	This will be done with this deliverable.
	IMPROVER	Yes (see below).
"Infrastructure"	ASSIST	No
	CRISCOMSCORE	Yes, the "Crisis communication guide for public organisations."
	IMPROVER	Yes (see below).
	INTERACT	Yes. Report on the "Rapid response action plan [9] " includes a description for a proposed information flow when an environmental risk/event occurs. The document is intended for Mountain Stations and focuses on reporting to scientific bodies. It is therefore excluded.
	SECRICOM	No
"Metro"	SAFETY4RAILS	This will be done with this deliverable.

[9] Bernardová, A. (2018). Report on the Rapid response action plan. INTERACT project deliverable D6.1. https://euinteract.org/app/uploads/2017/11/D6.1.pdf

Key word "crisis communication" +	Related projects on CORDIS (acronym)	Published a CCF
"Rail"	SAFETY4RAILS	This will be done with this deliverable.
"Tram"	No results	N/A (not applicable)
"Aviation"	No results	N/A
"Air"	ASSIST	No
"Maritime"	No results	N/A
"Sea"	No results	N/A

COUNTERACT

Part of the COUNTERACT (Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities) project guidance on Incident & Crisis Preparedness, Recovery and Business Continuity Planning[10] recommended that for security matters infrastructure operators should develop i) a media relations plan and ii) a passenger communication plan. The Media relations plan should identify:

1) How information is, where appropriate, coordinated with other Public Transport Operators (PTOs)/ Infrastructure Managers (IMs).
2) Who in the PTO/IM organisation is responsible for authorising security information to be released.
3) Who is authorised to release security information to the media. When security incidents occur this may be controlled by a government security agency or the police.

A policy for communicating with passengers on security matters would need to identify who will be involved in its development and how and by what means information is disseminated. COUNTERACT further recommends involving other security agencies who interface with passengers, such as the police.

CRISISCOMMSCORE

The CRISISCOMMSCORE document the "Crisis communication guide for public organisations[11]" focuses on crisis communication from the point of view of public authorities, such as municipalities or smart cities. This guide identifies three main stakeholder groups for external crisis communication: citizens, news media and response organisation and network. It identifies the main goal of crisis communication during the response phase to be saving lives. It recommends to:

[10] Rafaeli, G., Abbott.P. (2009). Planning, Organisation Public Transport Security, Countermeasures & Operations Guidance. Part D: Incident & Crisis Preparedness, Recovery and Business Continuity Planning. An output of the COUNTERACT project Cluster Of User Networks in Transport and Energy Relating to Anti- terrorist ACTivities.

[11] Reich, Z., Bentman, M., & Jackman, O. (2011). Crisis communication guide for public organisations. CrisComScore deliverable. Available at: https://cordis.europa.eu/docs/results/217/217889/final1-book-criscomscore-9789513942618.pdf

- Identify their needs for information by listening carefully to the ways in which various groups in society perceive the crisis,
- Have empathy,
- Meet these needs as fully as possible,
- Connect to leadership and social networks,
- Combine readiness and preparedness with resourcefulness, creativity, sensitivity and the capacity to adapt to changing circumstances.

It also recommends carrying out an evaluation of the crisis communication that took place during any crisis event and update plans to incorporate lessons learned.

IMPACT

The IMPACT (Impact of cultural aspects in the management of emergencies in public Transport) communication guidelines[12] were developed by examining by socio-cultural factors in managing safety and security issues related to emergencies in public transport systems. The guidelines are hereafter reproduced:

Communication guidelines during emergency aim to exploit communication strategies and messages framed before emergency, use information collected in advance to identify and reach vulnerable passengers, apply a communication style that is clear and concise (for example, providing short messages and giving the relevant information first), take into account the hypothetical incapacitation, both physical and psychological, experienced during an emergency by victims. To do so:

- Issue effective messages
- Ensure redundancy
- Reach all audiences (including audiences not familiar with main language used)
- Maintain constant access to mobile communication networks
- Enable feedback (two-way communication)
- Disseminate useful information
- Take care about social media communication role
- Prevent or promote specific crowd behaviours according to situation
- Optimize evacuation process
- Promote Cooperation
- Reach vulnerable audiences with last minute warnings
- Manage the “emotional” atmosphere
- Be aware of and control own body language
- Stimulate compliance

Communication guidelines for after an emergency aim to exploit time resources to personalize interventions, implement different interventions for short-term and long-term effects of the traumatic event, use information collected in advance to identify passengers with special needs, and apply a communication style that takes into account the symptoms experienced by victims. To do so:

- Identify, locate and reach people in need of help
- Help families and groups reunite
- Reduce long-term post-traumatic symptoms occurrences
- Avoid cultural clashes

[12]Tomasello, P., Hueting, R., Tedeschi, A., Golfetti, A., Dambra, C., & van der Wal, N. (2017). Multi-cultural Communication Guidelines: Before, During and After an Emergency. 3rd SCF International Conference on “Economic and Social Impacts of Globalization” Proceedings. http://www.scfconferences.com/wp-content/uploads/2019/07/3.SCF-INTERNATIONAL-CONFERENCE-PROCEEDINGS.pdf#page=222

- Manage organisation reputation
- Learn from experience

IMPROVER AESOP guidelines

The IMPROVER project developed the AESOP guidelines for effective communication between critical infrastructure operators and members of the public during crisis[13]. They are reproduced here:

- **Analyse** the information-seeking behaviours of local populations before deciding which media channels to deploy during disasters;
- **Engage** key stakeholders in order to ensure message consistency across traditional and social media platforms;
- **Social media** should be used to provide real-time updates to citizens about ongoing efforts to restore services;
- **Observe** and adhere to context-specific regulatory frameworks for emergency management and resilience:
- **Post-disaster learning** should be employed in order to enhance and develop future communication strategies.

LETSCROWD Communication Toolkit

The LETSCROWD project developed their LETSCROWD Communication Toolkit[14] to be used by Event organizers, Law Enforcement Agencies Officers (LEAs), Security officers and First responders. The toolkit is heavily focused on the organisation of major events. While not specifically addressing the needs of rail and metro transport operators, they are reproduced here for reference. The guidelines are divided into three parts pre-event phase, during an emergency and taking into account socio-cultural factors. The pre-event phase, as well as recommendations regarding the issuance of warnings is omitted as outside the scope of this project.

General Communication Guidelines For The Execution Phase, In Case Of Emergency

- Monitor and analyse what is happening on the field
- Exploit the communication strategies identified in the pre-event phase (e.g. concerning channels)
- Use information collected in advance on target audience to frame adequate messages to communicate with them
- Reach vulnerable audience (e.g. visually impaired visitors, auditory limited visitors, etc.).
- Tell people how to behave
- Facilitate information seeking in the event venue
- Address people's concerns with concrete answers
- Show that you care
- Local, regional, national communication should be coordinated

General Recommendations To Address Crowds' Socio-Cultural Aspects

- Be aware of the broader social, cultural or political considerations that may influence communication with your audience.
- Translate written materials in the major languages spoken by people attending the event
- All the information about the event should be provided in different languages

---

[13] These requirements are quoted from – IMPROVER D4.2 A communication strategy to build critical infrastructure resilience at link.

[14] DeepBlue. (2019). How To Communicate With Multicultural Crowds In Mass Gatherings - Communication Toolkit. LETSCROWD project. https://letscrowd.eu/wp-content/uploads/2019/09/LETSCROWD_Communication-TOOLKIT.pdf

- Set up language services
- Build partnership and networks with local cultural communities
- Identify bilingual/ multi-language employees who can provide assistance to people attending the event,
- Improve signs and signals recognisability

RESILENS European Resilience Management Guidelines

The RESILENS project produced the European Resilience Management Guidelines (ERMG)[15] giving guidance to CI organisations (CI operators and owners) to enhance the resilience of their and interconnected CI systems. While a dedicated CCF was not produced as part of the ERMG, some elements do relate to crisis communication as communication is important for CI resilience before, during and after any disruption.

ERMG states that CI organisations should:

- Establish a communications/media team
- Work to a pre-prepared communications plan with supporting procedures
- Consider the media as an important stakeholder who could be helpful with communicating when an event occurs and be considered as part of the communication plan.

Given the importance of external communication the ERMG identifies the following key needs:

- Know who in the CI organisation has the authority to release information, and on what issues to service customers, to the media and/or the public.
- Have pre-prepared communication templates for media/other release based on different scenarios (to be completed with real time detail) taking account of legal advice on content and the potential audience. Using templates during stressful periods and avoiding the use of jargon, industry/technical terms. These templates should be readily available as when an incident occurs responding is the priority.
- Have the necessary communications means (phone, radio, fax, mail, letter, use of social media etc.).
- Use and monitor media and social media information to check out communications related an incident. Ensure CI decision makers are aware of publicly available information.
- If the CI operation is e.g. a major hazard facility, fully understand the requirements of any related special plans or instructions.
- Present facts in a precise and factual way

SECUR-ED - Emergency & Crisis Preparedness Handbook

The SECUR-ED (SEcured URban Transportation – European Demonstration) Emergency & Crisis Preparedness Handbook[16] does not provide a CCF and instead recommends to implement the external communications strategy. It further identifies the following issues related to crisis communication:

- Ensure appropriate communications (good/bad news / press statements / liability);
- Provide passenger information on revised services/emergency timetable;
- Ensure public statements are coordinated with the police and/or other involved agencies to ensure the appropriateness also factual accuracy;

---

[15] Abbott, P., Rafaeli, G., Shazar, Y. & Cherpak, E. (2018). European Resilience Management Guidelines (ERMG). D3.2 of the RESILENS project. Available at : https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5be5bfda4&appId=PPGMS

[16] Rafaeli, G., Abbott.P. (2014). Emergency & Crisis Preparedness Handbook in 3 Parts –1. Security Incident Response & Crisis Management Plan Preparation & Maintenance. 2. Security Incident & Crisis Management Arrangements. 3. Specific Scenario Security Incident Response Plans. An output of the SECUR-ED project Secured Urban Transportation-European Demonstration.

- Employ pre-planned statements;
- Use a controlled single focus media contact;
- Communication with media should be subject to:
    - Full confidentiality concerning any details of the incident without the agreement of the police and specialist responders;
    - Non-disclosure of details of any external responding organisations.

SHERPA - Railways' Crisis Communication Guide Towards the Public for Terrorist Incidents

The SHERPA project reviewed how railway companies and authorities responsible for security in railway surroundings have used digital media to raise security awareness of both personnel and passengers. This led to the development of the Railways' Crisis Communication Guide Towards The Public For Terrorist Incidents[17], which provides recommendations on what should be considered when using digital media for crisis communication. They are provided below:

Railways' Crisis Communication Guide Towards The Public For Terrorist Incidents

Setting up one's digital media strategy

The following are recommendations on how to set up one's digital media strategy for security awareness and terrorism related crisis communication. The recommendations related to the setting up of a mobile application for security awareness have been removed as outside the scope of this deliverable.

- Determine appropriate types of information for dissemination;
- Identify target audiences;
- Identify preferred medium of communication;
- Identify when and why communication should be provided;
- Determine the appropriate format of information for dissemination;
- Set up an approval process;
- Provide for regularly response to posts and requests;
- Provide accurate information;
- Consider malicious or disruptive use of social media;
- Incorporate privacy law implications.

Executing one's digital media strategy

Response: during the response phase of the crisis management cycle, it is important to acknowledge the crisis and provide continuous updates, including updates that there is still no new information. During this phase, it is important to provide the public as soon as you are able to with information regarding how the terrorist attack might affect the railway transport offering/timetables. It is also a good time to make use of the crisis communication amplification potential of social media and other digital medias by repeating official information provided by official sources (e.g. law enforcement agencies). Indeed, studies have shown that the repetition of key messages as well as finding the same information from different sources helps the public to take the correct action. When a terrorist attack take place, people begin a search for information not only relating to what has happened, but also about how they should act. People want to be informed on this, and so it is a good opportunity to provide them with advice, such as those provided by national authorities.

Recovery: after the attack has happened and the security of all involved is once more assured, this is the prime time for the railway company to examine their crisis communication strategy to evaluate what worked and what didn't work. Another key aspect of crisis communication in the recovery phase of the crisis management cycle

[17] SHERPA. (2020). Best practices on the use of digital media for raising awareness among the public of customers and fostering cooperation with authorities. SHERPA project deliverable D5.3. Available at: https://sherpa-rail-project.eu/IMG/pdf/sherpa_20201030_d53_v3_report_on_digital_media.pdf

is to use digital media as a means to restore confidence in rail travellers. Indeed, people may be apprehensive to return to an area that was part of a terrorist attack. Communicating about new security measures put in place may help to recreate a feeling of security amongst travellers.

2.2.2 Relevant Professional Associations

Relevant professional associations were identified during a working meeting with all the partners. These where then checked to see if they had published a CCF that was publicly available. This is reported in Table 6.

TABLE 6 PROFESSIONAL ASSOCIATIONS WITH CCFS

Professional Association	Existing CCF
International Association for Business Communicators (IABC)	Yes, but not publicly available.
IATA	Yes. Crisis communication and reputation management in the digital age: A guide to best practice for the aviation industry
UIC	Yes. Recommendations for Crisis Management, Chapter on Crisis Communication, subchapter on Public Communication Management of Covid-19: Guidance For Railway Stakeholders, chapter on external communication.
UITP	No.

IATA

IATA regularly updates it's Crisis communication and reputation management in the digital age: A guide to best practice for the aviation industry[18], with its latest version dating from 2018 and focusing on the "always on" model of crisis communication. Since smartphones and social media are ubiquitous in this day and age, they recommend that aviation crisis communication uses the same approach. The guideline also mentions fake news and states that the best way to counteract it is for organisations to "say what it is doing, and do what it says (p.9)." The guidelines further lay out the main elements of a Crisis Communication Plan as follows:

- Statement of company communication policy, including the names (or positions) of authorized spokespeople
- Outline of the communication organization, and its interface with the corporate Crisis Management Team (the head of communications should sit on the CMT)
- Protocols for ensuring all available communication channels are properly coordinated and that information and messaging is consistent to all audiences

[18] IATA. (2018). Crisis communication and reputation management in the digital age: A guide to best practice for the aviation industry. https://www.iata.org/contentassets/86b7f57b7f7f48cf9a0adb3854c4b331/social-media-crisis-communications-guidelines.pdf

- Description of functional roles and responsibilities, and candidates
- Checklists for each functional role, outlining the main tasks
- Templates for initial statements and employee communications, including the first online posts, which can be issued immediately after key information is confirmed. Templates should be developed for various possible scenarios, including accident; serious incident; diversion; hijacking/security incident; service disruption (see section 8)
- Database with phone and email addresses of important internal and external contacts (including primary media outlets, online influencers and service providers)
- Standard forms and documentation (for example, media call logging form, press conference registration form)

The IATA guidance also has communication recommendations specific for a cyber attack:

- Identify the most likely scenarios or risk factors, in consultation with the IT department
- Agree the terminology which will be used to describe the nature of the event and the impact on the company's IT infrastructure, bearing in mind that it must be comprehensible to non-specialists
- Determine the external parties (police, regulatory authorities) which may be involved if a cyber attack is confirmed
- Determine the regulatory requirements for disclosure (to regulators and customers) in the event of a data breach which compromises customer data
- Become familiar with General Data Protection Regulations and any requirements/provisions which may apply to communications by the airline
- Develop a backup plan for how the communication team would operate if the company's IT or communication systems (telephones, email) were disabled or compromised. This may include plans to work remotely using personal computers, telephones and email or messaging services which do not interact with the company server.
- Ensure the communications department is notified immediately whenever a cyber attack is suspected or confirmed, even if the Crisis Management Team has not (yet) been activated
- Activate social listening to monitor any conversations about the cyber attack and the impact on customers
- Focus messaging on the actions being taken to mitigate the impact on customers and restore normal operations. Emphasize cooperation with the relevant authorities to investigate the nature and source of the attack.

UIC – Covid-19 Crisis Communication Guidelines

Within the UIC document Management of Covid-19: Guidance For Railway Stakeholders[19], there is a chapter on external crisis communication, reproduced here:

Why communicate? External communication is targeted at railway passengers and the general public. Railway undertakings and infrastructure managers are viewed as trustworthy, reliable sources by the public and as such there is an expectation for information to be shared. Meeting this expectation helps to combat the spread of misinformation & rumours and also to maintain corporate reputation both during and after a crisis event. Thus, one important challenge for the railway operator is to obtain fast and reliable information from the respective national authorities and relay it to both staff and end-users.

What to communicate? Types of information railway undertakings and infrastructure managers might be expected to provide to the public and passengers could include:

[19] UIC. (2020). Management Of Covid-19: Guidance For Railway Stakeholders. https://uic.org/IMG/pdf/guidance-for-railway-stakeholders.pdf

- Providing simple means for the public to become part of the solution:
    - Stay at home if you are sick;
    - Use of the flexed elbow method to cough;
    - Clean hands with soap and water or with alcoholic-based gel (ensure availability);
    - Take social distancing measures
- Explanation of Covid-19 symptoms
- Encourage customers to use online ticket purchasing (to avoid gathering in the railway station ticket offices)
- A clear cancellation policy (refund or exchange)
- Stating what clients should do if symptoms appear during their travel
- Sharing information about the current situation in the country
- Informing on any special measures for cross border services
- Providing information on who to contact for medical advice
- Reassuring users of the railway system as to the additional/reinforced cleaning regimes in place (e.g. what time the cleaning person passed)

On which channels to communicate? In a crisis, people tend to use the same communication means that they use in their everyday life and thus information on Covid-19 should be readily available on all communication channels regularly used by the company (website, social media, apps, in station announcements, via press releases, etc.).

How to communicate? At a general level, visual communication (infographics, videos and pictograms) is recommended. Visual communication helps to avoid language and other functional needs barriers. They can be provided by the National Authorities or International Health Organisations (WHO or ECDC). For example, cartoons depicting how to cover one's mouth when sneezing or coughing using the elbow technique are particularly relevant to the Covid-19 outbreak. It is also recommended to use easy to understand language (use laypeople's language and not technical terms), be concise, and adapt communication to people with specific special needs (deaf, blind, etc.). Collaboration with national associations of people with reduced mobility and special needs is strongly recommended. When using social media, keep in mind relevant hashtags. Examples currently (12/03/2020) trending on twitter include #covid_19, #CoronavirusPandemic, #COVID19. Sometimes a location is added to a hashtag when relevant, for example #covid19fr is trending in France.

When to communicate? During all stages of the crisis.

UIC – Recommendations for Public Communication

The UIC Recommendations for Crisis Management[20] includes a section on crisis communication to the public, reproduced here.

The intensity and the outcome of a crisis can be heavily influenced by the handling of the press and the media. Therefore, it is recommended that the public communication is taken into account in the Crisis Management Plan. It may be advisable to prepare a separate Crisis Communication Plan that covers (for example) the following:

- establishment of media and social media monitoring capabilities,
- spokesperson, space for press conferences and statements,
- communication to the key stakeholders,
- feeding of information into the social media,
- kind of information that should be released and how often,
- approval process and the authority for the release of information,

[20] UIC. (2017). Recommendations for Crisis Management. https://uic.org/IMG/pdf/crisis_management_report.pdf

- information process to your employees,
- handling of questions/requests from media, families, victims, etc. (amount!),
- preparation of key media contact sheets and telephone/stakeholder log sheets,
- preparation of black/dark websites or splash sites for crisis communication,
- preparation of pre-draft messages,
- preparation and publishing process of FAQ,
- (external) assistance by using Call Centers, Communication Advisors.

The responsibility for the crisis – and public communication – should be an integral part of the Central Crisis Management Team.

2.2.3 Crisis Communication Frameworks mapping

When analysing the 11 publicly available CCFs, four main categories of information present were discovered. Not all CCFs mentioned each thing, and some items are only from a single CCF. Table 7 demonstrates the grouping of elements found in the above mentioned CCFs, and in how many different CCFs a given element was found, indicated in parenthesis.

TABLE 7 CATEGORISATION OF CCF ELEMENTS

Components of a CCF	Communication means/channels mentioned	Recommendations on how to communicate	Elements pertaining to recovery
• Define the plan (6) • Set up roles and responsibilities (5) • Follow regulations (6) • Identify external stakeholders (3) • Coordinate with other relevant stakeholders (6) • Monitor & analyse what is happening (4) • Provide pre-prepared communication messages (5) • Determine media most used by target audiences (7) • Determine the information needs of target audiences (3) • Determine which information is considered sensitive (2)	• Multiple channels (3) • Social media (4) • Two-way communication (3) • Cultural leaders (2) • Facilitate information seeking in the location (e.g., staff, signage) (1)	• Be flexible (1) • Be clear & concise (6) • Be effective/ appropriate (3) • Provide regular updates (1) • Be inclusive/ accessible (3) • Show empathy (3) • Be consistent (1) • Be actionable/provide measures (5)	• Identify, locate and reach people in need of help (1) • Reduce PTSD[21] (1) • Restore Confidence (1) • Manage Reputation (1) • Identify lessons learned (4) • Update the CCF (4)

[21] Post-Traumatic Stress Disorder

2.2.4 Results from the questionnaire to end-users on their CCFs

The questionnaire can be seen in ANNEX III. Questionnaire. The questionnaire was sent to 41 railway and metro stakeholders. We received 13 responses. Questionnaire data was collected from 2 February 2022 to 25 March 2022.

When asked if their company has a CCF, 11 responded positively and two negatively (Figure 1). For the two respondents who do not have a written CCF, they explained that they are well aware of what to do in the case of a crisis. Those that have CCFs stated that they cover both malicious and non-malicious crises, as well as cyber, physical and cyber-physical crises. When it comes to roles and responsibilities, these are either defined in the CCF or are based on already existing (communication) structures/roles (Figure 2).

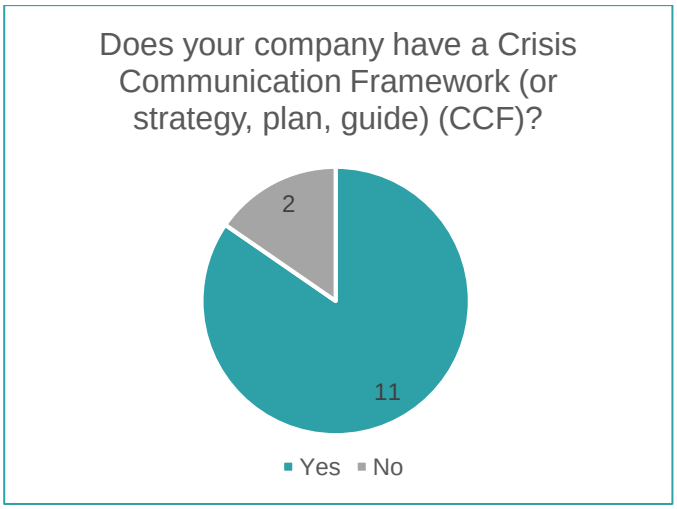

FIGURE 1 QUESTIONNAIRE Q1

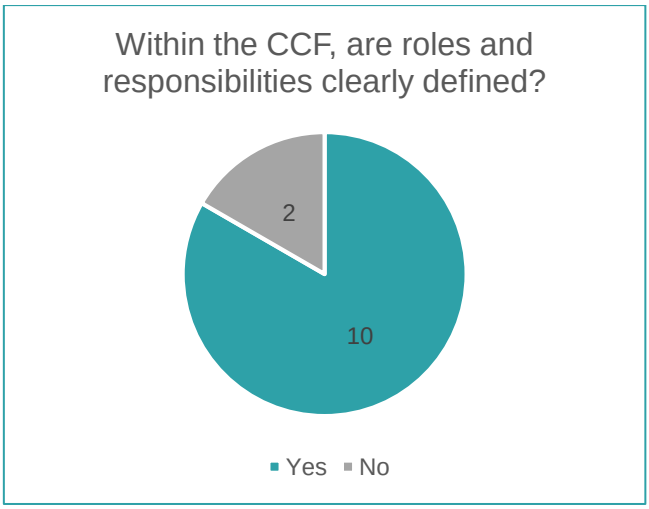

FIGURE 2 QUESTIONNAIRE Q2

When asked with whom the transportation stakeholders share crisis information, almost all respondents selected all of the proposed external stakeholders (traditional media, self-produced media, other transport operators and public authorities) (Figure 3). For one respondent, the communication to traditional media and through digital media only comes from the authorities. A similar result was found when asked which type of crisis information they share (Figure 4) and which means they use to share said information (Figure 5). When asked if the CCF provides guidelines for two-way communication, only one respondent said no (Figure 6).

Respondents were split when it came to including provisions for vulnerable groups directly in their CCFs (Figure 8). Those that stated that it was not the case explained that this is because the same inclusive communication methods are used whether there be a crisis or not. As explained by one respondent, the CCF “does not contain any specific elements pertaining to people with specific needs. However, [our company] is committed in all its activities (in non-crisis and crisis mode) to ensure full accessibility.”

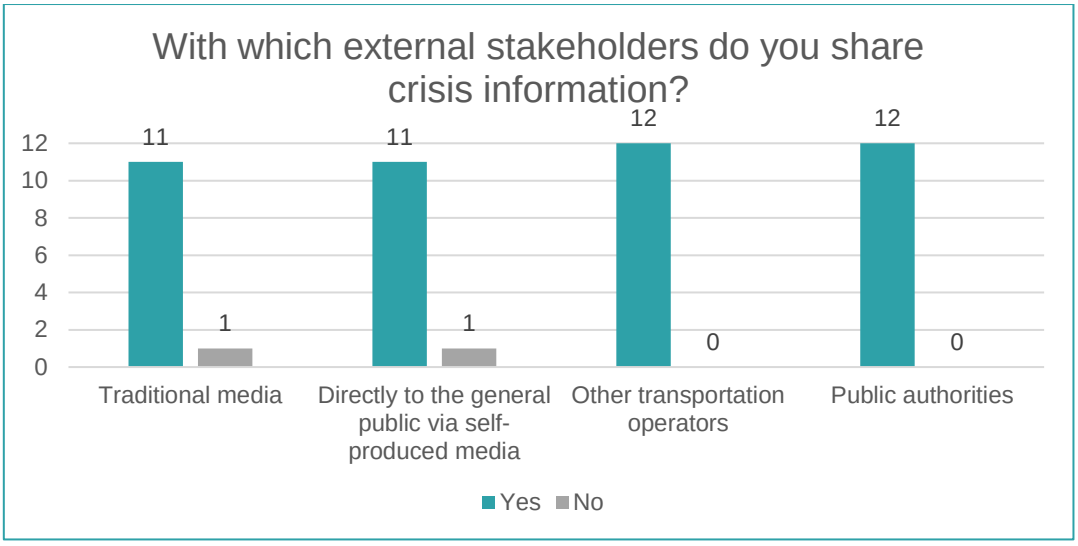

FIGURE 3 QUESTIONNAIRE Q3

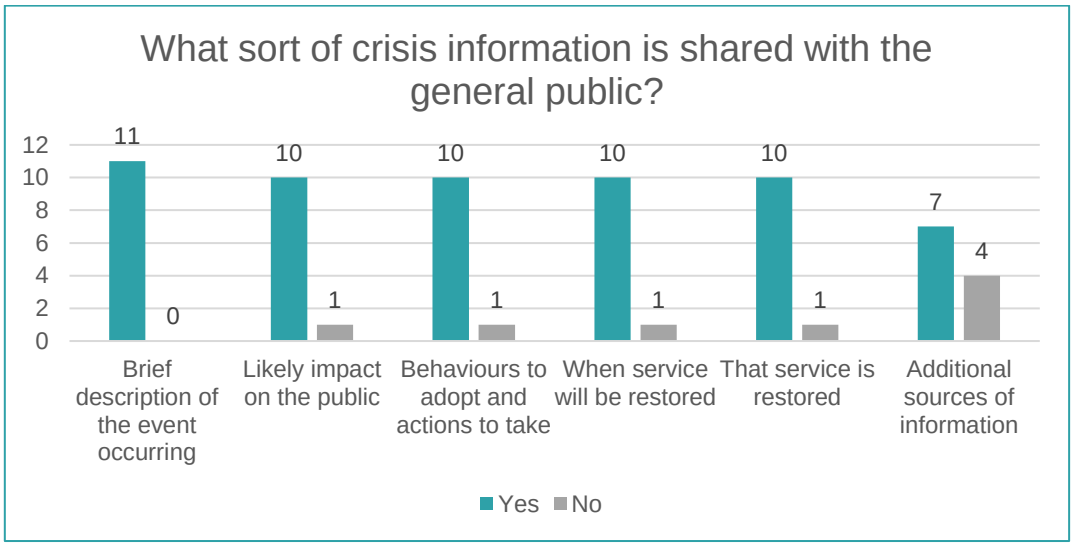

FIGURE 4 QUESTIONNAIRE Q4

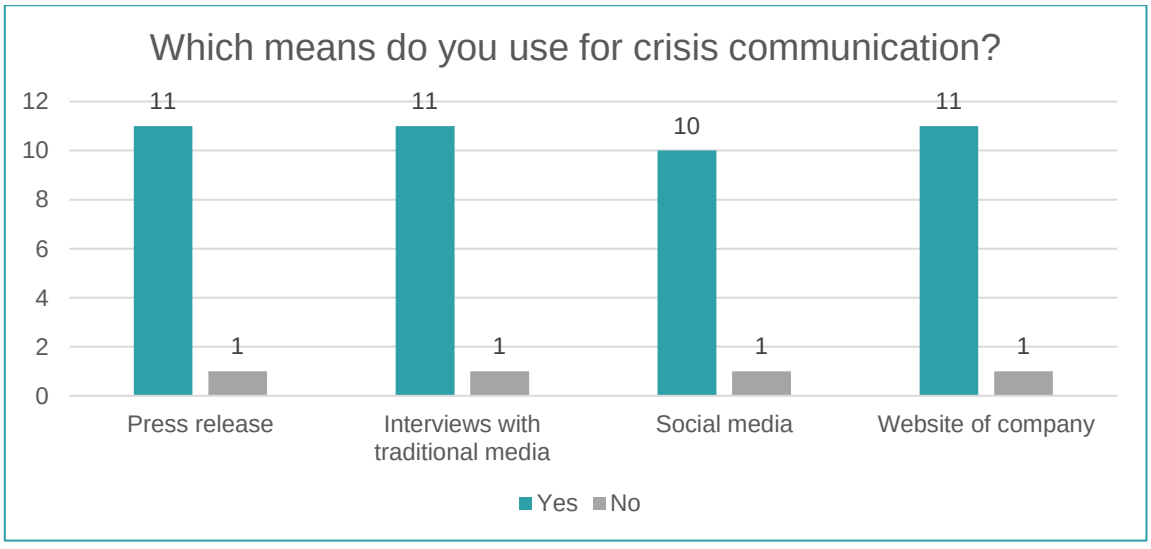

FIGURE 5 QUESTIONNAIRE Q5

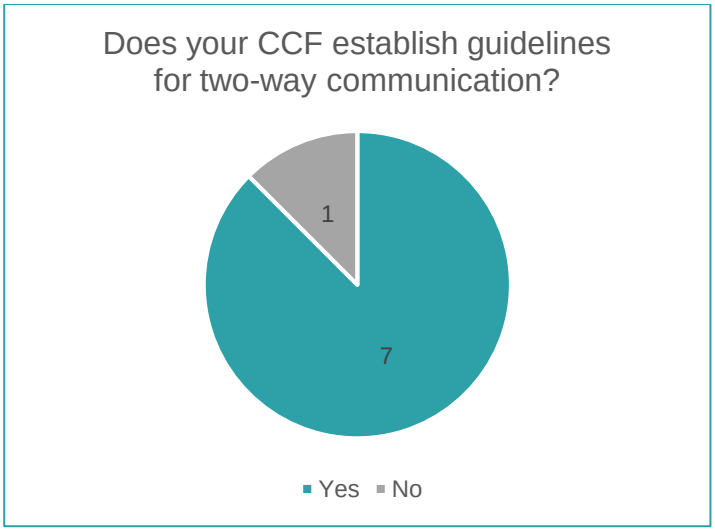

FIGURE 6 QUESTIONNAIRE Q6

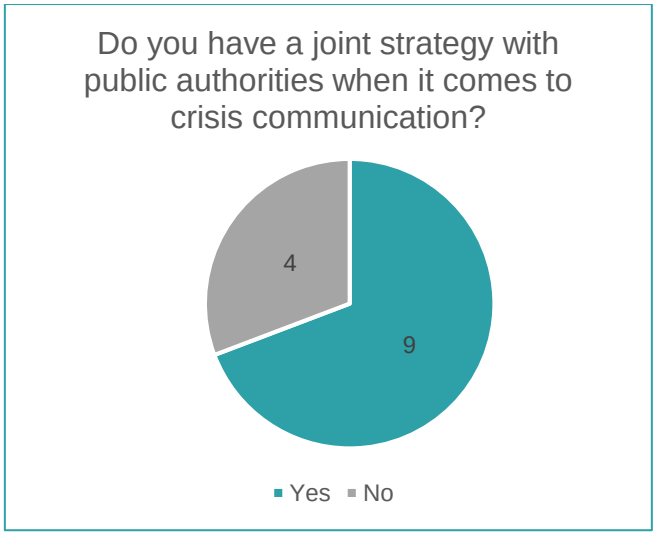

FIGURE 7 QUESTIONNAIRE Q7

The majority of respondents have a joint strategy with authorities when it comes to crisis communication. Those that said no explained that while there is no official joint strategy, they would of course work closely with authorities when it came to crisis communication. For example, one respondent replied that they "do not have a joint strategy or policy on this. But of course at the moment of a crisis we work together with all parties involved, also public authorities." While very few CCF differentiate between victims and witnesses (Figure 10), most respondents take into account privacy issues before sharing crisis communication, with several mentioning GDPR (General Data Protection Regulation).

When asked which information their company considers sensitive, the following information categories were shared:

- Personal details about victims (including photos),
- information that might help perpetrators,
- incident/Crisis management plans,
- locations of control rooms and suicide.

Concerning Fake News, while an official policy is present in only half of the CCFs, respondents indicated that they would tackle the issue by sharing the correct information. All 11 respondents to the question, "does your company take into account the feeling of security of passengers and station visitors when communicating crisis information?" stated "Yes." Lastly, ethical considerations brought up by respondents included:

- Transparency,
- Being in line with company's core values,
- Respecting privacy,
- Aftercare of victims.

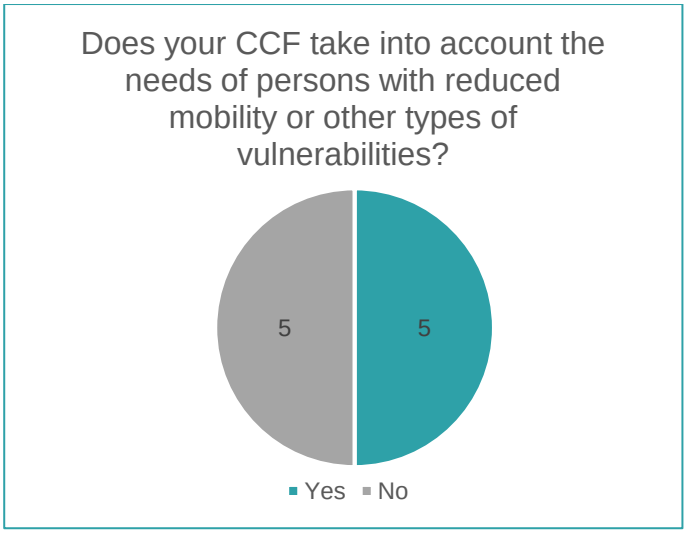

FIGURE 8 QUESTIONNAIRE Q7

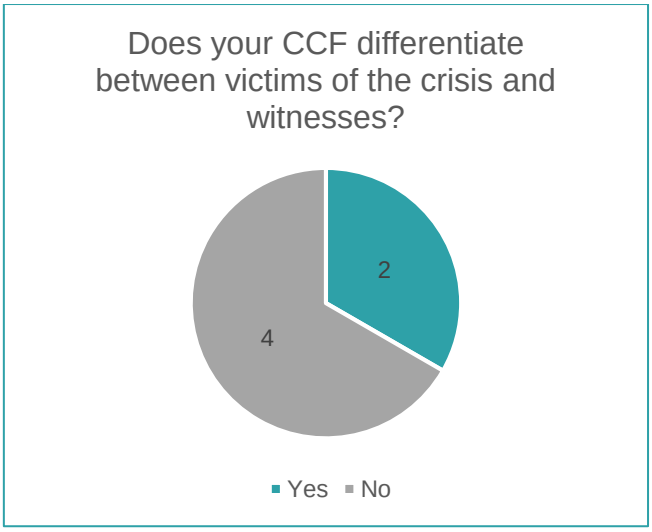

FIGURE 10 QUESTIONNAIRE Q9

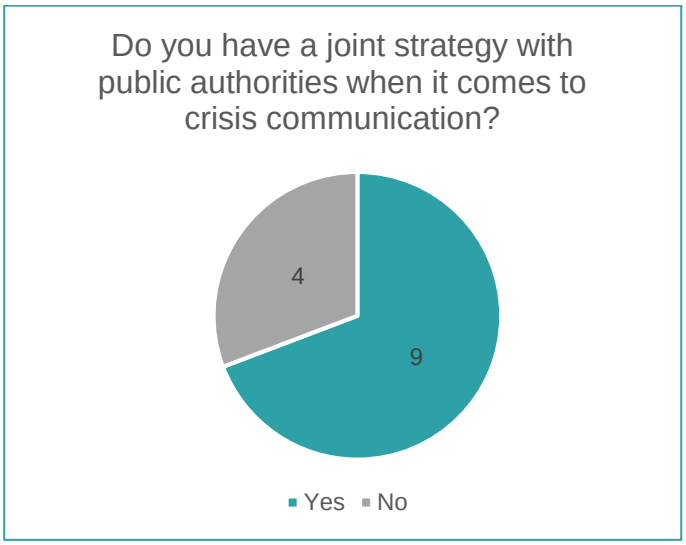

FIGURE 9 QUESTIONNAIRE Q8

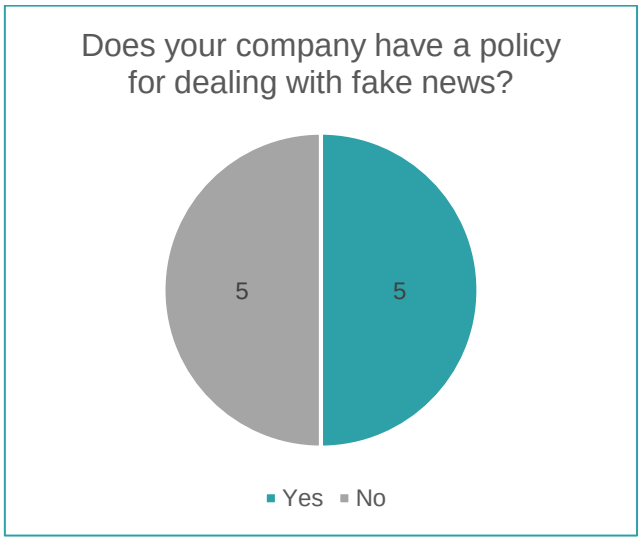

FIGURE 11 QUESTIONNAIRE Q11

2.3 Lessons learnt from past crises

This section examines past crises that have impacted the railway and metro sectors to derive learn lessons applicable to future crisis communication. It does so in two ways: through desk research based on the SAFETY4RAILS database of 94 past failures and incidents and through interviews with the consortium end-users.

2.3.1 Based on the S4R D2.2 data base

The SAFETY4RAILS database of 94 past failures and incidents which was published[22] as part of deliverable 2.2 – Report on past failure analysis and lessons learnt[23] was analysed anew through a crisis communication

[22] While the database is based on open-source information, it could be a useful collation of tactics providing information for would be attackers. On this basis, the database was declared confidential.

[23] Szabó, R, Belloy, F. et al. Report on past failure analysis and lessons learnt. Deliverable 2.2 of the SAFETY4RAILS project. https://safety4rails.eu/wp-content/uploads/2022/03/S4R_RPT_D2.2_V1_0.pdf

lens. Each open-source information (online resources such as newspaper articles, Wikipedia pages) associate with a given past failure/incident was analysed and any reference to communication was added to the database. Each past failure/incident was also subject to additional online research to detect any other sources not already available in the database and collected additional information related to crisis communication. In total, 41 out of the 94 past failures/incidents reported mentioned crisis communication aspects. It is important to note that as most of the open source information came from newspapers articles, these were most often published after the crisis had passed.

Looking closer at the 41 past crises, the information shared via the newspaper articles about the event mostly came from the railway stakeholders (Figure 12). In a few cases, the information shared about the railway came directly from the authorities. Most of the time, the information cited in the newspaper article was quoted from a spokesperson and other communication channels mentioned include announcements, press briefing, press release, website and social media (Figure 13). Overall, 80% of the crisis communication focused on describing the event and 20% communicating about service restoration (Figure 14).

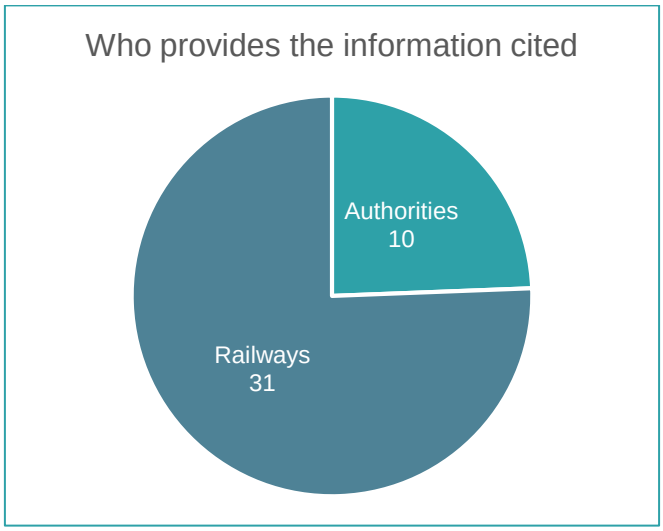

FIGURE 12 PAST CRISES DATA BASE INFORMATION PROVISION

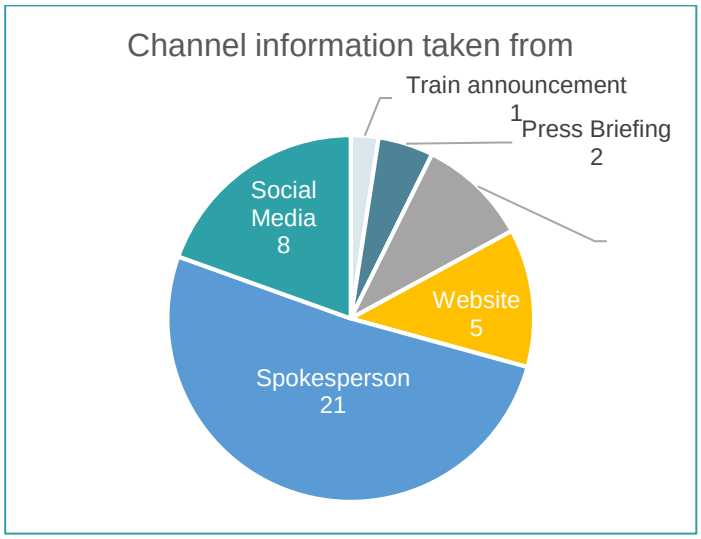

FIGURE 13 PAST CRISES DATA BASE INFORMATION CITED SOURCE

Out of the 41 past crises found, 14 were on the subject of cyber attacks. These types of attacks had some unique aspects considered in their crisis communication. Namely, in two cases the railways denied the attack and in one case, while assuring that the cyber attack had not been fruitful, that the company was implementing precautions for any future attack (Figure 14). Another specificity of cyber attacks found was stating that the cyber attack did not affect either operation safety or the safety of personal data.

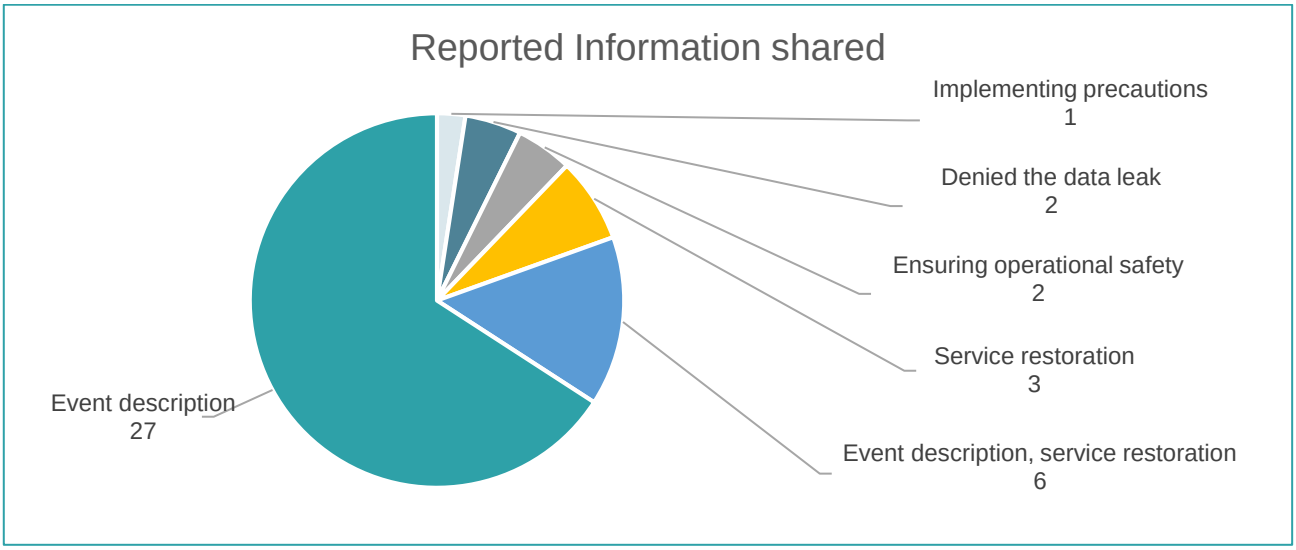

FIGURE 14 PAST CRISES DATA BASE INFORMATION TYPE

2.3.2 Based on interviews with end-users

Interviews were held with all consortium end-users for a total of 7 interviews. The interviewees were asked to pick a past crises event and tell the story of that event and the crisis communication as it unfolded. Interviews were held online and lasted for about an hour. The interview guide is available in ANNEX IV. Interview Guide.

The past events chosen by interviewees were:

- Flooding (twice),
- Communication loss and train stuck in tunnel,
- Train collision in tunnel with no passengers,
- Train collision with passengers but no casualties,
- Power loss and earthquake.

Which communication channels were used?

In the interviews, the importance of using all available communication channels was shared by interviews. This is encapsulated by one interviewee who said, “you need to use all the ways to inform people.” Specifically, social media, website, local information screens, public address systems inside stations and trains, and the press were mentioned. Social media was generally found to be the most effective means. As one interviewee put it, “Social media is the way to inform quickly, continuously, and most effectively.” The press was seen as less effective, as put by one interview, “In the press, the information typically appears a day after,” thus arriving too late to help the passengers and station visitors affect by the crisis.

By whom?

For two interviewee companies, crisis communication does not come from the railway or metro stakeholder but rather from the authorities. As one interviewee explained, “we cannot make any public announcements as a government employee.” For the other five companies, most of the time crisis communication came from the communication or public relations department. This is because, as one interview put it, the “press office or social media officer … have more tools and skills.” One interviewed company also uses non-communication department staff to provide crisis communication to the general public[24]. “We invite incident management staff to put messages on Twitter and Instagram by themselves,” they explained. However, other interviewees thought that this would be in conflict with the goal of responding to the crisis, as stated by on interviewee, “people who are managing the incident avoid social media coverage because it’s too complicated.” Another key person involved in crisis communication is the front line staff, especially the train driver, and control room staff. As put by one interviewee, “if something occurs during operation time, control center informs passengers through passenger announcement system.”

Specificities for communicating with the general public

When it came to communicating about the event to the general public, including stations visitors and passengers, interviewees put emphasis on the need to communicate quickly and effectively. As one interviewee put it, “the faster, the better.” Another said that the first communication about the crisis event should be “from the earliest stages.”

Not only was the need to inform quickly brought up, but this also went hand in hand with informing on a regular basis. A good example of this is from one interviewee who said, “you need to inform them continuously... Just because you are working to solve the situation does not mean that the customers know about it.”

Lastly the importance of trust was mentioned by one interview, “they have to trust our service.”

[24] This is dependant of the type of crisis they are dealing with and the phase the crisis is in. They’re not posting on twitter or Instagram in case of a terrorist attack or “in the heat of the moment”.

Specificities for communicating with authorities and other transport stakeholders

All interviewed companies communicated with the authorities and other transportation stakeholders during the described crisis and were aware of the importance of communicating amongst each other. This was made clear by one interviewee who said “That information is important not only inside but also outside the company. We have to inform the different agents that are involved in this situation.” That said, it wasn’t always the crisis communication team who took that role. “When we talk about crisis communication, we are mostly thinking about it from the public or the operators’ perspective. And then when we’re thinking about authorities, we’re thinking more along the lines of the crisis management team who talks to them.”

Concerning who to contact, external stakeholders mentioned included emergency services, police, government and other authorities. For example, one interviewee explained “it's clearly defined who you contact and when. At this level, we contact the police. At this level, we contact the Ministry of Transport.” Another brought up the fact that they “informed the police guys and emergency response units simultaneously and immediately.” Railway and metro companies also work closely with municipalities and “have communication strategies informing the municipality directly about what is happening.” Several interviewed companies described a type of joint command center, where information would be shared and communicated to all involved stakeholders. For example, one company has “one number for the government contact center managing - it’s like an emergency center. They involve police, medical assistance, and all the [communication] resources that are necessary.” Another mentioned that “we have a local transport authority, and normally when there is an incident affecting us or other operators, we inform them. They can adapt the offer to the situation we are living in.”

Fake News

When asked if fake news was an element in the described crisis, almost all interviewees said no. One interviewee put it well, “normally you don’t have fake news. Some fake news is often produced by the ignorance, not intentionally.” The exception was one of the flooding crises, whereby people were using photos from a past flood to claim that the flood water was still present in an area where the water had been removed. Despite not having much experience with fake news, most interviewees said they would respond to it and counteract it by sharing the true information.

Sensitive Information

When asked if any information was deemed sensitive during the described crisis, interviewees said it very much depended on the crisis type. For one interviewee, “in the middle of a crisis, all information is sensitive.” However, most acknowledged that in the past crisis they described, there was not any information deemed particularly sensitive. Two exceptions were brought up, but were not taken from the chosen crisis examples used in the interview. One, suicide, ““Transport operators don’t share the victims of suicide,” and the other, a terrorist attack, “with regard to the closure of stations because the perpetrator might have been there… we haven't shared any information about that and left it all to the official government agencies.”

Lessons Learned

Overall, three lessons learned were shared. The first was that explaining what is happening to the public is equally important to addressing the crisis at hand in an effective manner, for without communication “the client thinks you are not managing this situation right.” The second was the importance of communicating with other transportation actors and “to think about how we can work better together.” The third was that a crisis can go on longer than expected and so it is important “to prepare enough colleagues to be available.”

Recommendations

The following list demonstrates the crisis communication recommendations that interviewees would like to share with other transport operators:

- Create understanding
- Listen to the safety staff
- Try to put yourself in the client’s situation
- The first rule is to be sure to communicate the same information
- If you are quick in providing information for customers, they don’t have time to launch fake news
- You need to be honest and explain what is happening in a simple way, but without causing alarm

- Be active and open on social media during a crisis. It brings you more benefits than risks. Being transparent and open gives you a lot of credit and even compliments online

2.4 Feedback from S4R end-users workshops

A Crisis Communication Workshop was held on 4 April 2022 with 31 participants. Participants included consortium and advisory board end-users. The agenda can be seen in Figure 15.

Throughout the workshop, interactive sessions were held via an online polling system called Slido. A total of 29 participants joined the online live polling platform, however on average only 9 persons responded to a given question. Answers were collected completely anonymously.

Time	Agenda item
10:00 – 10:10	Welcome – ETRA
10:10 – 11:15	Presentation of the results from questionnaires, interviews, existing CCFs, past crises DB & literature review & interactive sessions on the results – UIC & LAU
11:15 – 11:25	Health Break
11:25 – 12:00	Presentation on the SAFETY4RAILS Crisis Communication Framework & interactive session - MRTS
12:00 – 12:25	Presentation on the Guidelines for sustainable communication during and after an event & interactive session - ETRA
12:25 – 12:30	Concluding remarks - ETRA

FIGURE 15 CRISIS COMMUNICATION WORKSHOP AGENDA

Overall, participants thought the workshop was a success and gave the workshop 4.8 out of 5 stars (Figure 16).

FIGURE 16 STAR RATING FOR THE WORKSHOP

2.4.1 Online Polling Platform results for Agenda Item 1

When asked if the findings from the Crisis Communication Questionnaire was in line with their expectations, 19 out of 20 respondents said yes and none said no (Figure 17).

Since the questionnaire (section 2.2.4) demonstrated that fake news is not normally considered in a CCF, during the workshop we asked if this is something that should be included. Overwhelmingly, respondents agreed (18/20 said yes) (Figure 18).

When asked to add to the list of sensitive information presented during the workshop (Personal details about victims (including photos), information that might help perpetrators, incident/Crisis management plans, locations of control rooms and suicide), the following was written in as open text:

- Other locations of the network
- Traffic control information
- Locations of devices used for controlling train traffic
- Security analysis documents
- Information which publicity might hamper investigations
- Plans of non-public areas.
- Location of security teams and access to secure areas
- Details of railway staff involved in the incident
- Workforce information
- Information, which might cause panic and social unrest
- Internal technical information

Since the questionnaire revealed that social media platforms are used for crisis communication, during the workshop it was asked which ones specifically. The question allowed for multiple answers and Twitter was found to be the most used social media platform (Figure 19). When asked if smartphone applications are used for crisis communication, respondents were split, with 5 responding yes and 4 responding no (Figure 20).

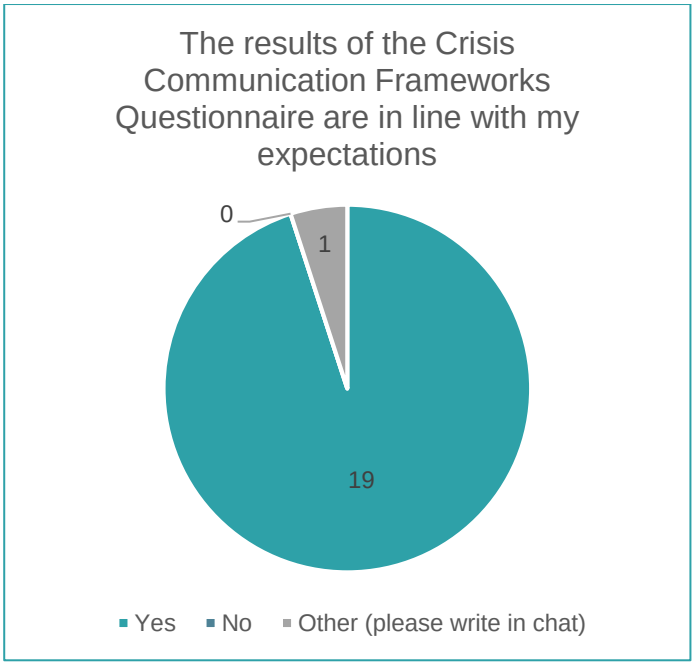

FIGURE 17 ONLINE POLLING PLATFORM QUESTIONNAIRE EXPECTATIONS

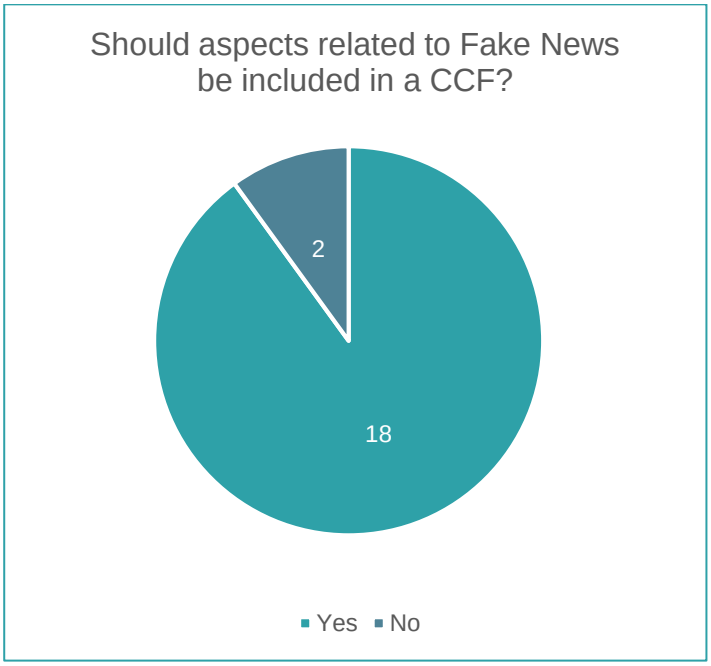

FIGURE 18 ONLINE POLLING PLATFORM FAKE NEWS

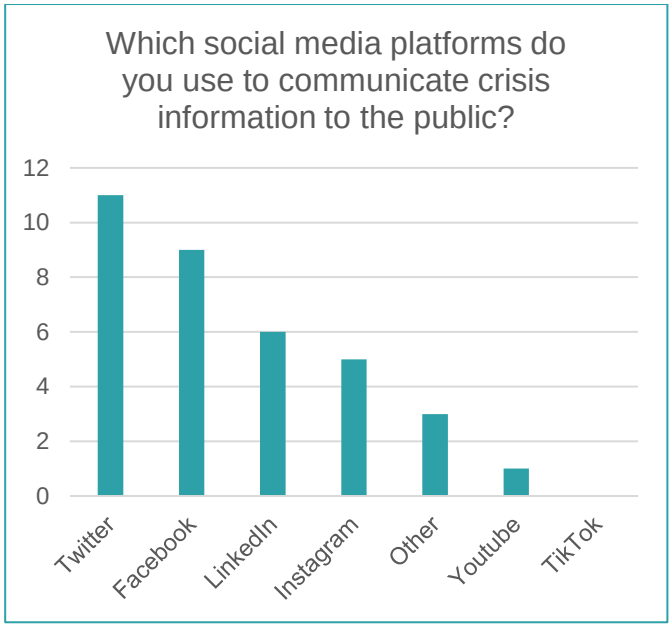

FIGURE 19 ONLINE POLLING PLATFORM SOCIAL MEDIA

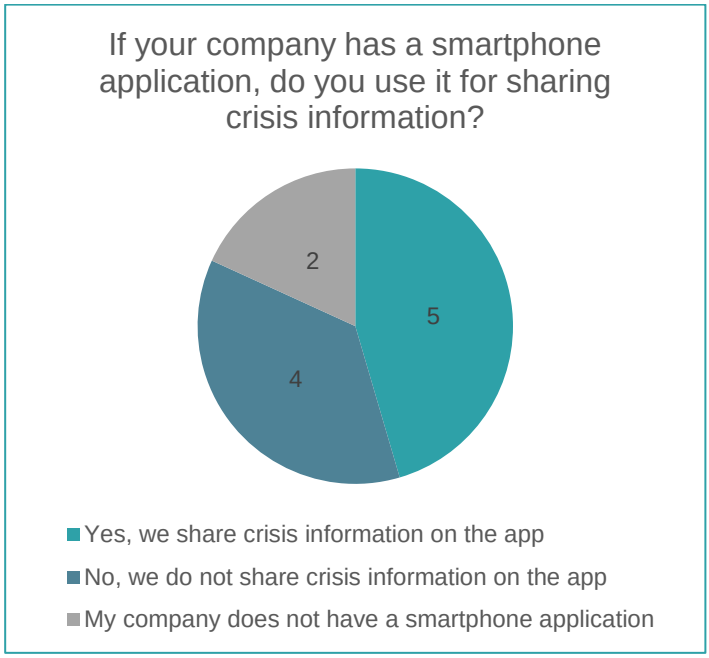

FIGURE 20 ONLINE POLLING PLATFORM SMARTPHONE APPS

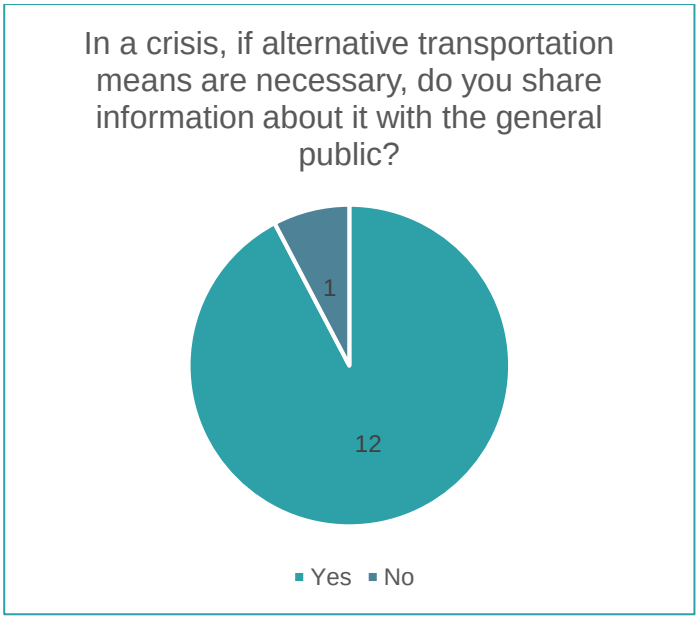

FIGURE 21 ONLINE POLLING PLATFORM ALTERNATIVE MEANS

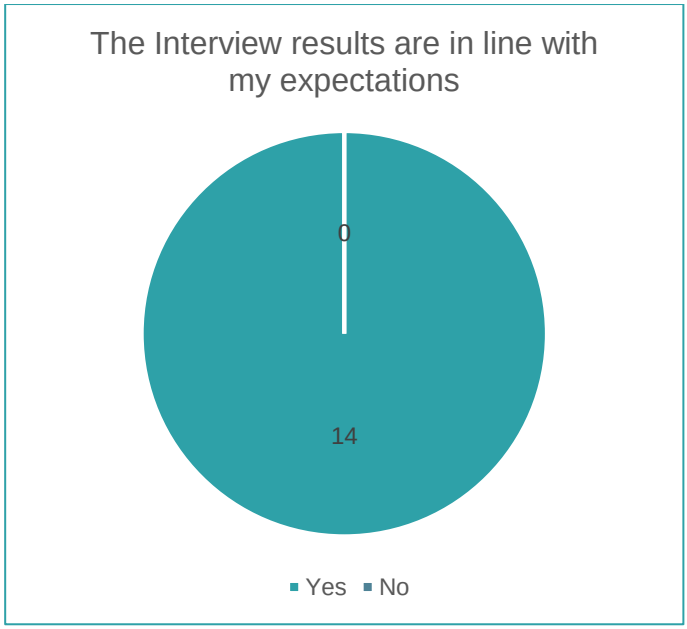

FIGURE 22 ONLINE POLLING PLATFORM INTERVIEW EXPECTATIONS

When shown the elements laid out in Table 7, respondents were asked two questions: 1) What is missing from this list in your opinion? & 2) Is there anything on this list that shouldn't be? Concerning the table column Components of a CCF, two respondents stated that the list covered everything. Other aspects identified include ensure staff know what is being said, aftercare following a crisis & evaluation KPIs of performance. Only one element was identified as missing: lessons learned. Concerning the table column Communication means/channels mentioned, one respondent suggested to add face to face contact, another suggested to add personal contacts and a last suggested to add Critical Communication Networks for emergencies: TETRA. For column Recommendations on how to communicate, the following were suggested to be missing: Transparent, have a repetitive part, fast and validated, In different languages, Possibly provide for feedback, True and Simple. When asked if there was something on the list that shouldn't be, one respondent said show empathy. For the column Elements pertaining to recovery, when asked what was missing from the list, respondents said minimise impact, measurements, rail staff understanding etc., show sympathy and KPIs performance. Nothing was found to be missing from the list.

When asked if the interview results were in line with their expectations, all 14 respondents said yes. When asked if they had any crisis communication recommendations to share, respondents said:

- "PEAR people environment assets reputation. In this order!
- Always show that you are working to show the crisis
- Continuous communication, don't wait 30 minutes for updates
- At the beginning short and cyclic infos only to save resources
- No Matter what you do, There is always room for improvement"

When asked if they had any lessons learned to share, respondents said:

- "Always consider the full audience, to include (Persons with Reduced Mobility) PRMs and the vulnerable
- If you do not communicate your work, it seems you are not doing anything to manager it
- Take care to have enough stuff in the background. A crisis can be longer than planned..."

When asked which aspects of crisis communication in railway and metro should be researched, respondents listed:

- "The role of all partners involved, how to work better together
- Relationship between openness and confidentiality

- Opinions and emotions of the users during a crisis
- Crisis communications on railways are done through classical procedures. It could be useful to update them by new technologies
- Establish a landscape of groups, bodies and communications that can happen in crises to prioritize them
- Relationship between railways and external responders to ensure common information is output
- Impact of information on crowds (what is the most effective way to communicate issues to a large amount of people whilst minimising discomfort, panic, and PTSD)
- Efficiency of using social networks during crisis"

2.4.2 Online Polling Platform results for Agenda Item 2

This part of the workshop asked about the work found in Chapter 4. When asked a question regarding internal and external stakeholders, for RU/IM, respondents were split between two answers, that coordination was either well organised or that is advisable to only coordinate with one entity (Figure 23). When asked to rank information streams, passenger information systems in stations and on trains was found to be the preferred channel (Figure 24). Lastly, participants were asked a question on the dissemination of sensitive information during a crisis, information that reveals personal details, vulnerability or create public chaos were the most often chosen (Figure 25).

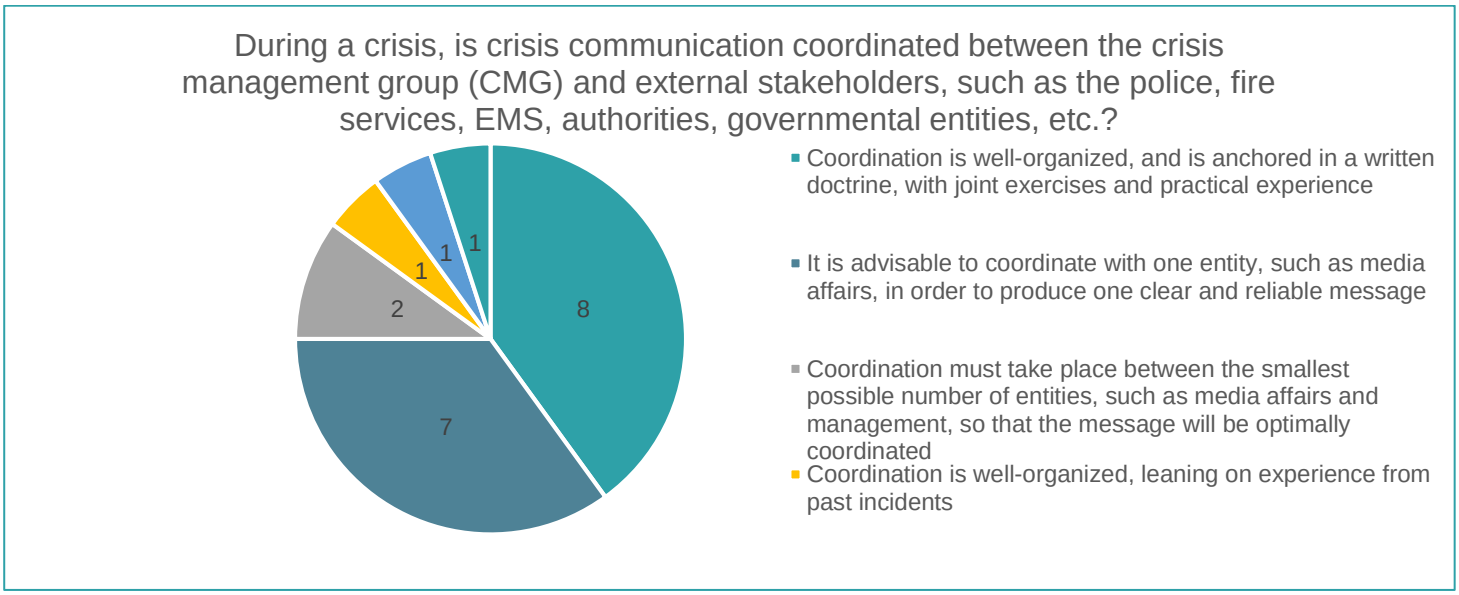

FIGURE 23 ONLINE POLLING PLATFORM INTERNAL AND EXTERNAL STAKEHOLDERS

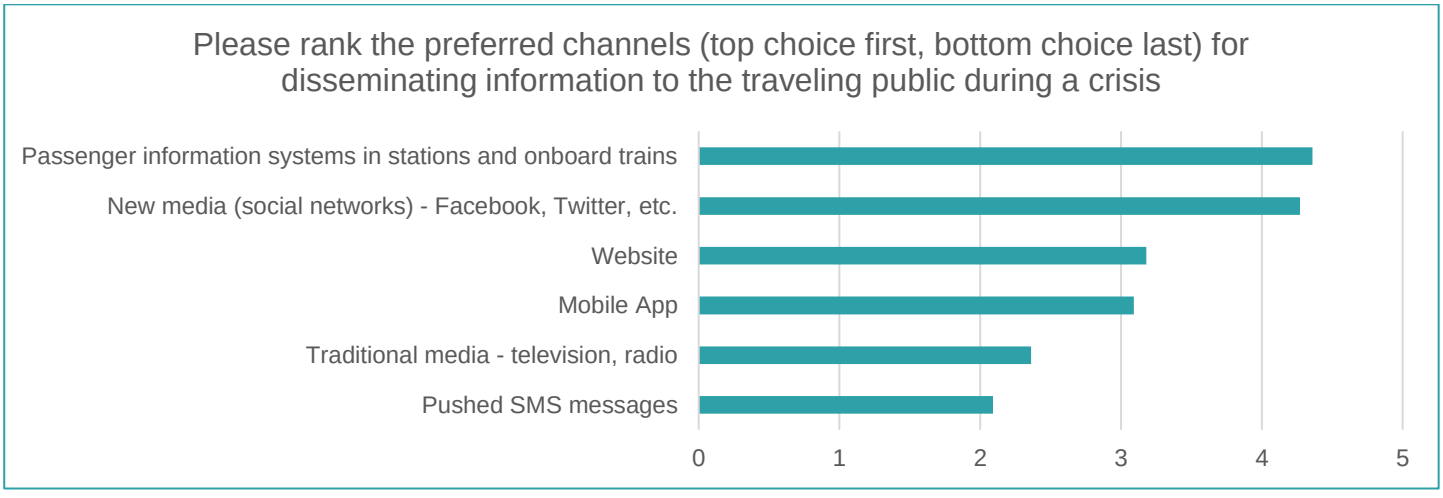

FIGURE 24 ONLINE POLLING PLATFORM INFORMATION CHANNELS RANKING

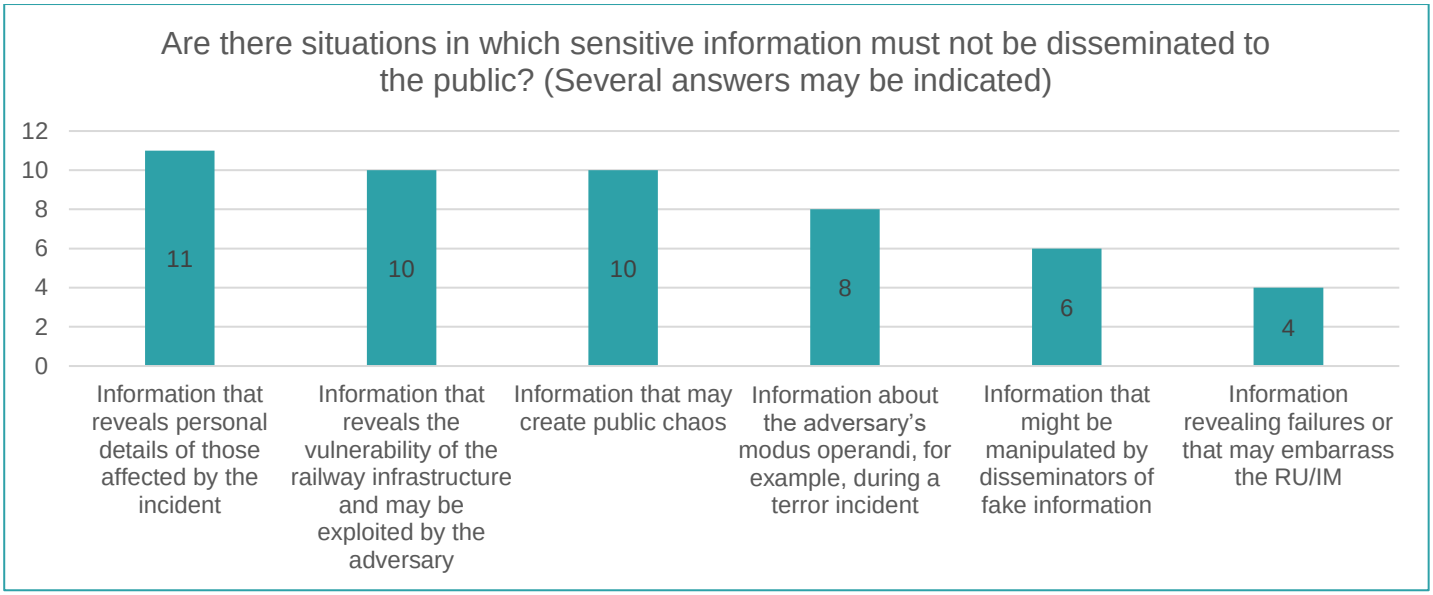

FIGURE 25 ONLINE POLLING PLATFORM SENSITIVE INFORMATION

2.4.3 Online Polling Platform results for Agenda Item 3

This part of the workshop presented the preliminary results which are now part of Chapter 4 and 5. The online polling questions focused on whether or not there was anything missing from the objectives presented. Respondents replied as follows:

- Possible safety impacts via FRMCS (Future Railway Management and Communication System) between rolling stock and landside[25]
- Keep clients satisfied
- Keep calm in the public
- To show empathy
- Ensure the safety of passengers, staff and responders
- To give prospects for action
- Keep uncertainty to the minimum possible
- Ensuring the safety of those on site also the continued safe operation of the railway.
- Clarify if it's an operational or IT based crises
- Ensure lessons learned are actually applied
- Increase the commitment, motivation and confidence between staff of the railway organisation
- Share lessons learned from the crisis.
- Communicate with vendors, to build in technical measurements to prevent a scenario twice

When asked, "What issues do you consider relevant in the case of misuse of mass media communication in a crisis (e.g.: confidential info leakage, psychological harm)?" respondents provided the following:

- Fake news
- The "hunt" effect: if you leak info about perpetrators people will be hunting a specific kind of person regardless of the relevance
- Public chaos
- Confidential issues
- Ensuring that consistent facts are regularly disseminated by all key organisations

[25] The system is in the process to be implemented and should be considered in future Crisis Communication Frameworks

- Creating chaos by publishing wrong/not validated (safety) causes
- Mass media is not for particular answers or problems

When asked if they felt that something was missing, respondents said roles of other partners in crisis communication, interface to parallel activities and don't forget that safety is the key responsibility of RUs and IMs. Lastly, when asked if they believed the information that the guidelines will provide could help your organization to improve crisis communication, respondents either said yes or not sure yet (Figure 26).

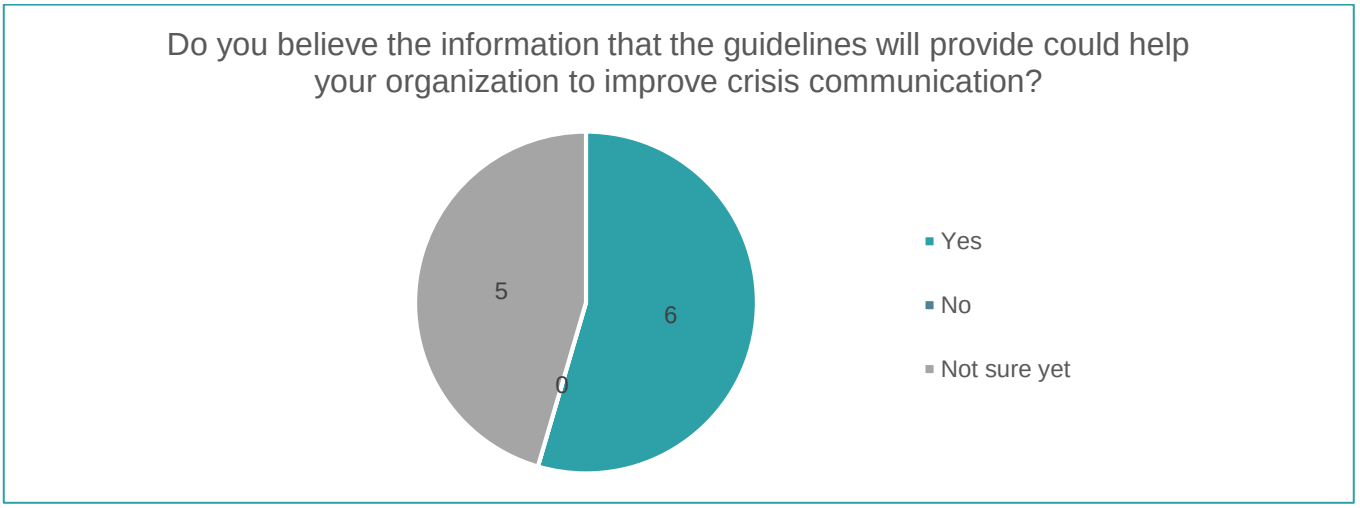

FIGURE 26 ONLINE POLLING PLATFORM HELPFULNESS OF THE GUIDELINES

2.5 Identified Gaps

2.5.1 Lack of publicly available CCFs specifically tailored to rail and metro

Based on the information found during the Crisis Communication State of the Art, it has become evident that while the majority of rail and metro stakeholders have written down crisis communication frameworks/plans/strategies, there is a lack of publicly available general frameworks.

2.5.2 Cyber security elements missing

Furthermore, only 1 out of the 11 identified CCFs specifically mentioned cyber security. This may be because, as found in SAFETY4RAILS deliverable 2.5, most crisis communication recommendations, such as showing empathy, communicating quickly and effectively, are also applicable to cyber attacks. That said, some specificities laid out in this chapter include the special vocabulary for such events as well as unique communication during past crises which included denial, ensuring operational safety and implementing precautions.

While research specific to cyber attacks in the rail sector is rare, learning from other domains we can say that in general the public expect companies to have adequate security measures in place to protect their data. Indeed, research has found that significant negative emotions are associated with data breaches[26], which are often directed towards the company who has been cyberattacked[27]. Therefore, it is especially important to

[26] E.g. Chen, H. S. & Jai, T.-M. (2018). Cyber alarm: Determining the impacts of hotel's data breach messages. International Journal of Hospitality Management; ZHANG, L., WEI, W. & HUA, N. 2019. Impact of data breach locality and error management on attitude and engagement. International Journal of Hospitality Management, 78, 159-168.

[27] Syed, R. (2018). Enterprise reputation threats on social media: A case of data breach framing. The Journal of Strategic Information Systems.

admit responsibility, as this should help restore trust[28, 29], and acknowledge the feelings and emotions of the people whose data has been breached by showing that the organisations care, as in the case of any other crisis. Research has found that, in the context of a cyberattack, transparency is the most important value to ensure company reputation protection[30]. Another particularity of data breaches is that when the data breach is announced by the media and not the company, this has a negative impact on company reputation[31].

2.5.3 Fake news not adequately addressed

None of the CCFs identified addressed fake news. This is most likely due to the more recent nature of this phenomenon. Thanks to the workshop, it is clear that rail and metro stakeholders expect CCFs to take into account how to respond to fake news.

2.5.4 Ethical considerations should be better understood

Thanks to the stakeholder consultation, this chapter was able to identify various ethical aspects of crisis communication that should be taken into account in the SAFETY4RAILS Crisis Communication Guidelines. This includes what kinds of information are considered sensitive, how to take into account vulnerable groups, and communicating truthfully, with transparency and in line with company values. While the data collected from the questionnaire, interviews and workshop demonstrated that suicide is considered sensitive information, the issue of suicide is not further addressed in this deliverable as it falls outside the scope of our definition of crisis.

[28] Seals, T. (2018). ThreatList: 1 Out of 5 Would Ditch a Business After a Data Breach [Online]. Available: https://threatpost.com/threatlist-1-out-of-5-would-ditch-a-business-after-a-data-breach/138612/ [Accessed 09/04/2020].

[29] Soomro, Z. A., Ahmed, J., Shah, M. H. & Khoumbati, K. (2019). Investigating identity fraud management practices in e-tail sector: a systematic review. Journal of Enterprise Information Management, 32, 301-324.

[30] Mañas-Viniegra, L., Niño-González, J.I. & Martínez-Martínez, L .(2019). Transparency as a reputational varaible of the crisis communication in the media contexts of wannacry cyberattack. Revista de Comunicación de la SEECI 48, 149-171

[31] Knight, R., & Nurse, J. (2020). A Framework for Effective Corporate Communication after Cyber Security Incidents. Computers & Security Journal.

3. 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

3.1 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)
- Targeted persons for Information Integration Acts (ICAs)

3.2 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.

3.3 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 (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**, i**ii) 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 other 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.

4. Crisis Communication Framework

4.1 Introduction

Effective communication is an essential input to the safe and efficient operation of transport modes, including railways. When a crisis occurs the need to communicate is immediate. The precise communication needs will depend on the type and scale of the involved circumstances as well as the implications for railway operations, for passengers and intending passengers, freight forwarders and receivers, as well as the wider public. In all cases, the priority action is to ensure that essential arrangements have been made to ensure the safety both of those involved and for the continued safe operation of the railway.

This advice can involve communication between the Operations Control Centres (OCCs) of the Railway Undertaking (RU) and Infrastructure Manager (IM) (these may be the same organisation) to ensure a common understanding of the circumstances and response needs as well as with managing their staff both on and off the site of the actual incident. Where required by the type and or scale of the crisis, a rail industry Crisis Management Group (CMG) may be established adding another range of communication needs to manage the strategic level of response. RU and IM organisations may vary in how the crisis communication needs identified in this section are applied.

4.2 Crisis Communication Framework (CCF) objectives

When a crisis occurs and rail business is disrupted the key railway organisations, the RU and IM, should communicate both with each other, to ensure a coordinated response, and with a broad range of potential audiences as outlined in Figure 27. Communications are both internal and external to the industry, the internal communications importantly supporting and informing the external crisis communications.

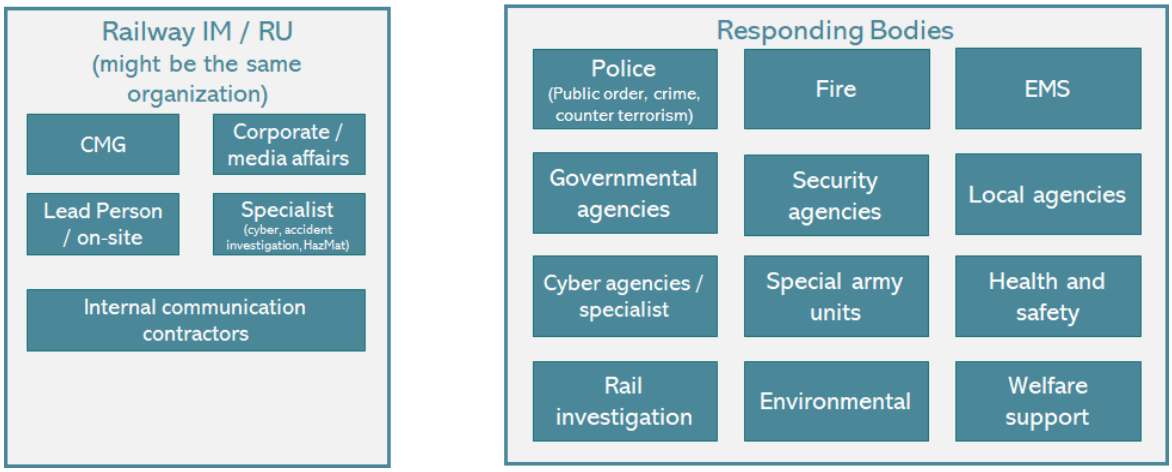

FIGURE 27: CRISIS COMMUNICATION AUDIENCE – INTERNALS AND EXTERNALS

The RU and IM will both need to identify how information of a sensitive nature is communicated appropriately (see Section 4.5) e.g., personal information of those involved in an incident – passengers, intending passengers and employees, details relating to the potential cause of the incident and freight traffics being carried.

4.3 Crisis communication strategy

RUs and IMs should prepare a crisis communication strategy (a plan) that enables them to respond promptly, accurately and with confidence: from reacting when an incident occurs to managing a strategy through to the incident conclusion. This strategy should be consistent with the Ethical Compliance Framework set out in D9.1 and in Section 3 of this document. Such a plan will form part of the overall RU and IM incident response plans. More details of incident and crisis management plan preparation and maintenance are given in D3.5 “An Incident and Crisis management Tool to Coordinate the Response to and Recovery from Railway Incidents”.

Key issues in preparing a communication strategy are:

- How the crisis communication strategy will be initiated, executed and by whom. This should include a pre-defined time window for implementation.
- Identification of the audiences that need to be reached as outlined in Section 4.2 and Figure 27. These include passengers and intending passengers, key RU & IM managers and personnel available 24/7, government and other external agencies.
- Identification, for each audience, of contact information that is regularly updated, kept securely and available to authorised users e.g. OCCs and CMG.
- Communication with employees, including those who may be involved in an incident involving death or serious injury where the sensitive nature requires close coordination between company management, the company spokesperson and public agencies such the police and health services.
- Identification of a trained lead public relations manager for the IM and RU to ensure one informed voice. A crisis may well produce a large number of requests for information, interviews and public statements and requires a policy that only authorised spokespersons are permitted to speak to news media to ensure one message.
- Identification of alternative routes in case of evacuation and threshold criteria to shut down the entire network (e.g.: in a large scale event).
- The need to co-ordinate the release of information given that initial information about the incident and its potential impact may be limited and that the 'picture' may change as more information becomes available. A consistent core message is also important with added information for particular audiences. This is helped by the preparation of pre-scripted messages targeted at the specific needs of each audience as writing messages during an incident can be challenging. These are likely to relate more to the potential impact/s of an incident. See also Section 4.5 relating to sensitive information.
- Co-ordination of off- and on-site public statements with the responding bodies, including the following:
    - Police
    - Fire
    - Emergency Medical Services (EMS)
    - Other agencies

When established the CMG undertakes a rail industry coordinating role to ensure a commonly applied strategy in response to the circumstances faced. In so doing it has a key communications role in the crisis communications strategy. In determining and overseeing the application of the crisis response strategy the CMG necessarily interfaces and communicates with a wide range of internal and external organisations as shown in Figure 28, taken from deliverable D3.5.

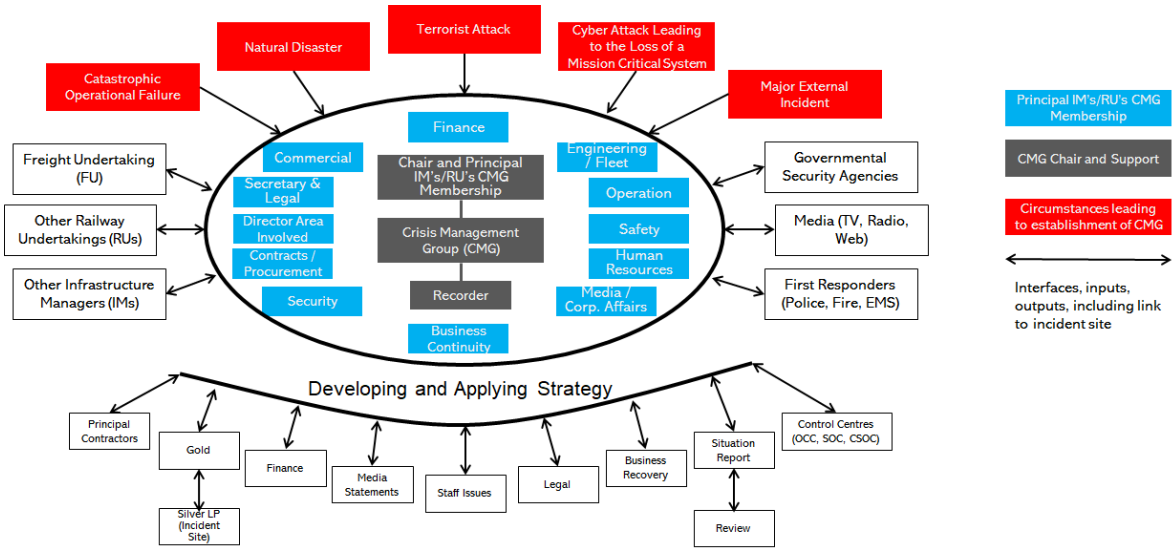

FIGURE 28: CRISIS MANAGEMENT GROUP (CMG) ROLES AND INTERFACES

4.4 Identification of information streams and communication channels

The various information streams involved are summarized in in Figure 29 below.

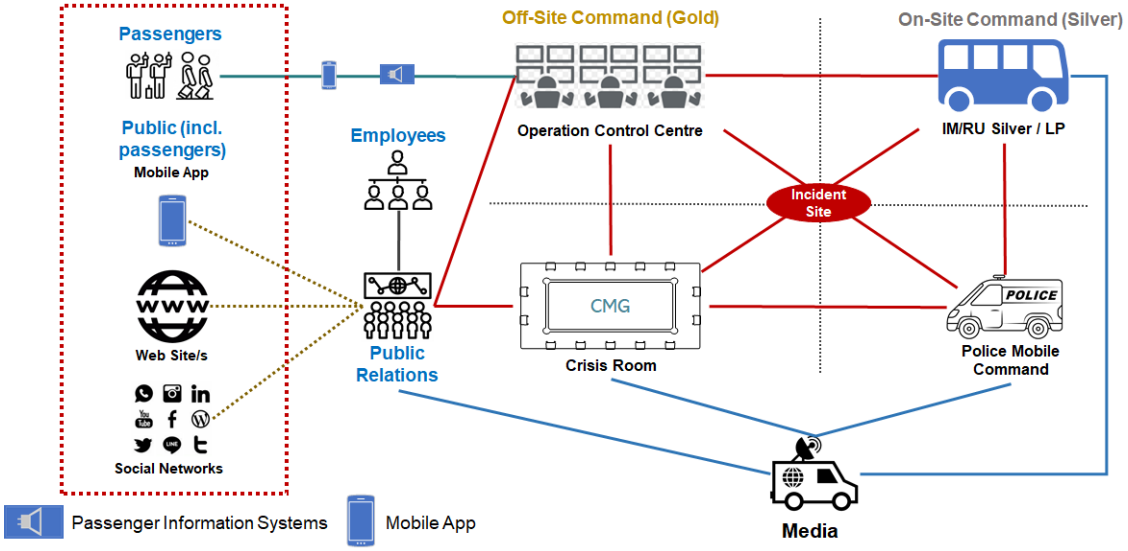

FIGURE 29: INFORMATION STREAMS AND CHANNELS DURING INCIDENT AND CRISIS

4.5 Information streams between RU, IM also responding organisations

These information streams are based on landline and mobile phones, trunked radio (e.g. TETRA, GSM-R, LTE-R, MCPTT, etc.) and data communication (not part of the public CCF).

For the RU these information streams are primarily interfaces with train crew as well as rolling stock providers and maintainers to deal with train defects and recovery. The RU will also be involved on site with the IM Lead Person and off site with the CMG if established.

The IM as infrastructure provider and maintainer, with overall control of train operations and co-ordinating the rail industry on site incident response management, is involved in a wide range of information streams with responding organisations. Many of these information streams are focused from the IM OCC providing the strategic response lead (unless a CMG is established taking on strategy decision making). The following IM information streams are involved:

- Fire, police and other EMS.
- On-site IM representative (Lead Person) - face to face coordination of the rail site response with the RU and liaison with on-site emergency services.
- Maintenance / recovery responders for infrastructure defects – track, structures, signalling, data links etc.
- Specialist contractors e.g. environment clean up.
- Governmental organisation on site e.g. rail accident investigators.
- Their employees (and families depending on the circumstances).
- The CMG if established.

4.5.1 Information streams with passengers and the public

These are primarily a RU responsibility

- Train crew - to inform and update passengers on the circumstances, delays and alternative travel arrangements.
- Station staff - for the management of station arrangements and station specific announcements to intending passengers.
- Intending passengers on line of route stations (unstaffed stations).
- Freight customers.
- The public.
- Their employees (and families depending on the circumstances).
- The CMG if established.

The following systems may be used to inform passengers and the public.

- Passenger related systems – Passenger Information System (PIS), Public Address System (PA)
- Mobile App for passengers
- Mass notification SMS (by push) in coordination with the responding bodies (see Section 4.7.3)
- Web site
- Social media – Facebook, Twitter, etc.

4.5.2 Information streams with the media

The RU and IM will both have information streams involving the media

- On-site communication with the media – the IM Lead Person and on-site media affairs, Police and Fire. This is subject to a RU and IM policy that only authorised persons should liaise with news media to ensure one message, also recognition that the Lead Person on site role is a demanding task.
- Off-site – CMG, media and corporate affairs

4.6 Handling sensitive information during crisis communications

Underlying the use or communication of any data relating to individuals is the need to ensure that legal and data protection compliance, as well as ethical compliance requirements are observed. When an incident occurs an effective response and care for individuals involved may, depending on the specific incident circumstances and why the information is needed, necessitate the sharing of an individual's information by the RU and IM with the police and other emergency services whilst respecting necessary privacy protection. The data subject may of course not be in a position to give consent to data sharing.

Ethical compliance considerations are detailed in Section 3 and involve the issue of preserving dignity. This aspect can be particularly challenging in the circumstances that can be faced when assisting those who are vulnerable e.g. having been directly involved in a major railway incident. Section 3 has also identified necessary crisis communication safeguards for those involved in the response to an incident.

4.6.1 Identification of sensitive information

It is essential to identify classified or sensitive information in advance, in order to determine the strategy for its handling and dissemination, if required. The identification of information as classified or sensitive will be based on whether it reveals information including in one or more of the following categories:

(1) **Adversary's modus operandi.** Classified information about the modus operandi of an adversary during a terror incident, including physical, cyber and combined cyber-physical incident.

(2) **Reveals vulnerabilities.** Information that reveals the vulnerability of the railway infrastructure and may be exploited by the adversary.

(3) Might create panic[32]. Information that may create public panic, concern or lack of confidence in using rail services.
(4) Can be easily manipulated. Information that might be manipulated by disseminators of fake information.
(5) Potentially reveals personal information. Information that reveals personal details (names, photos, videos, addresses, etc.) of those affected by the incident, including RU and IM personnel.

Table 1 below presents the categories of classified/sensitive information in crises, based on five use cases – catastrophic operational failure, natural disaster, terrorist attack, cyber attack (including combined cyber-physical) and major external incident.

TABLE 8 SENSITIVE INFORMATION MATRIX BY USE CASES

Use case (scenario)	Adversary's modus operandi	Reveals vulnerabilities	Can be easily manipulated	Might create panic	Potentially reveals personal information
Catastrophic Operational Failure			+	+	+
Natural hazard-based disaster				+	+
Terrorist attack	+	+	+	+	+
Cyber-attack (incl. combined cyber-physical)	+	+	+	+	+
Major external incident			+	+	+

4.6.2 Coordination of CMG, corporate affairs with the police and security agencies

The dissemination of classified or sensitive information during crises requires the involvement of internal or external experts, who will assist Corporate Affairs to identify and handle the dissemination of such information. This will require coordination between the CMG, Corporate Affairs, the police and the Member State's security authorities.

In principle, the RU/IM shall avoid disseminating classified or sensitive information, as this will result in negative consequences, as per the variables described in section 4.5.1. above. Therefore, the dissemination of classified or sensitive information pertaining to the Member State's police or security authorities shall be under the responsibility of these bodies.

As for the RU/IM, the classified or sensitive information shall be preserved to avoid any alteration or falsification, but **paraphrased** so that the information disseminated to the various media channels during interviews or press releases does not contain classified or sensitive details.

[32] Considering panic definition across the document as: "*A sudden feeling of great fear that cannot be controlled and prevents you from thinking clearly*"

4.7 Development and configuration of communication tools

Across the different tools that can be used for communication during and after a crisis, which are described below in detail, consistency and coherence should be kept to ensure message effectiveness and understanding.

4.7.1 Public Address (PA) and Passenger Information Systems (PIS)

The dissemination of automatic, incident-specific (crisis, for example) announcements in the PA or PIS systems requires integration and configuration of these systems, as follows:

(1) Definition and configuration of the announcements (in several languages, if required) in the PA or PIS system, which will be broadcast / displayed during a crisis.
(2) Integration, if required, to the information system supporting the handling of emergencies and crises incident.
(3) Definition of the manner in which the announcements will be disseminated – man in loop or automatically, and configuration of the location at which the announcements will be disseminated and the number of repetitions.

4.7.2 Mobile-App for passengers

An app for passengers is a very useful tool for most daily public transport users, particularly in aspects relating to service. Information can be relayed between the user (passenger) and the operational and/or maintenance entities through these apps. Threats and malfunctions can also be reported, in addition to service complaints.

In these apps, one can also define the ability to disseminate announcements – in routine these will be announcements about changes in the provision of services (such as delays), while in emergencies and crises they will comprise one or more of the following:

(1) Instructions – do's and don'ts, referring to passenger safety.
(2) Information and updates about the situation, alternative transport, contact details (phone number/s), requests for information and more.

4.7.3 Mass notification

The dissemination of mass notification location-based text messages via the cellular carriers is a highly efficient method for targeting a very large number of users in a defined geographic area. The RU/IM can achieve this capability through collaboration with the cellular carriers, in whose systems such capabilities are built in. In many cases, the police, fire services and security authorities have such capabilities by force of regulation or thanks to an existing agreement with the cellular carriers; therefore, the RU/IM can coordinate with these bodies and benefit from this capability as well.

4.7.4 Website

The RU/IM's website is a straightforward and available tool for information dissemination during a crisis. Information can be disseminated on the website using available tools, such as:

(1) Breaking news on the home page.
(2) Creating dedicated content for the dissemination of information about the crisis, on a dedicated page and via links.

4.7.5 Social media

Social networks, with Twitter and Facebook in particular, are excellent tools for disseminating real time updates of informative and actionable messages during a crisis. They can be utilised to disseminate messages such as:

(1) Informative details about the incident.
(2) Instructions – in text, video clips or combined media for the transport system users and the public, according to the strategy set by the CMG.

(3) Any information shared with traditional media, such as interviews (especially filmed reportages) and press releases, can be disseminated on these tools as well, in order to support the response strategy set by the CMG.

4.8 Training and exercises

It is important to ensure that the RU and IM crisis communication arrangements work effectively when a crisis occurs. This will only happen if the personnel with a role in the CCF are trained and the elements of the CCF are regularly tested with any identified shortcomings corrected. Examples of training and testing are:

- CMG tabletop exercises to ensure that those involved understand their role and responsibilities also that the supporting infrastructure functions as required.
- Understanding and application of personal data protection and ethical compliance considerations both in caring for those involved in an incident on or off site operational staff and rescuers, witness to the incident and victims or observers and with related communications.
- Capacity testing of passenger related systems (PIS, PA).
- Mobile App, SMS push, web site and social media – capacity testing on pre-production / testing environment.

Post incident reviews of communication arrangements during a crisis are also important – what went well and what did not.

5. SAFETY4RAILS Crisis Communication and Information Sharing Guidelines

This chapter presents the SAFETY4RAILS Crisis Communication and Information Sharing Guidelines, which comprises:

1. General Recommendations for Ethically Sustainable Crisis Communication with all involved stakeholders (internal, external and clients) during and after the crisis itself – which imply response and recovery phases in the resilience life-cycle, respectively.
2. Context-based Recommendations – based on specific crisis scenarios developed in WP8, comprising cyber-physical attacks, communications hacking and social media influence.

The guidelines are focused on internal and external communication, therefore covering the whole crisis communication framework elicited in Section 4. Their ultimate goal is to support critical infrastructure operators, railway/metro operators specifically, involved in a crisis to build specific mechanisms for an effective crisis management. Far from being exhaustive, guidelines stand as starting point for further actions. They do not provide a list of specific messages to be sent on each time step, but represent a **set of specific recommendations and support the building of partnerships with key stakeholders involved in the crisis**. Even though the specific content of the message is beyond the scope of this deliverable, a **message mapping template is provided in Annex II** to support their definition during the implementation of the crisis communication framework and guidelines.

In the process of developing the guidelines, the consortium has effectively integrated information retrieved from a comprehensive Crisis Communication State-of-the-Art review (Section 2), including end-users Crisis Communication Plans, systematic literature review, case studies review, past projects review, qualitative interviews with end-users and a final Workshop on Crisis Communication carried out online. On the other hand, the Crisis Communication Framework developed in Section 4 was also synthesised in the guideline's creation. The process is described in Figure 30.

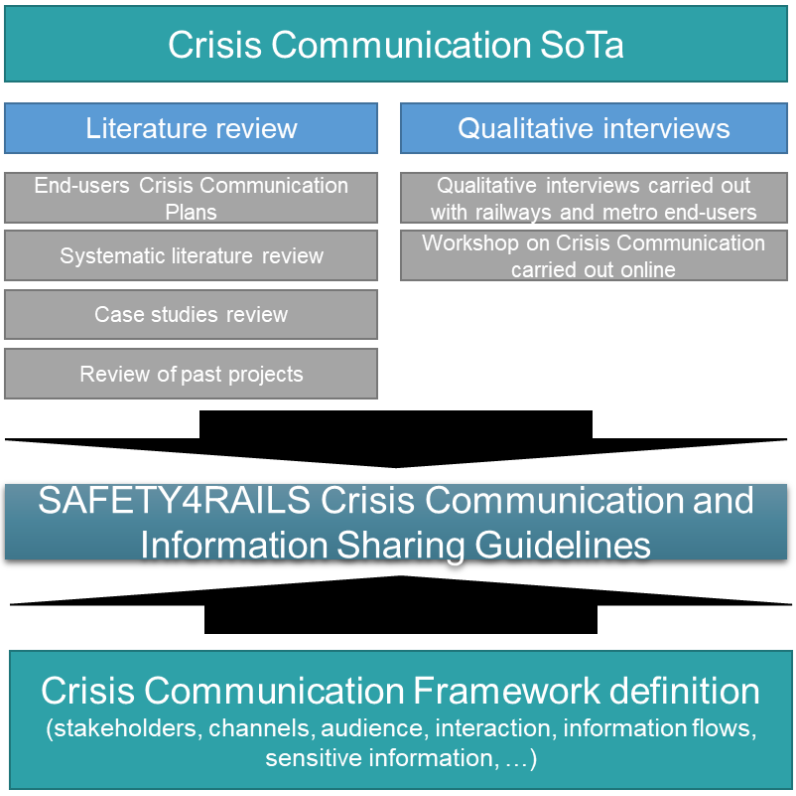

FIGURE 30 MAIN INPUTS USED FOR DEVELOPING THE GUIDELINES

5.1 Communication aspects influenced by mass media

5.1.1 Mass media as a key channel in a crisis

Mass media is a source/platform/technology that provides information to the 'masses' i.e. the majority of the general public. Mass media includes newspaper, social media, TV and radio.

5.1.2 Mass media relations: Who, what and how

Typically, an organisation's relationship with the media during a crisis is managed by its public relations and/or communication team, who serve as the organisation's 'one voice' with clear and consistent messaging.

Information shared with the media by the public relations team during a crisis usually includes an event description, public impact, actions and service restoration. When it comes to how this information is shared with the media, it is typically in the form of a press release, press interview, website and/or social media.

As to what is then reported on by the media, we can draw from this deliverable's review of media coverage of 41 past crises, which highlighted that 80% of the content is on the event description and the remaining 20% is on service restoration.

5.1.3 Managing sensitive information with the media

Across the board in this deliverable, there is consensus as to what can and cannot be shared with mass media. In particular, the following crisis information is deemed sensitive and must not be shared:

- Information that reveals personal details of those affected by the incident.
- Information that reveals the vulnerability of the railway infrastructure and may be exploited by the adversary.
- Information that may create public chaos.
- Information about the adversary's modus operandi, for example, during a terrorist incident.
- Information that might be manipulated by disseminators of fake information.
- Information revealing failures or that may embarrass the RU/IM.

There is agreement that if such information were to be inadvertently or intentionally leaked by the organisation, negative consequences would arise such as the 'hunt effect' (where people 'hunt' for a specific type of person based on information shared about the adversary), public chaos, as well as the potential for fake news.

5.1.4 Tackling fake news

This deliverable highlights that fake news (misleading and/or false information that is shared as news) should be addressed and included in a crisis communications framework, with elements such as:

- Being proactive in sharing information to ensure there is no time for fake news to be spread
- Addressing/counteracting the fake news by sharing the correct information
- Ensuring one voice (spokesperson) with the media for clear and consistent messaging
- Ensure coherence across the different channels used to communicate with stakeholders

5.1.5 Consideration of socio-cultural barriers in mass media

When sharing crisis information with mass media, organisations should also consider socio-cultural barriers, particularly in terms of language accessibility. Organisations can aim for inclusivity in press releases, press interviews, website and/or social media, through:

- **Translation of written materials in major languages.** Metro passengers should be considered in an international context, including subgroups of different languages.
- **Captioning of videos in major languages.**
- **Signs comprehension.** The interpretation of safety signs, sign language and other type of codes used in the Passenger Announcement Systems or Face-to-Face may vary from country to country. As one of the many measures to improve inclusivity, the inclusion of sign language interpreters at press interviews is recommended.

5.2 General Guidelines for ethically sustainable communication

5.2.1 Steps recommended for communication and coordination with stakeholders during a crisis

Communication during a crisis event is characterised by the following main aspects:

- It is carried out with time pressure[33].
- Passengers targeted during the communication are composed of people undergoing traumatic or stressful situations. In this condition, psychological processes are altered by the ongoing experience and cannot flow in a harmonised and effective way[33].
- Several actors need to be rapidly deployed/contacted in order to respond to the crisis, and therefore information flows should be quick and coordinated with consistent messages that can be replicated.
- Railway RU/IM should liaise with responding bodies and follow the instructions provided by governmental bodies/LEAs. Communication is in agreement and coordination with these bodies.

The general objectives of communication during a crisis have been extracted from section 2 and further discussed with the end-users participating in T9.2 to fit the scope of the guidelines:

1. **SAVING LIVES AND MINIMISING INJURIES.** At this phase, the priority is to minimise the number of casualties and people injured as a consequence of the crisis, both passengers and workers.
2. **SITUATION AND EVOLUTION UPDATING.** For effective and timely response, quick information sharing with all relevant internal and external stakeholders (passengers included) will enable coordination and further mitigation of any ongoing threat.
3. **PREPARING THE PEOPLE AND OPTIMISING EVACUATION TIME (IF THERE IS EVACUATION)**. Evacuation of those involved is a top priority during a crisis to minimise the number of casualties. Communication plays a key role to support a safe flow of passengers and protect the most vulnerable individuals.
4. **FACILITATING RESCUE OPERATIONS.** First responders are in charge of all rescue operations of victims involved in the crisis, however the RU/IM can facilitate this task through a close collaboration and information sharing.

[33] *IMPACT project. Deliverable 4.3 Cultural-based Emergency Communication guidelines. 2017.*

5. **PROMOTING COOPERATION AMONG STAKEHOLDERS**. Cooperation among all involved stakeholders, internal and external (clients included), is essential for an effective response and the Crisis Management Group (CMG) within the railway/metro operator plays a central role.
6. **PROTECTING PROPERTY AND REPUTATION**. While evacuating and protecting passengers is a top priority, the protection of the infrastructure itself through specific mitigation actions is fundamental to minimise the time of recovery. The protection of the infrastructure includes both physical and cyber domains, but also the corporate reputation which could be undermined by inaccurate or misleading communication in mass media.

For the characteristics and objectives mentioned above, the main recommendations for ethically sustainable communication during a crisis event are shown below. These recommendations have been extracted from Sections 2, 3 and 4 in the present deliverable and discussed with the end-users participating in the task:

(1) USE OFFICIAL CHANNELS ONLY: Secure established channels should be used to avoid leakage of any sensitive information. Classified/sensitive information should be encrypted.

(2a) COORDINATION AND CONSISTENCY: Make sure the communication is coordinated and consistent with all responding bodies involved in the crisis.

(2b) COORDINATION AND CONSISTENCY: Make sure that the communication with mass media is coordinated and consistent with responding bodies involved in the crisis. In particular, it should be subject to 1) Full confidentiality concerning any details of the crisis without the agreement of the police; 2) Non-disclosure of details of any external responding organisations.

(3) LIAISE WITH ON-SITE STAFF: Liaise with on-site staff, including OCC staff to communicate rapidly with the passengers affected on-site. If communications between OCC and station have been hacked, this is essential.

(4) ISSUE EFFECTIVE WARNINGS: Messages that should be timely, reliable, credible and concise, creating understanding of the crisis event but without causing alarm. This would reduce uncertainty to a minimum.

(5a) ENSURE REDUNDANCY: All warning messages should be issued via any available channel and repeated consistently over time to ensure the public take the correct actions.

(5b) ENSURE REDUNDANCY: All warning messages should be repeated consistently over time to ensure the public take the correct actions. In the case announcement systems are not available, it is recommended to allocate the necessary resources to ensure face-to-face communication is effective

(6) ADDRESS PEOPLE'S CONCERNS: Address people's (i.e. citizens and generic public) concerns with concrete answers and, if applicable, specific actions they can take.

(7) USE A MULTI-LANGUAGE APPROACH: The information to be provided should be understandable in different languages, including English, the national language and sign language.

(8) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS: Quick and efficient knowledge sharing with key personnel responsible for the affected services is fundamental to enable optimal response.

(9) MONITOR AND ANALYSE THE EFFECTIVENESS OF COMMUNICATION: The assessment should be on the basis of implementing feedback loops to optimise effectiveness.

(10) SHOW EMPATHY: Show that you care about the situation and understand what is going on. Empathy is the ability to identify with and understand somebody else's feelings or difficulties.

(11) USE VISUAL COMMUNICATION: When communicating through mass media, visual communication (infographics, videos and pictograms) are a key tool to prevent language or other functional needs barriers.

(12) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY should support and provide fast clearance for any crisis communication through mass media. Any video/audio reporting/announcement regarding the crisis must be screened to prevent the publication of any content which in any way may render a person re-identifiable, unless the person has consented to provide this information. Further details for each data subject are provided in section 3.3.

(13) PROMOTING COOPERATION among crowd members, recommending helping attitudes and collaborative behaviours within the crowd.

(14) REACH VULNERABLE AUDIENCE (e.g. visually impaired visitors, auditory limited visitors, etc.). All instructions provided during the evacuation phase should be delivered using a multi-channel and multi-language approach, with the ultimate goal of reaching all vulnerable groups affected.

(15) ACTIVELY INVOLVE RESPONDING BODIES: Responding bodies who interface with passengers, such as the police, should be involved in the crisis communication decision-making, including social-media.

(16a) BE PROACTIVE in sharing information to ensure there is no time for fake news to be spread. Use social media to provide real-time updates to citizens about the service disruption.

(16b) BE PROACTIVE: Liaise with cultural leaders and provide references to official information sources.

Regarding the use of social media, end-users explained that for **short-term crises** – such as a terrorist attack, **social media and RU/IM corporate channels** (websites, mobile apps) are preferred and recommended to communicate with the public fast and efficiently. Traditional mass media (TV, radio, magazine) is normally not recommended for short-term crisis. **For long-term crises**, when more response time is necessary to rescue victims and secure the area – such as a flood, traditional media is **recommended as an additional channel** to provide situation and evolution updates.

5.2.2 Steps recommended for communication and coordination with stakeholders after the crisis

Communication after a crisis event is characterised by the following main aspects:

- The main objective is to return affected services to normal operations, including pre-crisis passenger flow.
- Communication with passengers is mainly performed via mass media. Passengers targeted include the general public and regular passengers, who are affected by the crisis and the related business disruption, as well as victims and families who are suffering the consequences of the attack.
- Information sharing through public channels is more frequent in this phase and therefore a security/ethical scrutiny should be implemented. In such sense, RU/IM have a higher risk of lack of compliance with security/ethical standards which can affect their reputation, passengers involved and the future resilience of the infrastructure.

The general objectives of communication after a crisis have been extracted from section 2 and further discussed with the end-users participating in T9.2 to fit the scope of the guidelines:

1. **INFORM STAKEHOLDERS ABOUT THE STATUS OF THE BUSINESS DISRUPTION.** Actionable communication is required both with the passengers and all internal stakeholders involved in the

recovery of the infrastructure. From one side to minimise the concerns and help reorganise the passenger flow in the city and, on the other side to support service restoration.

2. **PROVIDE ALTERNATIVE MEANS OF TRANSPORT.** Communication with the local transport authority and alternative transport modes/operators is required to be able to deliver alternative transport services to the passengers and support the reorganisation of the passenger flow in the city.
3. **COORDINATE WITH STAKEHOLDERS THE RECOVERY OF THE INFRASTRUCTURE.** Recovery tasks are coordinated by the Operational Control Centre (OCC) who is in charge of overseeing and managing the restoration of the services, including physical and cyber infrastructure. RU/IM will be responsible of implementing the necessary countermeasures to augment the system resilience.
4. **ENHANCE PUBLIC AWARENESS OF THE INCIDENT.** Transparency, clean and clear information delivery, empathy and proactiveness are key features required to keep the clients calm, help them feel safe again in the metro infrastructure after the attack and enhance the public reputation.
5. **SUPPORT VICTIMS' RECOVERY.** First and second responders are the main responsible of helping the victims recover, e.g. find their loved ones and overcome mental health issues. However, the RU/IM can support this process by providing a dedicated hotline of information, also supporting their involved staff.

For the characteristics and objectives mentioned above, the main recommendations for ethically sustainable communication after a crisis event are shown below. These recommendations have been extracted from Sections 2, 3 and 4 in the present deliverable and discussed with the end-users participating in the task. It can be also identified that some recommendations are applicable from the phase when the crisis is ongoing, particularly recommendations (1) (2) (3) (4) (5) (6) (7) (8) (9) and (13) below.

(1) SHOW EMPATHY: Show that you care about the situation and understand what is going on. Empathy is the ability to identify with and understand somebody else's feelings or difficulties.

(2) USE A MULTI-LANGUAGE APPROACH: The information to be provided should be understandable in different languages, including English, the national language and sign language.

(3) ENSURE REDUNDANCY: All warning messages should be issued via any available channel and repeated consistently over time to ensure the public take the correct actions.

(4) USE VISUAL COMMUNICATION: When communicating through mass media, visual communication (infographics, videos and pictograms) is a key tool to prevent language or other functional needs barriers.

(5a) BE PROACTIVE in sharing information to ensure there is no time for fake news to be spread. Use social media to provide real-time updates to citizens about the service disruption.

(5b) BE PROACTIVE: Liaise with cultural leaders and provide references to official information sources.

(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY should support and provide fast clearance for any crisis communication through mass media. Any video/audio reporting/announcement regarding the crisis must be screened to prevent the publication of any content which in any way may render a person re-identifiable, unless the person has consented to provide this information. Further details for each data subject are provided in section 3.3.

(7) LIAISE WITH ON-SITE STAFF: Liaise with on-site staff, including OCC staff to communicate rapidly with the passengers affected on-site. If communications between OCC and station have been hacked, this is essential.

(8) USE OFFICIAL CHANNELS ONLY: Secure established channels should be used to avoid leakage of any sensitive information. Classified/sensitive information should be encrypted.

(9) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS: Quick and efficient knowledge sharing with key personnel responsible of the affected services is fundamental to enable optimal recovery.

(10) BE OPEN AS POSSIBLE AND CLOSED AS NECESSARY: Share only the required information with the transport authority to be able to appoint the alternative transport means and support the clients.

(11) IDENTIFY LESSONS LEARNT: Cross-disciplinary step-by-step review of the crisis and the affected services to identify weaknesses and potential countermeasures, with the goal of improving the system resilience.

(12) POST-EVENT EVALUATION of the crisis communication plan deployed to implement lessons learnt.

(13) COORDINATION AND CONSISTENCY: Make sure that the communication with mass media is coordinated and consistent with responding bodies involved in the crisis. In particular, it should be subject to: 1) Full confidentiality concerning any details of the crisis without the agreement of the police; 2) Non-disclosure of details of any external responding organisations.

(14) MAKE CLIENTS FEEL SAFE AGAIN: A general description of the security measures applied on the infrastructure and together with the responding bodies is required to help clients regain trust in the service. Information to be provided should be limited and avoid concrete details that could be used by future perpetrators.

5.3 Guidelines for ethically sustainable communication in specific scenarios

The SAFETY4RAILS Crisis Communication and Information Sharing Guidelines have been applied in this section through specific cyber-physical scenarios developed during the project. In section 5.3.1 the guidelines were applied to the context of the Metro de Madrid (MDM) Scenario, while section 5.3.2 focused on the context of the multimodal EGO&TCDD Scenario. A non-confidential version of the scenarios, taken from deliverable D6.2, including the aspects relevant to crisis communication is reported on each section.

The starting point to generate the context-based guidelines is the specific phase of the crisis (during or after a crisis). For both phases, the following 5 blocks of questions were used to collect information for their creation:

1. What do we communicate? (Objectives and sub-objectives of communication)
2. Who are the main communicators and audience? (main stakeholders involved in the communication process)
3. How do we communicate and what? (Channels used and typical information to be delivered)
4. Which communication aspects are influenced by mass media? (Ethical-Security risks to information sharing and mass media aspects to be considered)
5. How can we address communication with ethical guarantees? (General recommendations)

As mentioned above, the communication guidelines presented below could be enriched and further customized to the specific type of event under evaluation. Currently, the guidelines cover both cyber and physical events as well as multimodal effects on other transport infrastructure.

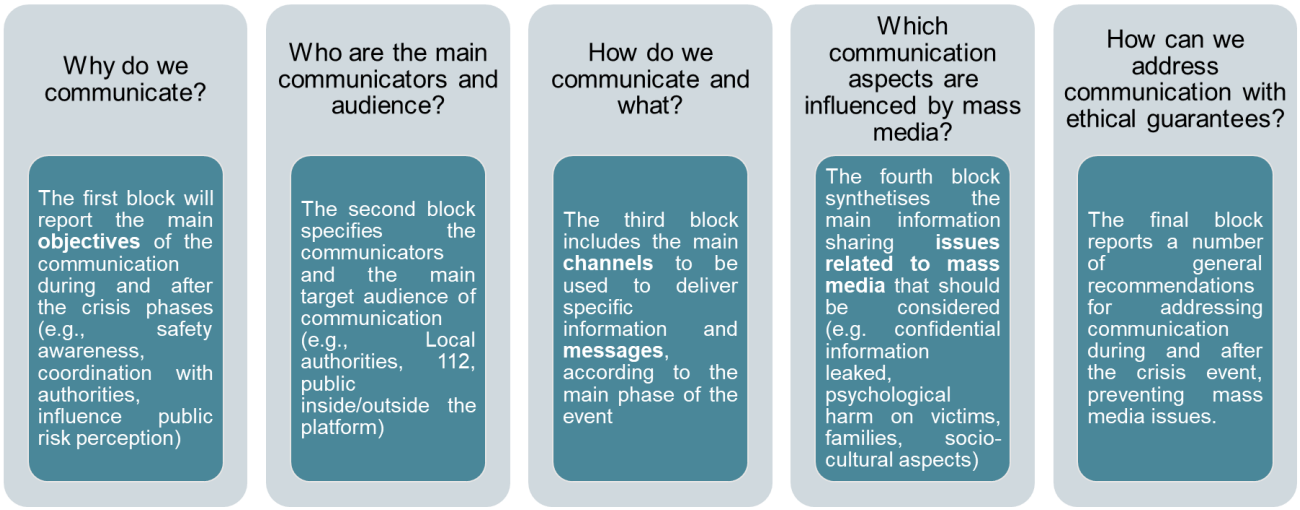

FIGURE 31 SAFETY4RAILS CRISIS COMMUNICATION GUIDELINES STRUCTURE

5.3.1 Context-based guidelines – Scenario 1

This section provides the SAFETY4RAILS Crisis Communication and Information Sharing Guidelines applied to the Metro de Madrid (MDM) Scenario:

TABLE 9 CONTEXT SCENARIO 1

Scenario: Combined cyber-physical terrorist attack on a metro station. During a mass event, an outdoor bomb explosion is used to create panic in the crowd close to a station. Right after, cyber-attack is used to block the metro service (trains) and close the station.				
ESTIMATED DAMAGE LEVEL	**ENVIRONMENTAL LAYOUT**	**INTERNAL STAKEHOLDERS INVOLVED**	**EXTERNAL STAKEHOLDERS INVOLVED**	**VULNERABLE GROUPS**
Large mass gathering event holding nearly 70,000 individuals. Service interruption would comprise the whole metro network, with 1,4 million passengers on a daily basis. 150 casualties and over 400 injured people estimated. Damage on metro infrastructure level, requiring repairs before continuation of service	Combination of events progressing from outdoors to inside the metro station. All types of individuals can be considered - students, workers, neighbours, people attending the mass gathering event, people dining at restaurants in the area. Due to the event, high media coverage is expected.	-Crisis Management Group (CMG) -Corporate/media affairs -Specialists (cyber, asset management, civil construction) -Internal communication contractors -Private Security Staff	-National and local Police -First Responders (Fire brigades, rescue team, medical emergency services) -local and National Governmental Authorities -Cyber agencies -Security agencies	-Children -Persons with reduced mobility (PRM) -Elderly -Visually impaired individuals

ID	Why do we communicate?		Who are the main communicators and audience?		How do we communicate and what?		Which communication aspects are influenced by mass media?		How can we address communication with ethical guarantees?
	Main Objectives	Sub-Objectives	Communicator	Audience	Channels	Messages	Ethical-Security risks to information sharing	Mass media considerations	General Recommendations
# 1	**SAVING LIVES AND MINIMISING INJURIES**	**#1.1.** Streamline coordination with responding bodies during interventions	Crisis Management Group (CMG) in coordination and in agreement with the RU/IM (if not in the same organisation) and the Operation Control Centre	Responding bodies: National and local governmental authorities (including also cyber agencies), National and local LEAs, fire brigades, medical emergency services and rescue teams	Landline and mobile phones, and specific data communication systems	Information to be communicated should include: 1. **Description as detailed as possible of the ongoing threat**, both in the physical and the cyber domains 2. **Risk to integrity and life of individuals**, including both passengers and workers 3. Relevant access points (compromised or not) 4. Key assets compromised 5. Probability of escalation based on available know-how	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked 4. Potentially revealing **personal information** of those involved in the incident	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** Secure established channels should be used to avoid leakage of any sensitive information. Classified/sensitive information should be encrypted. **(2a) COORDINATION AND CONSISTENCY:** Make sure the communication is coordinated and consistent with all responding bodies involved in the crisis.
		#1.2. Influencing public's risk perception and behaviour to allow a timely and effective response	Several communication flows go in parallel. Two communicators identified: 1. Operation Control Center in coordination and in agreement with CMG, Security staff on-site and	1. Public directly involved in the attack, **within the metro infrastructure** 2. Public directly involved in the attack, **outside the metro infrastructure**	**Multichannel strategy**: 1. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station 2. Face-to-	A **warning message** provides information on: **What** actions the public should take, actions to avoid and **Why** these actions are necessary. - The structure may vary according to the channel used to issue warnings - Should be **repeated at intervals**, rather	Information that might **create panic or concerns** if not delivered in the appropriate way	**Language.** Metro passengers should be considered in an international context, including subgroups of different languages **Signs**	**(3) LIAISE WITH ON-SITE STAFF:** Liaise with on-site staff, including OCC staff to communicate rapidly with the passengers affected on-site. If communications between OCC and station have been hacked, this is essential. **(4) ISSUE EFFECTIVE**

			responding bodies 2. Responding bodies: LEAs		face communication (spoken information - human direct contact), cell broadcast	than consecutively - Should **address the various audiences** within the public, e.g.: "Instructions for families"; "Instructions for vulnerable groups"; "Instructions for the general public" - The message should be different for audiences exposed to **different threats** (audience 1, and audience 2)		**comprehension.** The interpretation of safety signs, sign language and other type of codes used in the Passenger Announcement Systems or Face-to-Face may vary from country to country.	**WARNINGS:** Messages that should be timely, reliable, credible and concise, creating understanding of the crisis event but without causing alarm. This would reduce uncertainty to a minimum. **(5a) ENSURE REDUNDANCY:** All warning messages should be issued via any available channel and repeated consistently over time to ensure the public take the correct actions. **(6) ADDRESS PEOPLE'S CONCERNS:** Address people's (i.e. citizens and generic public) concerns with concrete answers and, if applicable, specific actions they can take. **(7) USE A MULTI-LANGUAGE APPROACH:** The information to be provided should be understandable in different languages, including English, the national language and sign language.

# 2	**SITUATION AND EVOLUTION UPDATING**	**#2.1.** Keep internal crisis management stakeholders informed	Crisis Management Group (CMG)	Several communication flows go in parallel: 1. Security staff on-site 2. Specialists (cyber, asset management, civil construction) 3. Corporate/media affairs 4. RU	Landline and mobile phones, and specific data communication systems	Information to be communicated should include: 1. Actionable items to respond to the crisis 2. Monitoring of the situation 3. Status updates of key assets and public opinion	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** See above **(8) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS:** Quick and efficient knowledge sharing with key personnel responsible of the affected services is fundamental to enable optimal response
		#2.2. Keep external crisis management stakeholders (responding bodies) informed	Crisis Management Group (CMG)	Several communication flows go in parallel with responding bodies: 1. LEAs 2. First responders (Fire service, rescue teams, medical emergency services) 3. Cyber agencies 4. National and local governmental authorities	Landline and mobile phones, and specific data communication systems	Information to be communicated should include: 1. **Risk to integrity and life of individuals**, including both passengers and workers 2. Key assets compromised 3. Probability of escalation based on available know-how	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked 4. Potentially revealing **personal information** of those involved in the incident	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** See above **(2a) COORDINATION AND CONSISTENCY:** See above

		#2.3. Keep clients informed about each step of the crisis	Several communication flows go in parallel. Two communicators identified: 1. Operation Control Center in coordination and in agreement with CMG, Security staff on-site and responding bodies 2. Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	1. Public (passengers) directly involved in the attack, **within the metro infrastructure** 2. General public	**Multichannel strategy:** 1. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station 2. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App	Message content should be provided with the ultimate goal of keeping the **clients calm** and **showing empathy**. Some of the information to be communicated include: 1. Disruptions on the metro transport offering/timetables 2. Stations affected to be avoided	Information that might **create panic or concerns** if not delivered in the appropriate way	**Language.** See above **Signs comprehension.** See above	**(2b) COORDINATION AND CONSISTENCY:** Make sure that the communication with mass media is coordinated and consistent with responding bodies involved in the crisis. In particular, it should be subject to: 1) Full confidentiality concerning any details of the crisis without the agreement of the police; 2) Non-disclosure of details of any external responding organisations. **(3) LIAISE WITH ON-SITE STAFF:** See above **(7) USE A MULTI-LANGUAGE APPROACH:** See above **(9) MONITOR AND ANALYSE THE EFFECTIVENESS OF COMMUNICATION**: The assessment should be the basis to implement feedback loops to optimise effectiveness. **(10) SHOW EMPATHY:** Show that you care about the situation and understand what is going on. Empathy is the ability to identify with and understand somebody else's

									feelings or difficulties. **(11) USE VISUAL COMMUNICATION:** When communicating through mass media, visual communication (infographics, videos and pictograms) are a key tool to prevent language or other functional needs barriers. **(12) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY** should support and provide fast clearance for any crisis communication through mass media. Any video/audio reporting/announcement regarding the crisis must be screened to prevent the publication of any content which in any way may render a person re-identifiable, unless the person has consented to provide this information. Further details for each data subject are provided in section 3.3

# 3	**PREPARING THE PEOPLE AND OPTIMISING EVACUATION TIME**	**#3.1.** Avoiding risky behaviours in the public directly involved (e.g. running, blocking exits, etc.)	Several communication flows go in parallel. Two communicators identified: 1. Operation Control Center in coordination and in agreement with CMG, Security staff on-site and responding bodies 2. Responding bodies: LEAs and first responders	1. Public directly involved in the attack, **within the metro infrastructure** 2. Public directly involved in the attack, **outside the metro infrastructure**	**Multichannel strategy**: 1. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station 2. Face-to-face communication (spoken information - human direct contact), cell broadcast	Message content would vary depending on the crisis and **how people are affected by this crisis**. In this case there would be 2 streams: - For audience #1, the message would be aligned with the principle "Stay calm, stay where you are" - For audience #2, the message would be aligned with the principle "Leave the place quickly but in an ordered way"	Information that might **create panic or concerns** if not delivered in the appropriate way	**Language.** See above **Signs comprehension.** See above	**(3) LIAISE WITH ON-SITE STAFF:** See above **(5a) ENSURE REDUNDANCY:** See above **(6) ADDRESS PEOPLE'S CONCERNS:** See above **(7) USE A MULTI-LANGUAGE APPROACH:** See above
		#3.2. Protect and facilitate evacuation for vulnerable groups (e.g. elderly, PRM, visually impaired passengers)	Several communication flows go in parallel. Two communicators identified: 1. Operation Control Center in coordination and in agreement with CMG, Security staff on-site and responding bodies 2. Responding bodies: LEAs and first responders	1. Vulnerable groups directly involved in the attack, **within the metro infrastructure** 2. Vulnerable groups directly involved in the attack, **outside the metro infrastructure**	**Multichannel strategy**: 1. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station 2. Face-to-face communication (spoken information - human direct contact), cell broadcast	Message content would vary depending on the crisis and **how people are affected by this crisis**, but it should reach all types of vulnerable audiences through the appropriate encoding to fit into each channel. Further, messages should facilitate the identification of vulnerable groups to enable support by security staff on-site	Information that might **create panic or concerns** if not delivered in the appropriate way	**Language.** See above **Signs comprehension.** See above	**(13) PROMOTING COOPERATION** among crowd members, recommending helping attitudes and collaborative behaviours within the crowd. **(14) REACH VULNERABLE AUDIENCE** (e.g. visually impaired visitors, auditory limited visitors, etc.). All instructions provided during the evacuation phase have to be delivered using a multi-channel and multi-language approach, with the ultimate goal

									of reaching all vulnerable groups affected.
# 4	**FACILITATING RESCUE OPERATIONS**	**#4.1.** Provide on-site information of the crisis to first responders	Crisis Management Group (CMG) in coordination and in agreement with the RU/IM (if not in the same organisation) and the Operation Control Centre	Responding bodies: LEAs, fire brigades, rescue teams and medical emergency services	Landline and mobile phones, and specific data communication systems	Information to be provided should include (if known): 1. Location of condition-critical individuals within the infrastructure 2. Location and status of assets that could hinder the rescue operations	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that **might create panic** or concerns if leaked 3. Potentially revealing **personal information** of those involved in the incident	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** See above.
# 5	**PROMOTING COOPERATION AMONG STAKEHOLDERS**	**#5.1.** Facilitate two-ways communication among communicators and audiences	Crisis Management Group (CMG)	All internal and external stakeholders, including the clients	**Multichannel strategy:** 1. Landline and mobile phones, and specific data communication systems 2. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station 3. Social media - Facebook, Twitter,	Present the crisis as a problem of the community, rather than a company problem	N/A	**Language.** See above **Signs comprehension.** See above	**(7) USE A MULTI-LANGUAGE APPROACH:** See above **(8) MONITOR AND ANALYSE THE EFFECTIVENESS OF COMMUNICATION:** See above **(12) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY:** See above **(15) ACTIVELY INVOLVE RESPONDING BODIES:** Responding bodies who interface with passengers, such as the police, should be involved in the crisis communication decision-making, including social-media.

					Corporate website and Passenger Mobile App				
# 6	**PROTECTING PROPERTY AND REPUTATION**	**#6.1.** Prevent further damage on infrastructure	Crisis Management Group (CMG) in coordination and in agreement with the RU/IM (if not in the same organisation) and the Operation Control Centre	Responding bodies: National and local governmental authorities (including also cyber agencies), National and local LEAs, fire brigades, medical emergency services and rescue teams	Landline and mobile phones, and specific data communication systems	Information to be communicated should include: 1. **Description as detailed as possible of the ongoing threat**, both in the physical and the cyber domains 2. Key assets compromised 3. Probability of escalation based on available know-how 4. Key measures adopted	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** See above **(2a) COORDINATION AND CONSISTENCY:** See above **(8) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS:** Quick and efficient knowledge sharing with key personnel responsible of the affected services is fundamental to enable optimal response
		#6.2. Ensure factual accuracy of public statements	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	General public	Social media - Facebook, Twitter, Corporate website and Passenger Mobile App	N/A	Information that might be **manipulated** by disseminators of fake information	**Language.** See above	**(5a) ENSURE REDUNDANCY:** See above **(7) USE A MULTI-LANGUAGE APPROACH:** See above **(8) MONITOR AND ANALYSE THE EFFECTIVENESS OF COMMUNICATION:** See above **(12) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY**: See above **(16a) BE PROACTIVE** in sharing information to ensure there is no time for fake news to be

									spread. Use social media to provide rea-time updates to citizens about the service disruption

COMBINED CYBER-PHYSICAL ATTACK ON A METRO STATION - SCENARIO 1- POST-EVENT PHASE									
	Why do we communicate?		Who are the main communicators and audience?		How do we communicate and what?		Which communication aspects are influenced by mass media?		How can we address communication with ethical guarantees?
ID	Main Objectives	Sub-Objectives	Communicator	Audience	Channels	Messages	Ethical-Security risks to information sharing	Mass media considerations	General Recommendations
#1	**INFORM STAKEHOLDERS ABOUT THE STATUS OF BUSINESS DISRUPTION**	**#1.1.** Keep clients informed about the expected duration and affected/closed lines, as well as access restrictions	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	General Public	**Multichannel strategy**: 1. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 2. Traditional media - TV, radio, newspapers, at **local level**	Message content should be provided with the ultimate goal of **keeping the clients calm** and **showing empathy**. Some of the information to be communicated include: 1. Expected **time of recovery** of the services affected 2. Access restrictions to specific public areas of the metro infrastructure 3. **New timetables**	1. Information that might **create panic or concerns** if not delivered in the appropriate way 2. Information that might be **manipulated** by disseminators of fake information	**Language.** Metro passengers should be considered in an international context, including subgroups of different languages. Interviews should include language interpreters. **Signs comprehension.** The interpretation of safety signs, sign language and other type of codes used in the Passenger Announcement Systems or Face-to-Face may vary from country to country. **Social media noise.** Posts that can be	**(1) SHOW EMPATHY:** Show that you care about the situation and understand what is going on. Empathy is the ability to identify with and understand somebody else's feelings or difficulties. **(2) USE A MULTI-LANGUAGE APPROACH:** The information to be provided should be understandable in different languages, including English, the national language and sign language. **(3) ENSURE REDUNDANCY:** All warning messages should be issued via any available channel and repeated consistently over time to ensure the public take the correct actions. **(4) USE VISUAL COMMUNICATION:** When communicating through mass media, visual communication (infographics, videos and pictograms) are a key tool to prevent language or other functional needs barriers. **(5a) BE PROACTIVE** in sharing information to ensure there is no time for fake news to be spread. Use social media to provide real-time updates to

								narrow, oversimplifying, misleading or false in some cases, may contribute negatively to the corporate communication through social media	citizens about the service disruption. **(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY** should support and provide fast clearance for any crisis communication through mass media. Any video/audio reporting/announcement regarding the crisis must be screened to prevent the publication of any content which in any way may render a person re-identifiable, unless the person has consented to provide this information. Further details for each data subject are provided in section 3.3
		#1.2. Keep internal stakeholders informed regarding affected services/assets	Operation Control Centre, in coordination with the CMG and RU/IM	All departments involved in the **services affected**, e.g.: operations, maintenance, security, civil construction, cybersecurity, ...	Landline and mobile phones, and specific data communication systems	Information to be communicated should include: 1. Share knowledge about key assets involved in the service disrupted 2. Monitoring of the situation and progress	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that might **create panic or concerns** if leaked	N/A	**(7) LIAISE WITH ON-SITE STAFF:** Liaise with on-site staff, including OCC staff to communicate rapidly with the passengers affected on-site. If communications between OCC and station have been hacked, this is essential. **(8) USE OFFICIAL CHANNELS ONLY:** Secure established channels should be used to avoid leakage of any sensitive information. Classified/sensitive information should be encrypted. **(9) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS:** Quick and efficient knowledge sharing with key personnel responsible of the affected services is fundamental to enable optimal recovery

# 2	**PROVIDE ALTERNATIVE MEANS OF TRANSPORT**	**#2.1.** Coordinate with local transport authorities the provision of alternative transport means, e.g.: buses	Railway undertaking (RU), if not the same organisation as the IM	Two communication flows go sequentially: 1. **Local transport authorities** at a first level to aid decision-making regarding what alternative mean is more suitable 2. **Transport operator** selected as alternative	Landline and mobile phones, and specific data communication systems	Information to be communicated at each step should include: 1. **Affected sections of each line**, expected time of recovery and required passenger capacity 2. Coordination for pick up and drop off passengers	Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM	N/A	**(8) USE OFFICIAL CHANNELS ONLY:** See above **(10a) BE OPEN AS POSSIBLE AND CLOSED AS NECESSARY:** Share only the required information with the transport authority to be able to appoint the alternative transport means and support the clients
		#2.2. Inform clients about alternative transport means	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	General Public	**Multichannel strategy**: 1. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 2. Traditional media - TV, radio, newspapers, at **local level**	Information to be shared should include: 1. **Pick up and drop off locations** for each substitutive line 2. Frequency of substitutive lines 3. Conditions (if any) to be fulfilled for its use	Information that might be **manipulated** by disseminators of fake information	**Language.** See above **Signs comprehension**. See above **Social media noise.** See above	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(3) ENSURE REDUNDANCY:** See above **(4) USE VISUAL COMMUNICATION:** See above **(5a) BE PROACTIVE**: See above **(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY**: See above

# 3	**COORDINATE WITH STAKEHOLDERS THE RECOVERY OF THE INFRASTRUCTURE**	**#3.1.** Coordinate the recovery of physical assets, e.g: repair/replacement	Operation Control Centre, in coordination and in agreement with the CMG and RU/IM	Several communication flows go in parallel: 1. Maintenance department 2. Civil Construction department 3. Security department 4. Operations	Landline and mobile phones, and specific data communication systems	Messages should be streamlined and well coordinated across all audiences involved. Information should include **status of key assets involved in the service affected**, repair/replacements activities ongoing and expected time to full recovery.	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that might **create panic or concerns** if leaked	N/A	**(8) USE OFFICIAL CHANNELS ONLY:** See above. **(9) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS:** See above
		#3.2. Coordinate the recovery of cyber assets, e.g.: remove malware from OS, unblock IoT devices	Operation Control Centre, in coordination and in agreement with the CMG and RU/IM	Several communication flows go in parallel: 1. Cybersecurity department 2. Maintenance department 3. Security department 4. Operations	Landline and mobile phones, and specific data communication systems	Messages should be streamlined and well coordinated across all audiences involved. Information should include **status of key assets involved in the service affected**, repair/replacements activities ongoing and expected time to full recovery.	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that might **create panic or concerns** if leaked	N/A	**(8) USE OFFICIAL CHANNELS ONLY:** See above. **(9) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS**: See above
		#3.3. Coordinate the implementation of new security	Operation Control Centre, in coordination and in	Several communication flows go in parallel:	1. Landline and mobile phones, and specific data	Information to be shared should include: 1. Gaps and	1. Infrastructure **vulnerabilities** that may be exploited if	N/A	**(8) USE OFFICIAL CHANNELS ONLY:** See above. **(11) IDENTIFY LESSONS LEARNT:** Cross-disciplinary step-

		countermeasures (cyber and physical) based on lessons learnt	agreement with the CMG, RU/IM and responding bodies	1. All departments involved in the **services affected**, e.g.: operations, maintenance, security, civil construction, cybersecurity, … 2. Technical providers, to implement relevant countermeasures	communication systems 2. Face-to-face communication (spoken information - human direct contact)	vulnerabilities identified in the physical/cyber domain, as well as the intersection 2. **Potential countermeasures** that could mitigate the identified vulnerabilities. When necessary, the feasibility and implementation should be discussed with the technical providers.	leaked or embarrass the RU/IM 2. Information that might **create panic or concerns** if leaked		by-step review of the crisis and the affected services to identify weaknesses and potential countermeasures, with the goal of improving the system resilience **(12) POST-EVENT EVALUATION** of the crisis communication plan deployed to implement lessons learnt
# 4	**ENHANCE PUBLIC AWARENESS OF THE INCIDENT**	**#4.1.** Facilitate two-ways communication with the clients	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	1. **Public directly involved** in the attack, within the metro infrastructure 2. General public	1. Hot line point of contact for **public involved in the attack** 2. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App	N/A	N/A	**Language.** See above **Signs comprehension.** See above **Social media noise.** See above	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(5a) BE PROACTIVE:** See above **(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY:** See above

		#4.2. Inform about the general aspects of the incident	Many communication flows go in parallel. Several communicators: 1. Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies, 2. Local governmental authorities 3. LEAs	General public	**Multichannel strategy**: 1. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 2. Traditional media - TV, radio, newspapers, at **local level**	Information to be communicated should be focused on **what the public can experience** and the content approved by the authorities in charge. Message content should be provided with the ultimate goal of showing **transparency**, **keeping the clients calm** and **showing empathy**: 1. General description of source of the attack and the consequences to the public involved and the infrastructure 2. Status of attack perpetrators 3. Status of victims	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked 4. Potentially revealing **personal information** of those involved in the incident 5. Information that might be **manipulated** by disseminators of fake information	**Language.** See above **Signs comprehension**. See above **Social media noise.** See above	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(5a) BE PROACTIVE:** See above **(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY:** See above **(13) COORDINATION AND CONSISTENCY:** Make sure that the communication with mass media is coordinated and consistent with responding bodies involved in the crisis. In particular, it should be subject to: 1) Full confidentiality concerning any details of the crisis without the agreement of the police; 2) Non-disclosure of details of any external responding organisations.
		#4.3. Inform on the general security measures applied	Two communication flows go in parallel: 1. Corporate/medi	General public	**Multichannel strategy**: 1. Social media - Facebook, Twitter,	Information to be communicated should be focused on what the public	1. Infrastructure **vulnerabilities** that may be exploited if leaked or	**Language.** See above **Signs comprehension**. See above **Social media**	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(5a) BE PROACTIVE:** See above **(6) AN INTERNAL OPERATIONAL ETHICAL**

			a affairs, in coordination and in agreement with CMG, RU/IMI and responding bodies, for security measures relevant to the **metro system** 2. Responding bodies: LEAs and governmental authorities, for security measures relevant to the **citizens security**		Corporate website and Passenger Mobile App 2. Traditional media - TV, radio, newspapers, at **local level**	can experience and the content approved by the authorities in charge. Message content should be provided with the ultimate goal of **showing transparency**, **keeping the clients calm** and making them **feel safe again in the metro**: 1. General description of the response to the crisis 2. General description of the recovery measures implemented to increase the system resilience and prevent the same attack happening twice 3. Collaboration established Metro-Authorities until full recovery	embarrass the RU/IM 2. Information that **might create panic** or concerns if leaked 3. Information that might be **manipulated** by disseminators of fake information	**noise.** See above	**AUTHORITY:** See above **(13) COORDINATION AND CONSISTENCY:** See above **(14) MAKE CLIENTS FEEL SAFE AGAIN:** A general description of the security measures applied on the infrastructure and together with the responding bodies is required to help clients regain trust in the service. Information to be provided should be limited and avoid concrete details that could be used by future perpetrators.

		#4.4. Enhance public reputation	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	General public	**Multichannel strategy**: 1. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 2. Traditional media - TV, radio, newspapers, at **local/national level**	N/A	N/A	**Language.** See above **Signs comprehension.** See above **Social media noise.** See above	**(5b) BE PROACTIVE:** Liaise with cultural leaders and provide references to official information sources **(13) COORDINATION AND CONSISTENCY:** See above **(14) MAKE CLIENTS FEEL SAFE AGAIN:** See above
# 5	**SUPPORT VICTIMS RECOVERY**	**#5.1.** Help victims find loved ones	Responding bodies: Local governmental authorities and first responders, liaising with CMG	1. Public **directly involved in the attack**, within the metro infrastructure, including relatives 2. Public **directly involved in the attack**, outside the metro infrastructure, including relatives	**Multichannel strategy:** 1. Dedicated hotline for families 2. Face-to-face communication (spoken information - human direct contact) 3. Traditional media - TV, radio, newspapers, at local level	Message content should be provided with the ultimate goal of **keeping victims calm** and **showing empathy**. Some of the information to be communicated include: 1. In which hospital the victims are been treated 2. General status of the victims	1. Information that might be **manipulated** by disseminators of fake information 2. Information that might **create panic or concerns** if leaked 3. Potentially revealing **personal information** of those involved in the incident	**Language.** See above **Signs comprehension.** See above	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(13) COORDINATION AND CONSISTENCY:** See above

		#5.2. Mental health aspects from victims, helping through recovery processes	Responding bodies: First and second responders	1. Public **directly involved in the attack**, within the metro infrastructure, including relatives 2. Public **directly involved in the attack**, outside the metro infrastructure, including relatives	1. Dedicated hot line for families 2. Face-to-face communication (spoken information - human direct contact)	N/A	N/A	N/A	-

5.3.2 Context-based guidelines – Scenario 2

This section provides the SAFETY4RAILS Crisis Communication and Information Sharing Guidelines applied to the multimodal EGO&TCDD Scenario:

TABLE 10 CONTEXT SCENARIO 2

Scenario: Combined cyber physical terrorist attack on a metro station. Communication between Operational Center and the Station is hacked and no longer reliable. Passenger Information System is hacked as well. Explosive detonation at the station. The whole situation is recorded and broadcasted through social media by the passengers in the station. Impact on timetabling in a close railway station				
ESTIMATED DAMAGE LEVEL	**ENVIRONMENTAL LAYOUT**	**INTERNAL STAKEHOLDERS INVOLVED**	**EXTERNAL STAKEHOLDERS INVOLVED**	**VULNERABLE GROUPS**
The attack happens on a station located in a business area during rush hours, holding a very high passenger flow. Service interruption would comprise the whole metro network, nearly 300,000 passengers on a daily basis. Over 50 casualties, including children, and nearly 100 people injured estimated. Timetabling of a nearby railway station will be also disrupted. Damage on metro infrastructure level, requiring repairs before continuation of service	Attack is focused on a single station, with the explosion happening in the main platform. Communication between the Operational Center and the Station are hacked. Threatening messages are sent through the PIS to the passengers. Main individuals involved would be workers who are travelling to their offices, but also students. Dissemination through social media escalates the panic and chaos, including the dissemination of fake news	-Crisis Management Group (CMG) -Corporate/media affairs -Specialists (cyber, asset management, civil construction) -Internal communication contractors -Private Security Staff	-National and local Police -First Responders (Fire brigades, rescue team, medical emergency services) -local and National Governmental Authorities -Cyber agencies -Security agencies -Railway undertaking (Railway system)	-Children -Elderly

In the table below, the issues related to the hacked communications have been reflected by ~~crossing out~~ those channels which are no longer available.

COMBINED MULTIMODAL CYBER-PHYSICAL ATTACK ON A METRO STATION WITH CASCADE EFFECTS TO A RAILWAY STATION - SCENARIO2 - EVENT PHASE									
	Why do we communicate?		Who are the main communicators and audience?		How do we communicate and what?		Which communication aspects are influenced by mass media?		How can we address communication with ethical guarantees?
ID	Main Objectives	Sub-Objectives	Communicator	Audience	Channels	Messages	Ethical-Security risks to information sharing	Mass media considerations	General Recommendations
# 1	**SAVING LIVES AND MINIMISING INJURIES**	**#1.1.** Streamline coordination with responding bodies during interventions	Crisis Management Group (CMG) in coordination and in agreement with the RU/IM (if not in the same organisation) and the Operation Control Centre	Responding bodies: National and local governmental authorities (including also cyber agencies), National and local LEAs, medical emergency services and rescue teams	Landline and mobile phones, and specific data communication systems	Information to be communicated should include: 1. **Description as detailed as possible of the ongoing threat**, both in the physical and the cyber domains 2. **Risk to integrity and life of individuals**, including both passengers and workers 3. Relevant access points (compromised or not) 4. Key assets compromised 5. Probability of escalation based on available know-how	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked 4. Potentially revealing **personal information** of those involved in the incident	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** Secure established channels should be used to avoid leakage of any sensitive information. Classified/sensitive information should be encrypted. **(2a) COORDINATION AND CONSISTENCY:** Make sure the communication is coordinated and consistent with all responding bodies involved in the crisis.

		#1.2. Influencing public's risk perception and behaviour to allow a timely and effective response	Several communication flows go in parallel. Two communicators identified: 1. Operation Control Center in coordination and in agreement with CMG, Security staff on-site and responding bodies 2. Responding bodies: LEAs	Public (passengers) directly involved in the attack	~~1. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station~~ 2. Face-to-face communication (spoken information - human direct contact), cell broadcast	A **warning message** provides information on: **What** actions the public should take, those actions to avoid and **Why** these actions are necessary. - Since only face-to-face communication is possible, **keeping the public calm and showing empathy** is essential - Should be **repeated at intervals**, rather than consecutively - Should **address the various audiences** within the public, e.g.: "Instructions for families"; "Instructions for vulnerable groups"; "Instructions for the general public"	Information that might **create panic or concerns** if not delivered in the appropriate way	**Language.** Metro passengers should be considered in an international context, including subgroups of different languages **Signs comprehension.** The interpretation of safety signs, sign language and other type of codes used in the Passenger Announcement Systems or Face-to-Face may vary from country to country.	**(3) LIAISE WITH ON-SITE STAFF:** Liaise with on-site staff, including OCC staff to communicate rapidly with the passengers affected on-site. If communications between OCC and station have been hacked, this is essential. **(4) ISSUE EFFECTIVE WARNINGS:** Messages that should be timely, reliable, credible and concise, creating understanding of the crisis event but without causing alarm. This would reduce uncertainty to a minimum. **(5b) ENSURE REDUNDANCY:** All warning messages should be repeated consistently over time to ensure the public take the correct actions. In the case announcement systems are not available, it is recommended to allocate the necessary resources to ensure face-to-face communication is effective **(6) ADDRESS PEOPLE'S CONCERNS:** Address people's (i.e. citizens and generic public)

									concerns with concrete answers and, if applicable, specific actions they can take. **(7) USE A MULTI-LANGUAGE APPROACH:** The information to be provided should be understandable in different languages, including English, the national language and sign language.
# 2	**SITUATION AND EVOLUTION UPDATING**	**#2.1.** Keep internal crisis management stakeholders informed while **mitigating the effects of the hijacked communications** in the station	Crisis Management Group (CMG)	Several communication flows go in parallel: 1. Security staff on-site 2. Specialists (cyber, asset management, communications, civil construction) 3. Corporate/media affairs 4. RU	1. Critical communications, such as TETRA to communicate **with the station** 2. Landline and mobile phones, and specific data communication systems **for the rest**	Information to be communicated should include: 1. Actionable items to respond to the crisis 2. Monitoring of the situation 3. Status updates of key assets and public opinion 4. Possible **countermeasures to regain communications**	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** See above **(8) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS:** Quick and efficient knowledge sharing with key personnel responsible of the affected services is fundamental to enable optimal response

		#2.2. Keep external crisis management stakeholders (responding bodies and railway infrastructure) informed	Crisis Management Group (CMG)	Several communication flows go in parallel with responding bodies: 1. LEAs 2. First responders (Fire service, rescue teams, medical emergency services) 3. Cyber agencies 4. National and local governmental authorities **5. Connected railway infrastructure**	Landline and mobile phones, and specific data communication systems	Information to be communicated to **responding bodies** should include: 1. **Risk to integrity and life of individuals**, including both passengers and workers 2. Key assets compromised 3. Probability of escalation based on available know-how Information to be communicated to **connected railway infrastructure** should include: 1. Affected line and station 2. Coordinate indications for commuters 3. Possibility to send clients to the railways to reorganise the passenger flow	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked 4. Potentially revealing **personal information** of those involved in the incident	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** See above **(2a) COORDINATION AND CONSISTENCY:** See above

		#2.3. Keep clients informed about each step of the crisis	Several communication flows go in parallel. Two communicators identified: 1. Operation Control Center in coordination and in agreement with CMG, Security staff on-site and responding bodies 2. Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	1. Public (passengers) directly involved in the attack 2. General public	**Multichannel strategy:** ~~1. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station~~ 1. Face-to-face communication (spoken information - human direct contact) 2. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App	Message content should be provided with the ultimate goal of **keeping the clients calm** and **showing empathy**. Some of the information to be communicated include: 1. Disruptions on the metro transport offering/timetables 2. Stations affected to be avoided	Information that might **create panic or concerns** if not delivered in the appropriate way	**Language.** See above **Signs comprehension.** See above	**(2b) COORDINATION AND CONSISTENCY:** Make sure that the communication with mass media is coordinated and consistent with responding bodies involved in the crisis. In particular, it should be subject to: 1) Full confidentiality concerning any details of the crisis without the agreement of the police; 2) Non-disclosure of details of any external responding organisations. **(3) LIAISE WITH ON-SITE STAFF:** See above **(7) USE A MULTI-LANGUAGE APPROACH:** See above **(9) MONITOR AND ANALYSE THE EFFECTIVENESS OF COMMUNICATION**: The assessment should be the basis to implement feedback loops to optimise effectiveness. **(10) SHOW EMPATHY:** Show that you care about the situation and understand what is going on. Empathy is the ability to identify with and understand somebody else's feelings or difficulties. **(11) USE VISUAL**

									COMMUNICATION: When communicating through mass media, visual communication (infographics, videos and pictograms) are a key tool to prevent language or other functional needs barriers. **(12) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY** should support and provide fast clearance for any crisis communication through mass media. Any video/audio reporting/announcement regarding the crisis must be screened to prevent the publication of any content which in any way may render a person re-identifiable, unless the person has consented to provide this information. Further details for each data subject are provided in section 3.3

# 3	**PREPARING THE PEOPLE AND OPTIMISING EVACUATION TIME**	**#3.1.** Avoiding risky behaviours in the public directly involved (e.g. running, blocking exits, etc.)	Several communication flows go in parallel. Two communicators identified: 1. Operation Control Center in coordination and in agreement with CMG, Security staff on-site and responding bodies 2. Responding bodies: LEAs and first responders	Public directly involved in the attack	~~1. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station~~ 2. Face-to-face communication (spoken information - human direct contact), cell broadcast	Message content would vary depending on the crisis and **how people are affected by this crisis**. In this case there would be only one stream an the message would be aligned with the principle "Leave the place quickly, but in an order way"	Information that might **create panic or concerns** if not delivered in the appropriate way	**Language.** See above **Signs comprehension.** See above	**(3) LIAISE WITH ON-SITE STAFF:** See above **(5b) ENSURE REDUNDANCY:** See above **(6) ADDRESS PEOPLE'S CONCERNS:** See above **(7) USE A MULTI-LANGUAGE APPROACH:** See above
		#3.2. Protect and facilitate evacuation for vulnerable groups - children, elderly	Several communication flows go in parallel. Two communicators identified: 1. Operation Control Center in coordination and in agreement with CMG, Security staff on-site and responding bodies 2. Responding bodies: LEAs and first responders	Vulnerable groups directly involved in the attack	~~1. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station~~ 2. Face-to-face communication (spoken information - human direct contact), cell broadcast	Message content would vary depending on the crisis and **how people are affected by this crisis**, but it should reach all types of vulnerable audiences - children and elderly in this case. Further, messages should facilitate the identification of vulnerable groups to enable support by security staff on-site.	Information that might **create panic or concerns** if not delivered in the appropriate way	**Language.** See above **Signs comprehension.** See above	**(13) PROMOTING COOPERATION** among crowd members, recommending helping attitudes and collaborative behaviours within the crowd. **(14) REACH VULNERABLE AUDIENCE** (e.g. visually impaired visitors, auditory limited visitors, etc.). All instructions provided during the evacuation phase have to be delivered using a multi-channel and multi-language approach, with the ultimate goal of reaching all vulnerable groups affected.

# 4	**FACILITATING RESCUE OPERATIONS**	**#4.1.** Provide on-site information of the crisis to first responders	Crisis Management Group (CMG) in coordination and in agreement with the RU/IM (if not in the same organisation) and the Operation Control Centre	Responding bodies: LEAs, fire brigades, rescue teams and medical emergency services	1. Critical communications, such as **TETRA to communicate with the station** 2. Landline and mobile phones, and specific data communication systems **for the rest**	Information to be provided should include (if known): 1. Location of condition-critical individuals within the infrastructure 2. Location and status of assets that could hinder the rescue operations	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that **might create panic** or concerns if leaked 3. Potentially revealing **personal information** of those involved in the incident	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** See above
# 5	**PROMOTING COOPERATION AMONG STAKEHOLDERS**	**#5.1.** Facilitate two-ways communication among communicators and audiences	Crisis Management Group (CMG)	All internal and external stakeholders, including the clients	**Multichannel strategy:** 1. Landline and mobile phones, and specific data communication systems ~~2. Passenger Information System (PIS) and Passenger Address (PA) system (loudspeakers) in the station~~ 2. Critical communications, such as TETRA to communicate with the station	Present the crisis as a problem of the community, rather than a company problem	N/A	**Language.** See above **Signs comprehension.** See above	**(7) USE A MULTI-LANGUAGE APPROACH:** See above **(8) MONITOR AND ANALYSE THE EFFECTIVENESS OF COMMUNICATION:** See above **(12) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY:** See above **(15) ACTIVELY INVOLVE RESPONDING BODIES:** Responding bodies who interface with passengers, such as the police, should be involved in the crisis communication decision-making, including social-media.

					3. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 4. Face-to-face communication (spoken information - human direct contact)				
# 6	**PROTECTING PROPERTY AND REPUTATION**	**#6.1.** Prevent further damage on infrastructure	Crisis Management Group (CMG) in coordination and in agreement with the RU/IM (if not in the same organisation) and the Operation Control Centre	Responding bodies: National and local governmental authorities (including also cyber agencies), National and local LEAs, fire brigades, medical emergency services and rescue teams	1. Critical communications, such as **TETRA to communicate with the station** 2. Landline and mobile phones, and specific data communication systems **for the rest**	Information to be communicated should include: 1. **Description as detailed as possible of the ongoing threat**, both in the physical and the cyber domains 2. Key assets compromised 3. Probability of escalation based on available know-how 4. Key measures adopted	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked	N/A	**(1) USE OFFICIAL CHANNELS ONLY:** See above **(2a) COORDINATION AND CONSISTENCY:** See above **(8) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS:** Quick and efficient knowledge sharing with key personnel responsible of the affected services is fundamental to enable optimal response

		#6.2. Ensure factual accuracy of public statements	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	General public	Social media - Facebook, Twitter, Corporate website and Passenger Mobile App	N/A	Information that might be **manipulated** by disseminators of fake information	**Language.** See above	**(5b) ENSURE REDUNDANCY:** See above **(7) USE A MULTI-LANGUAGE APPROACH:** See above **(8) MONITOR AND ANALYSE THE EFFECTIVENESS OF COMMUNICATION:** See above **(12) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY**: See above **(16a) BE PROACTIVE** in sharing information to ensure there is no time for fake news to be spread. Use social media to provide rea-time updates to citizens about the service disruption
		#6.3. Counter the panic and chaos (fake news included) created by the dissemination of images from the attack	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	General public	Social media - Facebook, Twitter, Corporate website and Passenger Mobile App	Provide evidence of facts based on official sources of information	Information that might be **manipulated** by disseminators of fake information	**Language.** See above	**(2b) COORDINATION AND CONSISTENCY:** See above **(5b) ENSURE REDUNDANCY:** See above **(7) USE A MULTI-LANGUAGE APPROACH:** See above **(10) SHOW EMPATHY:** See above **(12) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY**: See above **(16b) BE PROACTIVE:** Liaise with cultural leaders and provide references to official information sources

COMBINED CYBER-PHYSICAL ATTACK ON A METRO STATION - SCENARIO 1- POST-EVENT PHASE									
	Why do we communicate?		Who are the main communicators and audience?		How do we communicate and what?		Which communication aspects are influenced by mass media?		How can we address communication with ethical guarantees?
ID	Main Objectives	Sub-Objectives	Communicator	Audience	Channels	Messages	Ethical-Security risks to information sharing	Mass media considerations	General Recommendations
#1	**INFORM STAKEHOLDERS ABOUT THE STATUS OF BUSINESS DISRUPTION**	**#1.1.** Keep clients informed about the expected duration and affected/closed lines, as well as access restrictions	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	General Public	**Multichannel strategy**: 1. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 2. Traditional media - TV, radio, newspapers, at **local level**	Message content should be provided with the ultimate goal of **keeping the clients calm** and **showing empathy**. Some of the information to be communicated include: 1. Expected **time of recovery** of the services affected 2. Access restrictions to specific public areas of the metro infrastructure 3. **New timetables**	1. Information that might **create panic or concerns** if not delivered in the appropriate way 2. Information that might be **manipulated** by disseminators of fake information	**Language.** Metro passengers should be considered in an international context, including subgroups of different languages. Interviews should include language interpreters. **Signs comprehension.** The interpretation of safety signs, sign language and other type of codes used in the Passenger Announcement Systems or Face-to-Face may vary from country to country. **Social media noise.** Posts	**(1) SHOW EMPATHY:** Show that you care about the situation and understand what is going on. Empathy is the ability to identify with and understand somebody else's feelings or difficulties. **(2) USE A MULTI-LANGUAGE APPROACH:** The information to be provided should be understandable in different languages, including English, the national language and sign language. **(3) ENSURE REDUNDANCY:** All warning messages should be issued via any available channel and repeated consistently over time to ensure the public take the correct actions. **(4) USE VISUAL COMMUNICATION:** When communicating through mass media, visual communication (infographics, videos and pictograms) are a key

									that can be narrow, oversimplifying, misleading or false in some cases, may contribute negatively to the corporate communication through social media	tool to prevent language or other functional needs barriers. **(5a) BE PROACTIVE** in sharing information to ensure there is no time for fake news to be spread. Use social media to provide real-time updates to citizens about the service disruption. **(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY** should support and provide fast clearance for any crisis communication through mass media. Any video/audio reporting/announcement regarding the crisis must be screened to prevent the publication of any content which in any way may render a person re-identifiable, unless the person has consented to provide this information. Further details for each data subject are provided in section 3.3

		#1.2. Keep internal stakeholders informed regarding affected services/assets	Operation Control Centre, in coordination with the CMG and RU/IM	All departments involved in the **services affected**, e.g.: operations, maintenance, security, civil construction, cybersecurity, ...	1. Critical communications, such as TETRA to communicate **with the station** 2. Landline and mobile phones, and specific data communication systems **for the rest**	Information to be communicated should include: 1. Share knowledge about key assets involved in the service disrupted 2. Monitoring of the situation and progress	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that might **create panic or concerns** if leaked	N/A	**(7) LIAISE WITH ON-SITE STAFF:** Liaise with on-site staff, including OCC staff to communicate rapidly with the passengers affected on-site. If communications between OCC and station have been hacked, this is essential. **(8) USE OFFICIAL CHANNELS ONLY:** Secure established channels should be used to avoid leakage of any sensitive information. Classified/sensitive information should be encrypted. **(9) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS:** Quick and efficient knowledge sharing with key personnel responsible of the affected services is fundamental to enable optimal recovery
		#1.3. Keep Railway System Operator informed regarding affected/closed lines and timetabling impact for **redirecting passengers**	Railway undertaking (RU), if not the same organisation as the IM	Railway System Operator	Landline and mobile phones, and specific data communication systems	Information to be communicated should include: 1. Affected lines that could impact the specific railway station 2. Expected time of recovery and passenger load	Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM	N/A	**(8) USE OFFICIAL CHANNELS ONLY:** See above **(10a) BE OPEN AS POSSIBLE AND CLOSED AS NECESSARY:** Share only the required information with the transport authority/transport mode to be able to appoint the alternative transport means and support the clients

# 2	**PROVIDE ALTERNATIVE MEANS OF TRANSPORT**	**#2.1.** Coordinate with local transport authorities the provision of alternative transport means, e.g.: railway, buses	Railway undertaking (RU), if not the same organisation as the IM	Two communication flows go sequentially: 1. **Local transport authorities** at a first level to aid decision-making regarding what alternative mean is more suitable 2. **Transport operator/s** selected as alternative	Landline and mobile phones, and specific data communication systems	Information to be communicated at each step should include: 1. **Affected sections of each line**, expected time of recovery and required passenger capacity 2. Coordination for pick up and drop off passengers	Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM	N/A	**(8) USE OFFICIAL CHANNELS ONLY:** See above **(10a) BE OPEN AS POSSIBLE AND CLOSED AS NECESSARY:** See above
		#2.2. Inform clients about alternative transport means	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	General Public	**Multichannel strategy**: 1. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 2. Traditional media - TV, radio, newspapers, at **local level**	Information to be shared should include: 1. **Pick up and drop off locations** for each substitutive line 2. Frequency of substitutive lines 3. Conditions (if any) to be fulfilled for its use	Information that might be **manipulated** by disseminators of fake information	**Language.** See above **Signs comprehension.** See above **Social media noise.** See above	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(3) ENSURE REDUNDANCY:** See above **(4) USE VISUAL COMMUNICATION:** See above **(5a) BE PROACTIVE**: See above **(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY**: See above

# 3	**COORDINATE WITH STAKEHOLDERS THE RECOVERY OF THE INFRASTRUCTURE**	**#3.1.** Coordinate the recovery of physical assets, e.g: repair/replacement	Operation Control Centre, in coordination and in agreement with the CMG and RU/IM	Several communication flows go in parallel: 1. Maintenance department 2. Communications department 3. Civil Construction department 4. Security department 5. Operations	1. Critical communications, such as TETRA to communicate **with the station** 2. Landline and mobile phones, and specific data communication systems **for the rest**	Messages should be streamlined and well coordinated across all audiences involved. Information should include **status of key assets involved in the service affected**, repair/replacements activities ongoing and expected time to full recovery.	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that might **create panic or concerns** if leaked	N/A	**(8) USE OFFICIAL CHANNELS ONLY:** See above. **(9) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS:** See above
		#3.2. Coordinate the recovery of cyber assets, e.g.: remove malware from OS, unblock IoT devices	Operation Control Centre, in coordination and in agreement with the CMG and RU/IM	Several communication flows go in parallel: 1. Cybersecurity department 2. Communications department 3. Maintenance department 4. Security department 5. Operations	1. Critical communications, such as TETRA to communicate **with the station** 2. Landline and mobile phones, and specific data communication systems **for the rest**	Messages should be streamlined and well-coordinated across all audiences involved. Information should include **status of key assets involved in the service affected**, repair/replacements activities ongoing and expected time to full recovery.	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that might **create panic or concerns** if leaked	N/A	**(8) USE OFFICIAL CHANNELS ONLY:** See above. **(9) MAXIMISE KEY INTERNAL PERSONNEL AWARENESS**: See above

		#3.3. Coordinate the implementation of new security countermeasures (cyber and physical) based on lessons learnt	Operation Control Centre, in coordination and in agreement with the CMG, RU/IM and responding bodies	Several communication flows go in parallel: 1. All departments involved in the **services affected**, e.g.: operations, maintenance, security, civil construction, cybersecurity, … 2. Technical providers, to implement relevant countermeasures	1. Landline and mobile phones, and specific data communication systems 2. Face-to-face communication (spoken information - human direct contact)	Information to be shared should include: 1. Gaps and vulnerabilities identified in the physical/cyber domain, as well as the intersection 2. **Potential countermeasures** that could mitigate the identified vulnerabilities. When necessary, the feasibility and implementation should be discussed with the technical providers.	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that might **create panic or concerns** if leaked	N/A	**(8) USE OFFICIAL CHANNELS ONLY:** See above. **(11) IDENTIFY LESSONS LEARNT:** Cross-disciplinary step-by-step review of the crisis and the affected services to identify weaknesses and potential countermeasures, with the goal of improving the system resilience **(12) POST-EVENT EVALUATION** of the crisis communication plan deployed to implement lessons learnt
# 4	**ENHANCE PUBLIC AWARENESS OF THE INCIDENT**	**#4.1.** Facilitate two-ways communication with the clients	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	1. **Public directly involved** in the attack, within the metro infrastructure 2. General public	1. Hot line point of contact for **public involved in the attack** 2. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App	N/A	N/A	**Language.** See above **Signs comprehension.** See above **Social media noise.** See above	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(5a) BE PROACTIVE:** See above **(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY:** See above

		#4.2. Inform about the general aspects of the incident	Many communication flows go in parallel. Several communicators: 1. Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies, 2. Local governmental authorities 3. LEAs	General public	**Multichannel strategy**: 1. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 2. Traditional media - TV, radio, newspapers, at **local level**	Information to be communicated should be focused on **what the public can experience** and the content approved by the authorities in charge. Message content should be provided with the ultimate goal of showing **transparency**, **keeping the clients calm** and **showing empathy**: 1. General description of source of the attack and the consequences to the public involved and the infrastructure 2. Status of attack perpetrators 3. Status of victims	1. **Terrorist modus operandi** both in the physical and cyber domain 2. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 3. Information that **might create panic** or concerns if leaked 4. Potentially revealing **personal information** of those involved in the incident 5. Information that might be **manipulated** by disseminators of fake information	**Language.** See above **Signs comprehension.** See above **Social media noise.** See above	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(5a) BE PROACTIVE:** See above **(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY:** See above **(13) COORDINATION AND CONSISTENCY:** Make sure that the communication with mass media is coordinated and consistent with responding bodies involved in the crisis. In particular, it should be subject to: 1) Full confidentiality concerning any details of the crisis without the agreement of the police; 2) Non-disclosure of details of any external responding organisations.
		#4.3. Inform on the general security measures applied	Two communication flows go in parallel: 1. corporate/media affairs, in coordination and in agreement with CMG, RU/IMI and responding bodies, for	General public	**Multichannel strategy**: 1. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 2. Traditional media - TV,	Information to be communicated should be focused on **what the public can experience** and the content approved by the authorities in charge. Message content should be provided with the ultimate goal of **showing**	1. Infrastructure **vulnerabilities** that may be exploited if leaked or embarrass the RU/IM 2. Information that **might create panic** or concerns if leaked 3. Information that might be **manipulated** by	**Language.** See above **Signs comprehension.** See above **Social media noise.** See above	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(5a) BE PROACTIVE:** See above **(6) AN INTERNAL OPERATIONAL ETHICAL AUTHORITY:** See above **(13) COORDINATION AND CONSISTENCY:** See above

			security measures relevant to the **metro system** 2. Responding bodies: LEAs and governmental authorities, for security measures relevant to the **citizens security**		radio, newspapers, at **local level**	**transparency**, **keeping the clients calm** and making them **feel safe again in the metro**: 1. General description of the response to the crisis 2. General description of the recovery measures implemented to increase the system resilience and prevent the same attack happening twice 3. Collaboration established Metro-Authorities until full recovery	disseminators of fake information		**(14) MAKE CLIENTS FEEL SAFE AGAIN:** A general description of the security measures applied on the infrastructure and together with the responding bodies is required to help clients regain trust in the service. Information to be provided should be limited and avoid concrete details that could be used by future perpetrators.
		#4.4. Enhance public reputation	Corporate/media affairs, in coordination and in agreement with CMG, RU/IM and responding bodies	General public	**Multichannel strategy**: 1. Social media - Facebook, Twitter, Corporate website and Passenger Mobile App 2. Traditional media - TV, radio, newspapers, at **local/national level**	N/A	N/A	**Language.** See above **Signs comprehension.** See above **Social media noise.** See above	**(5b) BE PROACTIVE:** Liaise with cultural leaders and provide references to official information sources **(13) COORDINATION AND CONSISTENCY:** See above **(14) MAKE CLIENTS FEEL SAFE AGAIN:** See above

# 5	**SUPPORT VICTIMS RECOVERY**	**#5.1.** Help victims find loved ones	Responding bodies: Local governmental authorities and first responders, liaising with CMG	Public **directly involved in the attack**	**Multichannel strategy:** 1. Dedicated hotline for families 2. Face-to-face communication (spoken information - human direct contact) 3. Traditional media - TV, radio, newspapers, at local level	Message content should be provided with the ultimate goal of **keeping victims calm** and **showing empathy**. Some of the information to be communicated include: 1. In which hospital the victims are being treated 2. General status of the victims	1. Information that might be **manipulated** by disseminators of fake information 2. Information that might **create panic or concerns** if leaked 3. Potentially revealing **personal information** of those involved in the incident	**Language.** See above **Signs comprehension.** See above	**(1) SHOW EMPATHY:** See above **(2) USE A MULTI-LANGUAGE APPROACH:** See above **(13) COORDINATION AND CONSISTENCY:** See above
		#5.2. Mental health aspects from victims, helping through recovery processes	Responding bodies: First and second responders	Public **directly involved in the attack**	1. Dedicated hot line for families 2. Face-to-face communication (spoken information - human direct contact)	N/A	N/A	N/A	-

5.4 Fulfilment of requirements

This section provides a review of the relevant user requirements to this deliverable, established in D1.4, and describes their fulfilment through the Crisis Communication Guidelines and Framework developed in this document:

TABLE 11 REQUIREMENTS FULFILLED FROM D1.4

Req. ID	Description	Fulfilled	Specific actions
UR-SM-2	Have adequate crisis management plans and support structures in place, coordinated with all potential responders, that can be quickly activated as needed and that provide a well-defined, predictable and reliable frame-work for reacting to crises that affect the transport sector. Such a frame-work should comprise different components dealing with the various challenges that the transport sector could face.	√	Covered.
UR-CC-R01	Establish contact and build partnerships with broadcast media agencies, including those linked to specific cultural groups or other recognised online communities, who may provide support for emergency communication, in case of necessity.	√	The guidelines include this as part of the crisis communication framework and provides specific recommendations for uptake.

UR-CC-R02	The crisis communication plan:
	• Adheres to regulatory frameworks:
	  • E.g., the General Data Protection Regulation requires that personal data breaches are notified to the competent national supervisory authority and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach (Articles 33 and 34)[34].
	• Identifies:
	  • communication channels used by passengers & station visitors, public risk awareness levels.
		√	The guidelines include communication with the relevant national authorities in case of cyber-attacks. It also identifies communication channels to allow the necessary public risk awareness levels.

UR-CC-R03	• Inform on behaviours to be taken in case of emergency; • Raise safety awareness: knowledge. Underline on a regular basis the importance of knowledge about safety instructions, providing a hub's safety instruction leaflet, printed and available online, addressed to all cultural groups and translated by mother-tongue professionals in as many as possible languages; be sure the instructions are to be found where related groups may easily find it.	-	The guidelines include the first action. The second action belongs to the prevention actions that could be taken for crisis communication and, therefore, this is out of the scope of this deliverable.

[34] Guidelines 01/2021 on Examples regarding Data Breach Notification Adopted on 14 January 2021. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

UR-CC-R04	• What:
	  • Brief description of the event occurring;
	  • Likely impact on the public;
	  • Behaviours to adopt and actions to take;
	  • When service will be restored/That service is restored;
	  • Additional sources of information.
	• How:
	  • Inclusive (including for PRM- Passengers with Reduced Mobility)
	  • Use text and audio (public audio announcements or pre-recorded videos) in different languages, provide graphic displays, use pictograms, write in easy-to-read formats;
	  • Repetitive;
	  • Consistent;
	  • All & multi-channel (traditional & social media);
	  • Empathy not reputation;
	  • Engaging with the public.
		√	Covered.

UR-CC-R05	• Help the passengers to find alternative ways to reach their final destination and avoid that the passenger has to be present in the station to get the right information. • The most adapted communication vector available should be used to ensure that the information provided is an official source of communication.	√	Covered.

UR-CC-R06	• Locate unreached victims;
	• Help families and groups reunite;
	  • Put in place a strategy to identify and bring together people belonging to the same groups or facilitate the recognizability of different post-event logistic areas, providing provisional signs and directions addressing all involved audiences.
	  • Inform victims about the existence of (free) post event support.
		√	Covered.

UR-CC-R07	Communicate about the measures put in place to return to normal.	√	Covered.
UR-CC-R08	• Collect all available information about the event which occurred and reflect on what worked and what could use improvement. • Update the crisis communication plan to reflect this. • Inform the public of any new security measures put in place.	√	Covered.

6. Conclusion

6.1 Summary

Deliverable D9.3 provides one of the project's Key Exploitable Results: SAFETY4RAILS Crisis Communication and Information Sharing Guidelines, which aims at supporting railway/metro operators to define their mechanisms for communication during and after a crisis.

Communication in the context of a crisis serves a large variety of stakeholders through a multitude of channels and message contexts. In such complex landscape, the management and handling of sensitive information is of paramount importance to minimise ethical-security risks such as leakage of classified information regarding adversary's modus operandi and critical infrastructure vulnerabilities, but also provoking psychological harm on victims or boosting panic creation during an ongoing crisis. The guidelines provided in this document considered key inputs (including the main concerns in this sense) from a representative sample of metro and railway end-users in Europe and beyond. Existing gaps and needs in the field were also considered to move one step forward the current state-of-the-art. Such inputs were used to materialise more than 20 actionable recommendations that can be used to enhance crisis response and recovery by means of better communication.

6.2 Future work

Regarding the application of the Guidelines beyond SAFETY4RAILS project lifespan, this could be used as a training toolkit for security personnel working at railway/metro operators to enable better communication. For such application, it could aim at improving awareness of ethical-security risks that exist in crisis communication and articulating mechanisms/methodologies to mitigate them. Based on this, the end-user could define specific messages for the objectives and sub-objectives described in Section 5. In the future, the guidelines could be expanded to cover other types of scenarios not considered in this deliverable.

For the future industrialisation of the SARIS platform, recommendations described in this deliverable could be integrated in an incident management tool to support the Crisis Management Group in their decision-making.

ANNEXES

ANNEX I. GLOSSARY AND ACRONYMS

TABLE 12 GLOSSARY AND ACRONYMS

Term	Definition/description
SOTA	State-of-the-Art
DET	Data extraction table
ANG	Anger
SAD	Sadness
REP	Reputation
CCF	Crisis Communication Framework
LEA	Law Enforcement Agency
EU	European Union
PRM	Passengers with reduced mobility
PTO	Public Transport Operator
IM	Infrastructure Manager
RU	Railway Undertaking
ERMG	European Resilience Management Guidelines
CI	Critical Infrastructure
CMT	Crisis Management Team
GDPR	General Data Protection Regulations
IT	Information Technology
PTSD	Post-traumatic stress disorder
KPI	Key Performance Indicator

TETRA	TErrestrial Trunked RAdio
CMG	Crisis Management Group
NGO	Non-governmental authority
OCC	Operation Control Centre
EMS	Emergency Medical Services
PIS	Passenger Information System
PA	Public Address System
WP	Work Package
D	Deliverable
T	Task
EGO	Elektrik-Gaz-Otobüs
MDM	Metro de Madrid

ANNEX II. Crisis Communication & Information Sharing Message Map Template

In a more detailed planning of the communication with the various stakeholders, a message map can be a powerful tool to organise ideas and set clearly what needs to be communicated. In the context of this deliverable, a message aims at providing information to the audience to perform an action during or after a crisis. In this Annex, a template is provided to the end-user in order to better define such messages. The template was inspired, and adapted, from that defined in LETSCROWD project[14].

TABLE 13 MESSAGE MAP TEMPLATE

<table>
<tr><th colspan="4">MESSAGE MAP TEMPLATE</th></tr>
<tr><td colspan="4">Please write the specific target audience identified within the guidelines in Section 5 that will be addressed</td></tr>
<tr><td colspan="4">Audience addressed:……
Information to be delivered:……</td></tr>
<tr><td colspan="4">Before framing the message for the specific audience selected, it is important to define WHAT and WHY as a minimum, and WHO, WHEN, WHERE and HOW, if possible</td></tr>
<tr><td colspan="2">REQUIRED INFO</td><td colspan="2">REQUIRED INFO</td></tr>
<tr><td>WHAT actions the specified should take</td><td>WHY these actions are necessary (description of the threat and its consequences)</td><td>WHAT actions the specified should take</td><td>WHY these actions are necessary (description of the threat and its consequences)</td></tr>
<tr><td colspan="2">OPTIONAL INFO</td><td colspan="2">OPTIONAL INFO</td></tr>
<tr><td>WHO is providing the message (source)</td><td>WHEN the stakeholder need to react (time)</td><td>WHO is providing the message (source)</td><td>WHEN the stakeholder need to react (time)</td></tr>
<tr><td>WHERE is the emergency taking place (location)</td><td>HOW the message can be delivered (channel)</td><td>WHERE is the emergency taking place (location)</td><td>HOW the message can be delivered (channel)</td></tr>
</table>

Are there any Ethical-Security risks to information sharing that should be considered?	Are there any Ethical-Security risks to information sharing that should be considered?
KEY MESSAGE 1	**KEY MESSAGE 2**

ANNEX III. Questionnaire

Introduction

This questionnaire is being carried out within the SAFETY4RAILS EU H2020 funded project. The goal of the study is to examine crisis communication towards external parties during a cyber and/or physical attack. **It is intended to be filled out by the persons responsible for crisis communication within your organisation.**

Please also consider sharing the CCF directly with the S4R project for an in-depth analysis. It will be kept confidential and, if requested, anonymous.

Crisis Communication Framework

1. Does your company have a Crisis Communication Framework (or strategy, plan, guide) (CCF)? If yes, what is the scope/main goal? of the CCF? Does it cover both malicious and non-malicious crises? Does it cover cyber, physical and cyber-physical attacks?

2. Within the CCF, are roles and responsibilities clearly defined (e.g., coordinator/team leader, spokesperson, press officer,)? If so, please provide them here.

3. With which external stakeholders do you share crisis information?
   - ☐ Traditional media (e.g., press releases, journalists, interviews)
   - ☐ Directly to the general public via self-produced media (e.g., social media such as Twitter, Facebook, directly on your own website)
   - ☐ Other transportation operators
   - ☐ Public authorities (e.g., law enforcement, firefighters)

4. What sort of crisis information is shared with the general public? More than one answer is possible.
   - ☐ Brief description of the event occurring
   - ☐ Likely impact on the public
   - ☐ Behaviours to adopt and actions to take
   - ☐ When service will be restored
   - ☐ That service is restored
   - ☐ Additional sources of information
   - ☐ Other (please specify):

5. Which means do you use for crisis communication? More than one answer is possible.
   - ☐ Press release
   - ☐ Interviews with traditional media (e.g., newspapers, broadcast, radio)
   - ☐ Social media (e.g., Twitter, Facebook, Instagram)
   - ☐ Website of company

6. Does your CCF establish guidelines for two-way communication (e.g., responding to queries on social media)?

7. Does your CCF take into account the needs of persons with reduced mobility or other types of vulnerabilities? Please describe which measures your company takes (e.g., text and audio in different languages, graphic displays, pictograms, easy-to-read formats)?

8. Do you have a joint strategy with public authorities when it comes to crisis communication?

9. How does your CCF differentiate between victims of the crisis and witnesses? Which considerations are given towards privacy issues?

10. Which information does your company consider sensitive information (e.g., that which may have a psychological impact on spectators, or which might be helpful for perpetrators)?

11. Does your company have a policy for dealing with fake news?

12. Does your company take into account the feeling of security of passengers and station visitors when communicating crisis information? How so?

13. Are there any other ethical considerations within the CCF?

14. Any other comments?

ANNEX IV. Interview Guide

Background information

1. Tell me a bit about yourself (name, company, position, in which country is your company located, etc.)

Background on the event

2. Please briefly describe the crisis event we will be talking about during our interview.
3. How did your organisation first become aware of this incident?
4. Did your organisation already have in place a Crisis Communication Framework (CCF)? How was it used?
5. What was your specific role?
6. When was your first statement issued to traditional media (press release, interviews)? Social media (e.g., Twitter)?
7. What was the content of these statements and how did they evolve overtime?
8. Did you engage in two-way communication directly with the public about the crisis (on the phone, on social media)?
9. Was any information related to the crisis deemed sensitive? If so, what was it and why was this the case?
10. In which ways did your CCF have to be adapted to fit the challenges with the crisis?
11. Which communication means (social media, radio) was most effective during this crisis and why?
12. Was fake news an element during the crisis? How do you respond to fake news?

Lessons Learned

13. Looking back, would you have done anything differently?
14. After the incident, were any changes made to the company CCF? What were they?
15. What crisis communication recommendations would you share with other transport operators based on the lessons you learned from this event?

SAFETY4RAILS

Partners:

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