SAFETY4RAILS

A Specific Crisis Management Tool

Deliverable 3.5

Lead Author: MTRS3 Solutions and Services Ltd.

Contributors: LDO, IC

Dissemination level: PU – 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.

D3.5 A Specific Crisis Management Tool		
Deliverable number:	3.5	
Version:	4.2	
Delivery date:	20/05/2022	
Dissemination level:	PU - Public	
Nature:	Report	
Main author(s)	Gilad Rafael, Paul Abbott & Yael Shazar	MTRS
Contributor(s) to main deliverable production	Claudio Porretti Uli Siebold	LDO IC
Internal reviewer(s)	Uli Siebold Artur Krukowski Laura Petersen Stephen Crabbe	IC ICOM UIC Fraunhofer
External reviewer(s)	Yves Rougier	

Document control

Version	Date	Author(s)	Change(s)
0.1	8.06.21	Gilad Rafaeli, Paul Abbott & Yael Shazar	Deliverable headings and content brief
0.2	30.06.21	Gilad Rafaeli, Paul Abbott & Yael Shazar	First draft for internal review
0.3	21.07.21	Paul Abbott	Internal draft with chapter 2 inputs
0.4	12.08.21	Gilad Rafaeli & Yael Shazar	Internal draft
0.5	26.09.21	Gilad Rafaeli & Yael Shazar	Internal draft with all missing inputs
1.0	30.09.21	Gilad Rafaeli, Paul Abbott & Yael Shazar	Final draft for SAFTY4RAILS review
2.0	26.01.22	Gilad Rafaeli, Paul Abbott & Yael Shazar	Final deliverable draft for internal review, following Curix comments
2.2	17.02.22	Gilad Rafaeli, Paul Abbott & Yael Shazar	Final deliverable for internal review
3.0	21.03.22	Gilad Rafaeli, Paul Abbott & Yael Shazar	Final deliverable draft for inputs by LDO and internal review by ICOM and UIC
4.0	1.05.22	Gilad Rafaeli, Paul Abbott & Yael Shazar	Final deliverable following MdM, Fraunhofer & UREAD review
4.1	9.05.22	Gilad Rafaeli, Paul Abbott & Yael Shazar	Final deliverable following Fraunhofer comments and IC inputs
4.2	20.05.22	Uli Siebold, Stephen Crabbe	Smaller updates to V4.1 by IC and Fraunhofer

DISCLAIMER AND COPYRIGHT

The information appearing in this document has been prepared in good faith and represents the views of the authoring organisation(s). Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authoring organisation(s) accept no statutory, contractual or other legal liability for any error or omission to the fullest extent that liability can be limited in law.

This document reflects only the view of its authoring organisation(s). Neither the Research Executive Agency, nor the European Commission are responsible for any use that may be made of the information it contains. The use of the content provided is at the sole risk of the user. The reader is encouraged to investigate whether professional advice is necessary in all situations.

ABOUT SAFETY4RAILS

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

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

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

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

TABLE OF CONTENT

List of tables

List of figures

Executive summary

This document identifies aspects that must be considered by railway undertakings and infrastructure managers when preparing response and recovery plans for the effective management of incidents and crises. These may arise from the wide range of risks resulting from natural or human causes, including those of a cyber or cyber-physical nature. Use-cases are identified to assist this process. Consideration is given to legal and organisational responsibilities, plan preparation, incident reporting and classification. On and off site incident and crisis management, in coordination with external organisations, is supported by documented architecture for an incident and crisis management tool drawing on sub systems, including the S4RIS developed within the SAFETY4RAILS project.

1. Introduction

1.1 Overview

The DoA (Description of Action) describes this deliverable as a Crisis Management Tool to coordinate the response to and recovery from railway infrastructure incidents. It is also intended to support the adoption of strategies and of actions and procedures derived from them. From a functional viewpoint, the Incident and Crisis Management Tool (ICMT) supports decision making and a coordinated, integrated, system-wide (mainline rail / metro system) response to incidents and crises.

The main objective of this document is to describe an ICMT, which can be integrated with the tools developed in Task 5.5 (e.g. Decision Support System). The ICMT supports the management and coordination of all the teams involved in the response to and recovery from a railway / metro incident or crisis. It will identify:

- An incident and crisis management tool for infrastructure managers (IMs) and other relevant stakeholders.
- The mechanism for entry of incident and crisis information into the response activities as predefined in the ICMT.
- Project-related interfaces with other SAFETY4RAILS tools.
- Interfaces with existing multimedia crisis communication tools and arrangements, as in SAFETY4RAILS project Tasks 9.2 and 10.3, to support efficient and safe incident and crisis management.

The components and functionalities of the ICMT are also identified in the interfaces with railway undertaking (RU)/IM sub systems.

1.2 Structure of the deliverable

This document includes four sections:

(1) This section identifies incident and crisis management arrangements and specific arrangements for cyber-physical incident management. Details are provided of essential considerations for the preparation of incident response plans and their implementation, when required. The arrangements for on and off site incident management are presented, including the role of a crisis management group. Consideration is also given to the management of cyber- physical incidents.

(2) Incident and Crisis Management Tool (ICMT). The structure for an ideal ICMT is described, covering operations monitoring, the identification of incidents, assessment and alerting of stakeholders, situational awareness and overall incident management, taking account of use-case scenarios, records for subsequent review, and provision of crisis management exercises.

(3) An example of an ICMT.

(4) Use-cases: This section provides a list of the various incident scenarios and circumstances potentially faced by Railway and metro system Undertakings (RUs) and Infrastructure Managers (IMs), which can be referenced to help ensure that their incident response plans and management arrangements are soundly based.

2. Incident and Crisis Management Plans – Preparation and Maintenance

2.1 Overview

This section identifies the issues that should be considered by RUs and IMs when preparing their incident response and crisis management plans and ensuring that these are updated and remain effective (subsequent references to Incident Response Plans refer to the response plans for incidents of whatever scale, including crises). Consideration is also given to specific use-cases such as safety, operational and security incidents.

A generic approach is provided for incident response management plans. The arrangements applied by individual RU/IMs will necessarily depend on legal requirements, their organisational structure, the individual roles and responsibilities of the different units/position holders as well as those of external responding organisations, such as the police.

2.1.1 Objectives and scope

This section identifies the arrangements the RU/IM should implement to prepare and maintain effective incident management response plans, to ensure that associated risks, both when incidents occur and during the response, are as low as reasonably practicable. Chapter 5 identifies the wide range of incidents and crises potentially faced by RUs and IMs. RU/IMs should have measures in place to prevent reasonably foreseeable operational and security incidents involving their operations but cannot completely prevent these from occurring. Some response requirements can be dealt with by the application of local procedures, arrangements and plans, but these must be coordinated with the overall planned requirement and with one (clearly identified) organisation in the lead. RU/IM plans should provide an effective and flexible means of managing and mitigating the risks arising from the potential impact of these incidents. Supported by use of the ICMT, the response will implement on- and off-site actions to make the incident site safe, summon assistance and initiate service recovery arrangements leading to service restoration. Examples of potential impact are loss of life and injury, physical damage, operational, social and economic disruption.

It is sensible to have only one incident response plan for each location or route. Line of route plans can be split into manageable sections. There can also be separate incident response plans for a station and the route through it, providing the content of the plans are co-ordinated.

The RU/IM incident response plans should clearly define each organisation's roles and responsibilities. The IM generally has the lead incident response management coordination responsibility for mainline railway incidents.

2.1.2 Plan preparation responsibility

The RU/IM should appoint a single person within their organisation with overall responsibility for ensuring the development and management of incident response plans. This person, subsequently identified in this document as the **Lead Planner**, may delegate plan preparation actions to others, with these responsibilities documented, e.g., in job descriptions.

It is important to liaise with the police and other authorities when preparing the incident response plans for security related issues. Therefore, it is also important to ensure the responsible person within the RU/IM has the appropriate security clearance; this will help assure an effective co-ordinated response in these circumstances.

2.1.3 Legal requirements

The Lead Planner should:

- Identify the legal roles and responsibilities of the RU/IM in providing plans for the management of incidents and crises;

- Identify and recognise the legal responsibilities of the police (federal, regional and local), Fire & Rescue Services, EMS, local authorities and other responding organisations, such as the national rail accident investigation body and environmental agencies, in RU/IM incident response plans and how these interface with the RU/IM response;
- Ensure that the legal responsibilities are understood by RU/IM staff with an incident response role.

2.1.4 Incident identification & risk classification

The Lead Planner, in liaison with RU/IM functional managers and potential external responders, should undertake risk identification and classification. This entails identifying foreseeable incidents and crises, whether a natural event or person initiated, and of whatever scale (see Chapter 5: Use-cases) and the potential risks these circumstances present to RU/IM operations. Consideration should also be given to the extent to which these risks might be increased in the following example circumstances:

- Fire involved;
- Smoke and toxic fumes in confined spaces;
- Geographical location, e.g. remote or with difficult access;
- Infrastructure problems – tunnels, deep or steep sided cuttings, on bridges or viaducts;
- Hazardous materials involved;
- Time of day, e.g. involving peak passenger flows;
- Population and features adjacent to the railway;
- Temporary activities, such as construction work.

Each incident scenario should be assigned an incident level category, as in Section 3.6.2.

Within SAFETY4RAILS, the tool SecuRail from STAM provides the functionality of risk assessment. In this incidents and their estimated risk quantities can be managed.

2.1.5 Incident plan development, implementation and maintenance

2.1.5.1 Plan development

The Lead Planner should ensure, in conjunction with RU/IM managers as appropriate, that plans:

- Are clearly identified with a unique identification number and version, distribution list, implementation date and the person responsible for their upkeep;
- Have a defined structure with clearly identified sections;
- Are subject to controlled issue, with previous issues withdrawn when a new plan is implemented;
- Are available (fully or as extracts) to all those with an identified incident response role, also to the external organisations involved.

The circumstances of a cyber or cyber-physical incident, including where these are an element of a railway incident, such as a collision, may mean that cyber issues are necessarily managed remotely from any physical incident outcome. Incident response plans and their associated management will need to take into consideration, for example, identification of what constitutes the incident site, the need for ensuring site security and the preservation of evidence. Also overall management coordination should be considered.

Within the SAFETY4RAILS tool landscape the tool RAM² from Elbit provides the possibility to automatically refer to mitigation measures and runbooks when a crisis situation (or an element of it) is identified. Those mitigation measures can be taken out of incident response plans. RAM² then will provide decision support based on incident plans (and implementations), see also below.

2.1.5.2 Plan implementation

(1) **Plan implementation.** Implementation of the incident response plan requirements will generally be the responsibility of the Operation Control Centre (OCC) / Railway Incident Management Centre (RIMC) manager using ICMT, although implementation may be automatic after a specific event, e.g., identification of cyber or cyber-physical activity with the potential to compromise safe railway operation, an item is

considered to be suspicious, or the initiation of a fire alarm automatically initiating evacuation. Initial safety responses may also be required by operational rules together with necessary advice to the OCC/RIMC.

Automated event identification is provided by real-time monitoring tools of SAFETY4RAILS, e.g CuriX (from CuriX / IC), DATA FAN (from Fraunhofer) or WINGSPARK (from WINGS) for cyber or cyber physical activity, and the identification of suspicious items, e.g., unattended luggage, is provided by Ganimede from LDO.

(2) **Liaison with external responders:** Ensuring links with external responders work as planned when required is essential. Routine operational contact should be supplemented by regular formal liaison meetings, as understanding each other's operational arrangements, risks, equipment and needs will help ensure an effective incident response. Whilst the principal audience is the Police and other first responders, the needs of local authorities, Public Transport Authorities (PTAs), other involved RUs and specialist responders such as rolling stock owners etc should not be overlooked.

(3) **Documentation of interfaces, roles and responsibilities:** Identifying and agreeing interfaces, roles and responsibilities will help ensure a clear understanding of each organisation's roles and responsibilities and minimise potential problems with incident response management. With some organisations, the response may be on a contractual basis. A documented Memorandum of Understanding (MOU), involving the RU/IM and organisations, such as the Police or other external organisations with a response role in the RU/IM incident response plan, provides a structured approach.

(4) **Staff Competence:** An effective response to incidents requires those involved to be competent in their allocated incident response plan duties. Managers should ensure that all staff are trained in the basic response to incidents, and in actions to be taken during fire alarms and security alerts, appropriate to their normal place of work.

The degree of training required to ensure staff competence to undertake their planned incident response role will depend upon the nature of the role, the complexity of the location that may be involved, and the potential circumstances. Simple plans based on obvious actions may require little formal training, while some incident response plans and the roles in certain locations may involve more extensive training. Refresher or update training of staff, particularly those with designated roles, is vital to ensure that they remain competent to fulfil their roles.

Within SAFETY4RAILS, there are several tools that provide functionalities to assess possible progressions of incidents to increase understanding of particular situations and therefore make training of staff easier. The tool iCrowd of NCSRD provides e.g. passenger flow simulations within stations to assess bottlenecks and/or to reveal guidance necessities. The tool CaEASAR allows cascading effects analysis on top level grid level to support planners in preparing an optimal selection of routes or station closing decisions in advance of a crisis. The tools SARA and BB3D allows the assessment of blast consequences for attacks with explosives in use.

2.1.5.3 Plan Maintenance

Incident response plans should be kept up to date to ensure they provide an effective and safe response to the circumstances involved. The need for making changes to plans may arise from a review of the response to actual incidents, from changes in regulations or from liaison meetings with RU/IM functions or external organisations. Exercises of plans and supporting procedures can be used to help ensure plans remain fit for purpose.

The Lead Planner should organise reviews of incident response plans as a means of checking whether they remain fit for purpose or need modification. Review meetings may be held at agreed intervals or convened urgently in response to an identified deficiency in a plan. Reviews may involve:

- Relevant RU/IM managers and staff with a planned incident response responsibility;
- Liaison with the Police and other involved organisations;
- RU/IM input to reviews organised by an external organisation, where RU/IM plans are involved.

Monitoring aspects of implementation of incident response plans can also help ensure these plans are up to date and effective. Examples of monitoring measures include maintaining an overview of the response time to an incident site of key RU/IM staff and external organisations (Police, Fire & Rescue Services, EMS), recovery times when an incident occurs, and service delays and cancellations to services following an incident.

Audits of the various resources – people and equipment – required by an incident response plan are another means of ensuring effectiveness of a plan, e.g. of the plan preparation and maintenance process, staff competence training, equipment availability, evacuation arrangements. RU/IMs should develop an audit plan identifying an appropriate frequency and scope relating to planned responses.

Within SAFETY4RAILS the tool CAMS from RMIT provides means to assess degradations of equipment and foresight of expected outages of those to optimize maintenance also in the light of plan maintenance.

Debriefs, with controlled feedback of lessons learned, in order to consider lessons learned and implications for the future, held as soon as reasonably practicable after any part of the incident response plan has been implemented, or an exercise of an incident response plan, are another means of ensuring plans are up to date.

Necessary changes to plans will need to be implemented at a speed commensurate with the implications of the deficiency of the plans. All changes need to be tracked until implemented and, where appropriate, tested by exercise.

Detailed records of plan preparation, implementation and maintenance will provide the basis for any subsequent necessary review of incident response arrangements. Original records made by RU/IM staff involved in an incident response need to be retained as a key input to any subsequent investigation of the circumstances involved.

2.2 Incident and crisis management implementation

This section identifies the arrangements that should be implemented by the RU/IM to manage an incident or crisis of whatever scale.

2.2.1 Incident reporting

The RU/IM needs to ensure that incidents are reported promptly to the OCC/RIMC, including information received from external sources. The information received from the on-site reporting entity and from any external sources is entered into the incident intake form, which is a dynamic form within the ICMT capturing all information received from the incident site. In addition, a notification of an incident may be automatically initiated by the ICMT, which identifies the response considerations and necessary actions based on the RU/IM incident response plan. The ICMT also contains a structure of incident classifications (Section 3.7.2), based on delay severity / potential, to identify and enable a response appropriate to the circumstances. Together with information provided as the incident response develops, the ICMT provides a common situational awareness for the RU/IM and other agencies with access to the ICMT to support the ongoing incident response. Accurate information is vital for an effective response.

2.2.2 Initial actions

Using the information received, the OCC/RIMC manager will check that immediate operational safety actions have been taken, then use the ICMT and incident classification to advise required individuals and organisations. The OCC/RIMC will also use the ICMT to identify necessary actions to check or take in accordance with operational safety, incident response plan requirements and location-specific actions, according to the incident type, location and scale. Implementation of the incident response management structure will follow with the appointment of an on-site RU/IM Lead Person (LP) responsible for coordinating all rail activities and liaising with external responders.

Within SAFETY4RAILS the tool collaboration between real time monitoring tools (e.g. CuriX, DATA FAN, WINGSPARK) and RAM^2 provides features to classify incidents and provide advice for mitigation actions.

When an incident involves two or more separate sites, each location will require the appointment of an LP to act in accordance with this document and coordinate as necessary with other LPs. For the rail organisations, it is generally the case that the LP on site is an IM person.

2.2.3 Incident management structure

Effective incident site management requires the actions of responding organisations to be co-ordinated both on and off site. It also requires effective on site communication between all organisations involved. An incident may involve more than one site, e.g. cyber issues involving a signalling control centre and a related train incident. Where the incident involves a Police/ Fire & Rescue Services response, overall incident response and management coordination is likely to be undertaken by one of those organisations – usually, but not always, the Police. An outer cordon will be provided, with the Fire & Rescue Services, when necessary, working within an inner cordoned area.

The OCC/RIMC and LP will work within an incident management structure aligned with that applied by the emergency services, whether or not the emergency services attend the incident. Emergency service command and control in many countries is typically based on the structure identified in FIGURE 1 below. The strategic level is located off site, e.g. for the RU/IM at the OCC/RIMC, unless a separate Crisis Management Group (CMG) is established for major incidents and takes on the Gold role supported by the OCC/RIMC.

2.2.4 Liaison

If an external (away from the incident site) Strategic Gold Coordination Group is established by the Emergency Services, the OCC/RIMC will appoint an RU/IM person to liaise with that group to represent the RU/IM needs and expectations. Support and input should be provided to the Police / Fire & Rescue Services Gold, taking account of the RU/IM strategy and priorities for restoration of services, temporary arrangements, associated risks and operational safety requirements. The RU/IM should seek to achieve a shared strategy for the earliest possible release for normal working of parts or all of the incident site.

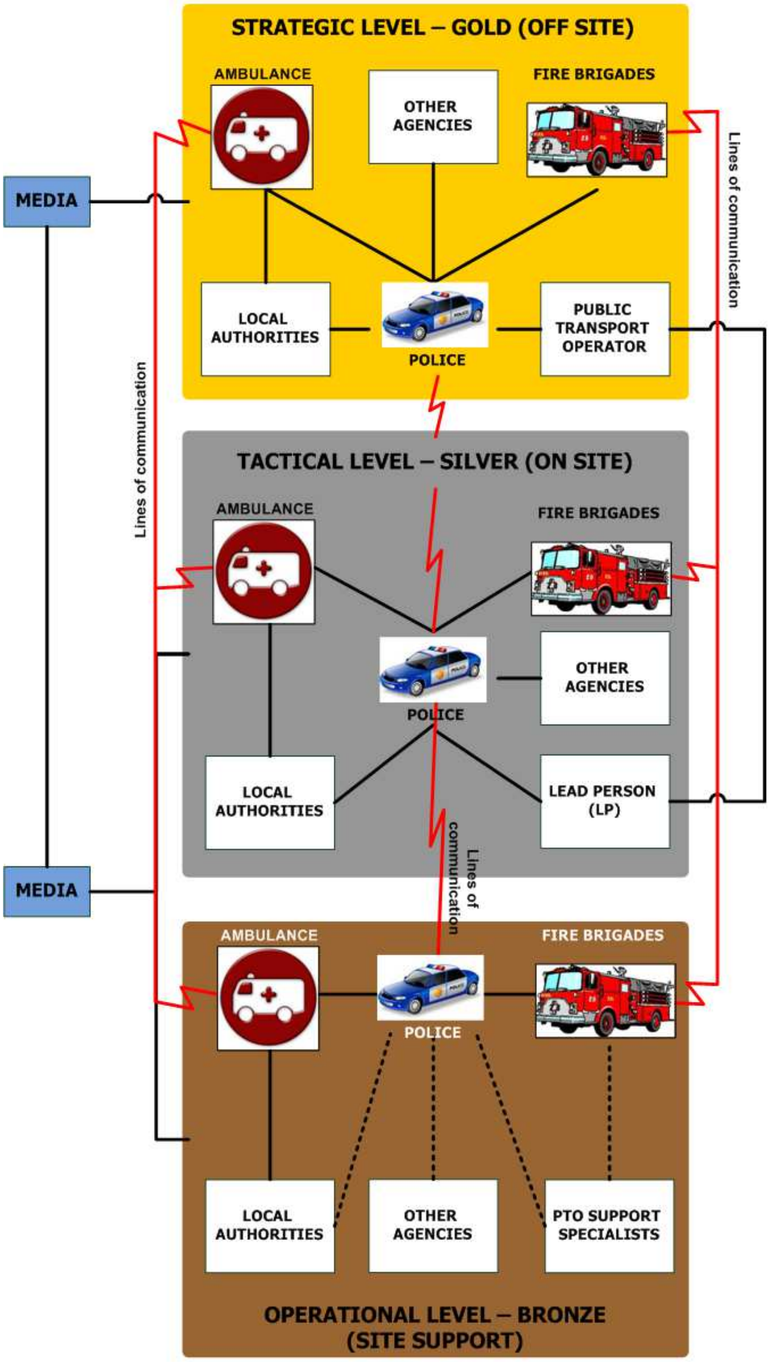


FIGURE 1: INCIDENT MANAGEMENT STRUCTURE (BASED ON POLICE IN LEAD)

2.2.5 On site response & support

The OCC/RIMC should liaise with the Lead Person (LP) on site to resolve any issues and ensure appropriate support, for example, of staff and material, to meet the strategy.

As shown in Figure 2 below, the LP is indirectly responsible for:

- Safety including cyber and cyber-physical issues
- Welfare
- Media
- Recovery
- Investigation
- Environment

- Infrastructure engineering
- Commercial customer support
- Rolling Stock operators and owners

The LP should establish a control point as the focus for RU/IM Silver and equipped according to the seriousness of the incident.

The LP should also:

- Liaise with the OCC/RIMC and, as necessary, any other appointed LPs, in setting site priorities to fulfil the overall strategy;
- Liaise with external responders, e.g. site safety, access and controls, equipment provision;
- Ensure site safety controls;
- Monitor recovery progress, coordinate operational support (Bronze) and resource requirements;
- Ensure site welfare provision;
- Maintain record of actions taken – updating the ICMT;
- Support investigation on and off site (RU/IM and/or external organisations);
- Ensure safe site restoration of operations

FIGURE 2 presents the on-site incident management structure and the wide range of IM/RU activities the on-site activities of which need to be co-ordinated by, or with the involvement of, the LP or LPs if more than one involved.

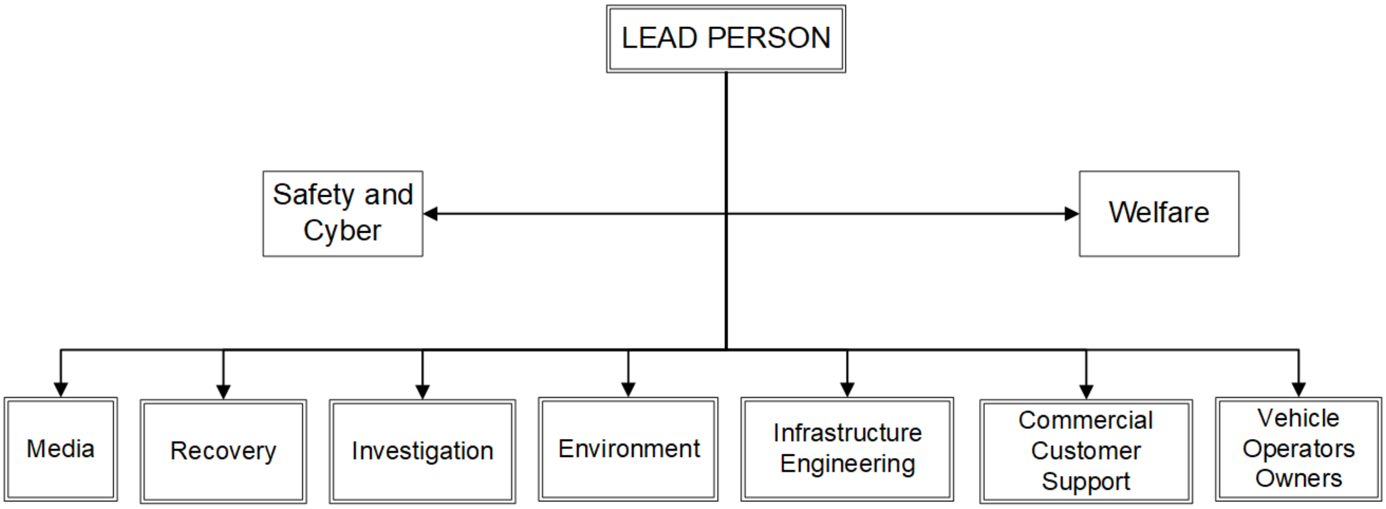


FIGURE 2: ON SITE RU/IM INCIDENT MANAGEMENT STRUCTURE

The LP is supported on site by personnel and equipment necessary to achieving an effective safe recovery, identified as Bronze. This support provides specialists on aspects such as, for example, lifting, infrastructure restoration and testing, rolling stock repairs, managing environmental impact and operational movements for service restoration.

2.2.6 Incident site considerations

This section summarises important incident response considerations, as follows:

2.2.6.1 Site Safety

An incident site and the dynamic nature of an effective incident response will present safety circumstances that need to be addressed by the LP on site, as part of the Silver coordinating role. In major incidents, the LP will need the support of a Site Safety Manager to manage site safety in coordination with external incident responders, including the emergency services and RU/IM contractors. Considerations include evacuation of passengers from the site, access and egress routes and controls, safety briefings, competency checks, use of PPE, working hours, site hazards (e.g. caused by the incident, equipment used, site utilities, organisations working together), dynamic risk assessments, method statements, fire precautions, lighting, rail operational movements).

The consideration of evacuation routes for passengers can be carried out by applying the tool iCrowd of NCSRD.

Records should be maintained and retained, of all aspects of site safety management applied during the incident response, including the retention of hard copy documents such as a work method statement.

2.2.6.2 Investigation

The saving of lives and dealing with injured persons take priority over investigation.

Various external agencies may be involved in investigating the incident cause in addition to the RU/IM, for example, the Police, the national rail incident investigation body, Health & Safety, Environment agency. The LP will liaise with these agencies to determine coordinated safe, effective site investigation arrangements and evidence collection, taking account aspects such as body and property recovery and the need to support RU/IM staff. The RU/IM may be the only organisation with the appropriate specialist capability to make a full assessment of the safety significance of evidence. The LP and/or RU/IM should record all details of evidence, including off site evidence collected or removed and by whom, also details of related discussions with external organisations.

2.2.6.3 Logistic support

An effective incident response will require the availability of a range of resources that may be needed depending on aspects such as the type and scale of incident, location, time of year, weather and the anticipated recovery time. Resources provision availability will have been considered during the incident response planning process, taking account of reasonably foreseeable incident/crisis scenarios that could affect the RU/IM operation. The RU/IM incident response plan should identify the requirements and provision timescale. Most resources will be provided by RU/IM functions or specialist contractors, with some provided by government agencies. Some RU/IM equipment may have long lead delivery times if replacement is necessary. Regular checks are necessary before a plan has to be implemented, to ensure that planned competent staff and resources, both from RU/IM sources and contractors, are available within the planned timescale. These checks should also be undertaken when incident response plans are updated.

Resources to be considered include equipment for first aid, PPE, welfare, portable and emergency lighting, crisis communication equipment, staffing (including relief) for the specialist issues potentially involved, transport, firefighting, environmental decontamination, investigation including cyber issues, construction details of rolling stock, stations, depots and other infrastructure, recovery and breakdown. For the incident response, the LP on site (Silver) should coordinate Bronze requirements, working with the other functions involved (see Figure 2), identifying when resources are needed, and liaise with the OCC/RIMC as necessary to ensure provision at a defined time – and removal when no longer required.

The LP should regularly liaise with the OCC/RIMC on resourcing issues, recording on the ICMT details of requests made, supply times and other actions.

2.2.6.4 Welfare support

Effective incident management requires the RU/IM to provide welfare support to passengers and staff involved in the actual incident, including those providing the response or potentially traumatised by the circumstances. These arrangements complement the established RU/IM systems for the workplace health and safety of their employees.

On site, the initial care of those involved may be undertaken by the emergency services with the RU/IM managing the circumstances, where passengers and staff are likely to remain on site for an extended period. The OCC/RIMC should coordinate with on-site staff and the LP to determine the welfare needs for those involved. These will depend on the circumstances, for example, the incident scale, any stranded trains and passengers, location and access, ground and weather conditions and the demand, as well as the anticipated recovery time. For a major incident or crisis, welfare needs are likely to include toilet and washing facilities, refreshments, hot and cold beverages, light and substantial meals and rest facilities – with all facilities regularly serviced.

Where passengers are involved off site, the RU/IM should make provision to care sensitively for them, working with the Police as necessary. Considerations include provision of support at hospitals for those involved and their relatives, e.g. onward transportation, home visits, letters of condolence (if approved by the management and legal advisor) and financial assistance. For legal reasons, there may be restrictions on what information the Police can release, although the RU/IM will need details of passengers and staff involved, injuries and fatalities to enable statutory incident reporting. Given that the on and off site circumstances of an incident may well involve gathering information on those involved, the need to ensure data protection is of key importance.

RU/IM staff involved in an accident – responding to an incident or simply working for an RU/IM, including their families – can be affected by what has happened and experience post-traumatic stress. The RU/IM should ensure that the wellbeing of those directly involved in an incident is assessed, with specialist support provided if appropriate. With very serious incidents, all RU/IM staff need to understand what has happened and the response being provided, with local briefings and the identification of individuals requiring a specialist response.

2.2.7 Incident conclusion - decision making

Upon the conclusion of an incident, the LP should ensure that:

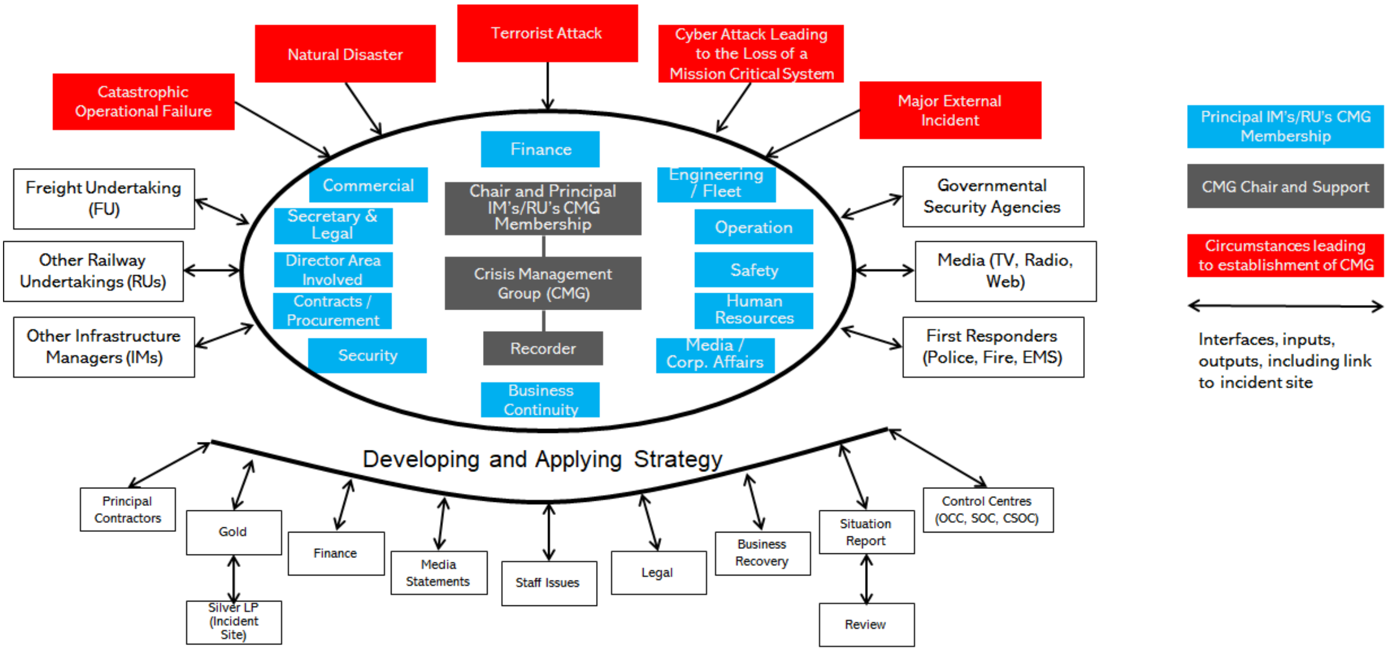
- It is safe to resume operations, either full planned service or in a planned degraded mode;
- External responders and RU/IM staff have concluded their work and they and their equipment are clear of the line;
- Site investigations are complete;
- All damage, defects and outstanding actions are recorded, identified and advised to the OCC/RIMC and LP;
- If appropriate, a hot debrief is organised to identify key issues/lessons from the incident response;
- All records of the incident and response are available, for example the LP's log, records of meetings, details external responders, site photographs, site safety, briefings, risk assessments and management, investigation records, staff interviews and report, details of injuries.

2.2.8 Crisis management

Incidents and their potential impact can vary considerably. Infrequent but serious incidents may require crisis management provided by the highest levels of an RU/IM organisation to ensure effective business continuity. These circumstances may be of such severity, for example, requiring large scale evacuation of urban areas, that they involve the implementation of plans by government agencies with the RU/IM having a supporting role. This section complements the arrangements identified in Sections 2.2.1 - 2.2.7, which may however also be required.

The OCC/RIMC will determine from the incident ranking contained in the ICMT whether the reported circumstances constitute a crisis Level 5 (see Table 2) and likely to involve circumstances beyond the management capacity of the OCC/RIMC. Having ensured that operational safety actions have been taken, the OCC/RIMC manager will determine, in conjunction with senior specified RU/IM managers, whether the reported circumstances require implementation of the CMG. The OCC/RIMC should use the ICMT to advise those identified on the incident response plan with a role in the crisis management group or need to be advised that the CMG is being established. FIGURE 3 provides an example of the key interfaces involved in a CMG, both within the RU/IM and externally, hence who is likely to be notified. Much will depend on the type and scale of the crisis faced and the required RU/IM response.

When established, the CMG should take on the RU/IM Gold strategic policy making role.



Terrorist Attack
Natural Disaster
Cyber Attack Leading to the Loss of a Mission Critical System
Catastrophic Operational Failure
Major External Incident
Finance
Commercial
Chair and Principal IM's/RU's CMG Membership
Engineering / Fleet
Secretary & Legal
Operation
Director Area Involved
Crisis Management Group (CMG)
Safety
Contracts / Procurement
Human Resources
Security
Recorder
Media / Corp. Affairs
Business Continuity
Freight Undertaking (FU)
Other Railway Undertakings (RUs)
Other Infrastructure Managers (IMs)
Governmental Security Agencies
Media (TV, Radio, Web)
First Responders (Police, Fire, EMS)
Developing and Applying Strategy
Principal Contractors
Gold
Silver LP (Incident Site)
Finance
Media Statements
Staff Issues
Legal
Business Recovery
Situation Report
Review
Control Centres (OCC, SOC, CSOC)
Principal IM's/RU's CMG Membership
CMG Chair and Support
Circumstances leading to establishment of CMG
Interfaces, inputs, outputs, including link to incident site

FIGURE 3: CRISIS MANAGEMENT GROUP – EXAMPLE OF KEY INTERFACES

2.2.9 Crisis management group (CMG) meetings

CMG meetings should be formal, with a meetings timetable, a predetermined agenda and minutes identifying actions with allocated individual responsibilities. The CMG should:

- Determine and coordinate the RU/IM strategy for response and priorities, including direction of resources to the issues faced liaising with the OCC/RIMC, and, as appropriate, with Police Gold and other external organisations;
- Ensure support for involved RU/IM staff and relatives;
- Develop the internal and external response strategy and communications, in line with the guidelines for ethically sustainable crisis communication and information sharing among stakeholders developed in Task 9.2 and, for citizens and the use of social media, Task 10.3, ensuring the issue of regular situation reports within the RU/IM organisation and externally, as appropriate;
- Enable individual CMG members to provide functional support to achieve the strategy, both on and off the crisis site;
- Review recovery response actions and progress with the disposal of outstanding actions to individuals at the conclusion of the CMG;
- Advise involved organisations when recovery actions are to be concluded;
- Organise a debrief/subsequent review of the CMG arrangements, effectiveness of decision-making and actions taken;
- Ensure that CMG logs and all records related to the CMG are retained

2.3 Cyber-physical related incidents management

2.3.1 Cyber-physical incident identification and management

When an incident is first identified or reported the full facts may well not be known including whether or not it potentially involves cyber issues or is a cyber-physical attack. In general, the response should follow the all-embracing incident and crisis management framework set out in this document. As the circumstances of an incident are clarified, the need or otherwise for specialist cyber support both in incident management and investigation (see Section 2.2.6.3 Logistic Support) can be determined and organised. Depending on the type of incident, and within the overall need to ensure a safe operation and the safety of those involved, cyber specialists may lead all or be involved in some aspects of the incident response coordinating with other RU/IM functions if a cyber-physical attack is involved. Where cyber specialists necessarily have to work with external responders or specialists, coordination must be maintained with the RU/IM response management teams working within the structure identified in this document.

From the perspective of cyber-physical incidents affecting the systems in the railway ecosystem, it is necessary to distinguish between three system types in the context of user safety:

(1) Critical railway systems, such as S&TC (signalling and traffic control) systems, the traction power supply system and fire life safety system.

(2) Operational and passenger related systems, such as PIS (passenger information system), PAS (public address system), ticketing system, security systems, BMS (building management systems) and more.

(3) Administrative / back office systems, which include all the systems that do not directly affect safety, operations, passenger and freight services, such as office systems, duty roster system, ERP (enterprise resource planning) and more.

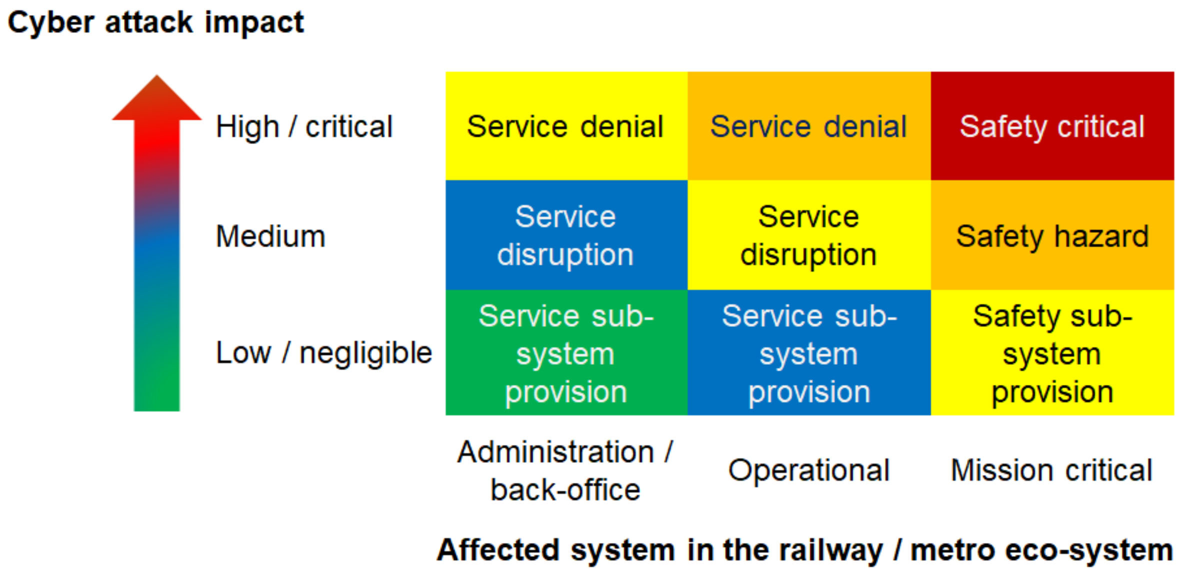
The effect of a cyber incident on these systems will be classified into three levels:

(1) Critical – depriving the system of its functionality, which may potentially cause an accident, physical damage to systems or discontinue the commercial service of the transport system.

(2) Moderate – functional disruption of the system.

(3) Low / marginal – disruption in the supply of a sub system.

FIGURE 4 illustrates the risk matrix of cyber-physical incidents in the operational and administrative railway ecosystem.



Cyber attack impact

High / critical	Service denial	Service denial	Safety critical
Medium	Service disruption	Service disruption	Safety hazard
Low / negligible	Service sub-system provision	Service sub-system provision	Safety sub-system provision
	Administration / back-office	Operational	Mission critical

Affected system in the railway / metro eco-system

FIGURE 4: CYBER-PHYSICAL RISK MATRIX

The purpose of the real-time monitoring tools within SAFETY4RAILS is to continuously monitor (i.e., retrieve data on a regular basis in types of logs and/or metric data) all three system types, mentioned above.

2.3.2 Cyber-physical incident management paradigm

When we refer to the cyber-physical incident management paradigm via the ICMT, we refer to the mission critical and operational systems in the railway ecosystem, which affect the safety of the passengers and/or freight transported on the one hand, and quality, availability and reliability of the service, on the other hand.

The cyber-physical incident management paradigm via the ICMT requires a logical connection between several command and control centres, the main ones being:

- The OCC (Operation Control Centre) – which is essential to the effective handling of cyber-physical incidents, as it is directly involved in the operation of the mission critical systems.
- The cyber SOC (Security Operation Centre) or SIEM SOC – which is essential for the monitoring of cyber incidents in networks, data and applications, with emphasis placed on mission critical systems and operational systems.
- Scheduling and incident management control centre – mainly relevant to the mainline railway operation in the context of managing schedules due to delays and overall management of incidents at the regional and/or national level.
- Assets and maintenance management control centre – an additional command and control centre, which is responsible for managing assets and maintenance for rolling stock, railway systems, safety systems, BMS, operational systems and more.

FIGURE 5 illustrates the cyber-physical incident management paradigm with the relevant control centres connected via the ICMT. The connections between the command and control centres and the system are indicated by broken lines, to signify that the connection does not require a logical interface and can be achieved by operating the system from that control centre, with a logical connection with the system workstations in other operation and maintenance control centres.

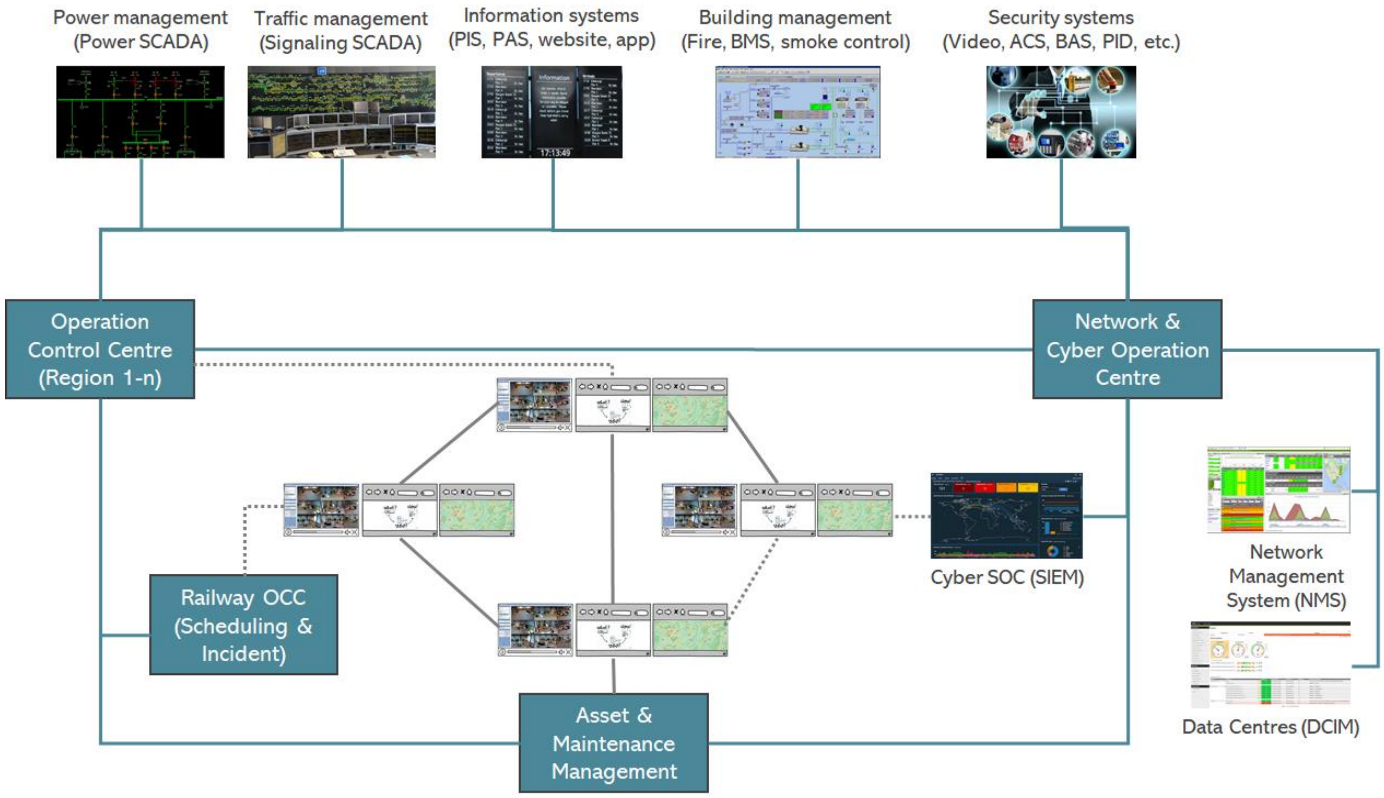

Power management
(Power SCADA)
Traffic management
(Signaling SCADA)
Information systems
(PIS, PAS, website, app)
Building management
(Fire, BMS, smoke control)
Security systems
(Video, ACS, BAS, PID, etc.)
Operation Control Centre (Region 1-n)
Network & Cyber Operation Centre
Cyber SOC (SIEM)
Network Management System (NMS)
Railway OCC (Scheduling & Incident)
Data Centres (DCIM)
Asset & Maintenance Management

FIGURE 5: CYBER-PHYSICAL INCIDENT MANAGEMENT PARADIGM

Within SAFETY4RAILS a distributed messaging system (DMS) was implemented in S4RIS to allow an easy to implement (bidirectional) connectivity between S4RIS internal tools but also to external tools or systems as mentioned above.

3. Requirements for an Incident and Crisis Management Tool (ICMT)

The ICMT concept was developed following consideration of D1.4 (Specification of the overall technical architecture) and D2.5 (Specific Requirements for Multi Modal Transport Systems) and our understanding, as subject matter experts, of the needs of potential end users and of the market. The ICMT concept described provides an ideal set of extended requirements forming a tool for crisis management, as reflected in the SC2 tool by LDO, shown in Section 4.

3.1 SAFETY4RAILS requirements pertaining to D3.5

The following table details how the ICMT addresses the requirements identified in Deliverable 1.4 (Specification on the overall technical architecture), section 2.2.9 in this deliverable. Where a section 2.2.9 requirement is not addressed here the D1.4 identifies the primary S4RIS components addressing them.

TABLE 1: SAFETY4RAILS REQUIREMENTS MATRIX – INCIDENT AND CRISIS MANAGEMENT

Nr.	Requirements	ICMT Specifications	Referenced to chapter in this document
1	UR-CM-R01 - Adequate crisis management and support structures and UR-CM-R02 - Collaboration between stakeholders	The incident and crisis management system provides a system-wide solution for real-time operational monitoring, incident management and coordination between off-site control centres (rail / metro operation, train re-scheduling, crisis management room, maintenance support, etc.) and on-site responders.	3.2.1 (Users) 3.2.2 (CONOP) 3.4.5 (Roles)
2	UR-CM-R03 - Clear definition of roles and responsibilities	The incident and crisis management system, , clearly defines the roles and responsibilities in the handling of each incident through an assignee and collaborator/s module, which define/s who is responsible for managing the incident and the relevant stakeholders.	3.4.4 (Users and operators) 3.4.5 (Roles – assignee and collaborators)
3	UR-CM-R04 - Expert knowledge – a prerequisite for being able to assess all types of incidents, including both physical and cyber/physical incidents affecting rail / metro traffic	The incident and crisis management system enables the management of a wide range of emergency and disaster incidents – operational and safety, natural disasters, terror and cyber. The system infrastructure enables subject matter experts to define business process workflows for emergency procedures, to effectively manage the scenarios potentially faced.	3.4.3 (Support throughout the incident life cycle) 5 (Use cases)
4	UR-CM-R05 - Training and exercises	The incident and crisis management system includes a training and simulation model that enables conducting an exercise for a single operator or a group of operators in control room configuration, and in a variety of emergency scenarios, while examining the decision-making processes and collaboration between the involved entities, off- and on-site.	3.13 (emergency and crisis exercise tool)

Nr.	Requirements	ICMT Specifications	Referenced to chapter in this document
5	UR-CM-R09 - Early warning systems to alert when problematic weather conditions are forecasted – shall be implemented in all prevention tools	The incident and crisis management system enables an interface to early warning systems to forecast dangerous weather conditions that may potentially affect the railway / metro system. Using the business process tools, the system will initiate advance actions in order to prevent or mitigate the effects of extreme weather on railway / metro operation.	3.10.15 (Weather alerting systems)
6	UR-CM-R10 - Threat intelligence	An increase in the level of external intentional terror and cyber threats is handled by the incident and crisis management system using its business process tools and rule-based tools, which enable initiating advance actions in order to prevent or mitigate the risks arising from these threats.	5.2 (Security incidents) 5.3 (Cyber security incidents) 3.12.1 (Business process management notation) 3.12.2 (Workflow planning tool) 3.12.3 (Reusable Modules)
7	UR-CM-R0211 - Detection of abnormal situation/anomalies in sensors, IT systems, assets, behaviour, forbidden objects, suspicious items, etc.	Sub-system anomalies and alerts are transferred to the incident and crisis management system, which processes the data using rule-based and correlation-based tools that rely on expert knowledge and artificial intelligence algorithms. When the system tools or external tools define these events as incidents, the system handles them using its built-in incident management tools.	5.2 (Security incidents) 5.3 (Cyber security incidents) 3.12.1 (Business process management notation) 3.12.2 (Workflow planning tool) 3.12.3 (Reusable Modules)
8	UR-CM-R12 - Detection of combined attacks	From the perspective of the incident and crisis management system, the combined attacks are entered and handled using the built-in incident management tools. In the specific context of combined attacks, the system has tools with which it defines the incident severity level based on the nature of the incident, so that the appropriate resources required for the combined on- and off-site response will be allocated, taking into consideration the incident's characteristics and the expected risks, and also indicating the need to establish a crisis management group, if required.	2.3 (Cyber-physical related incidents management) 5.2 (Security incidents) 5.3 (Cyber security incidents)
9	UR-CM-R14 - Harmonised reporting tool for exchanging information	The reporting tools of the incident and crisis management system include an internal module for displaying the incident status to all stakeholders and an internal chat tool, as well as a mass notification system that enables disseminating messages to a large number of recipients via text, images, video files and email.	3.4.2 (Situational picture at a glance) 3.10.9 (Mass Notification System) 3.9.4 (Reporting tool)
10	UR-CM-R15 - Ensure that the same degree of concern (slight - moderate - severe) is understood by both sides, the Central IT	The incident and crisis management system defines the severity level of the incident based on the input of the incident manager, who is defined as the incident assignee. Therefore, the severity level and the characteristics of the incident, as seen by all the stakeholders	3.7.2 (Incident levels and categorisation by delay time)

Nr.	Requirements	ICMT Specifications	Referenced to chapter in this document
	Body and the Central Security Body	involved in the incident management, are one and the same.	
11	UR-CM-R16 - The moment (threshold) must be determined as to what and to whom an incident is reported - and by what communication means	The incident and crisis management system depends on peripheral systems, such as the SIEM system, to define a cyber incident. Therefore, upon the definition of an event / alert as a cyber incident by the SIEM system, the incident and crisis management system activates the business process tool and the message dissemination tool, to enable effective management of the cyber incident	2.3 (Cyber-physical related incidents management) 3.2.2 (CONOP) 3.10.9 (Mass Notification System) 3.9.4 (Reporting tool) 3.10.10 SIEM)
12	UR-CM-R17 - The threshold for reporting by the Central IT Body or Operation Centres to the Central Security Body must be defined.	The incident and crisis management system is a decentralised system that is operated from a variety of control centres – for operation, security, cyber security, crisis management and maintenance management. Therefore, it enables communication, information dissemination / sharing, collaboration, decision-making and effective management of a wide range of incidents among the various operational control centres.	2.3 (Cyber-physical related incidents management) 3.2.2 (CONOP) 3.4.2 (Situational picture at a glance) 3.8 (Incident assessment – incident intake, analysis, alerting and handling) 3.10.10 (SIEM)
13	UR-CM-R18 - The reporting from the Central IT Body or the Operation Centres	The incident and crisis management system enables human in the loop decision making for the purpose of defining the incident's characteristics and the risks arising from it. The incident and crisis management system's reporting tools include an internal module for displaying the incident status to all stakeholders, as well as an internal chat tool and a mass notification system.	2.3 (Cyber-physical related incidents management) 3.2.2 (CONOP) 3.8 (Incident assessment – incident intake, analysis, alerting and handling) 3.9.4 (Reporting tool) 3.10.9 (Mass Notification System) 3.10.10 (SIEM)
14	UR-CM-R19 - Information on the situation to be provided to the company staff	The incident and crisis management system includes applications enabling to disseminate information concerning the incident to company staff. These include tools such as Web client and mobile app, as well as information dissemination tools via text messages and email.	3.10.9 (Mass Notification System) 3.11.1 (Mobile devices for the IM / RU staff) 3.11.2 (Web clients)
15	UR-CM-R20 - Ensures the standardised and simplified exchange of incident information	The incident and crisis management system's display and reporting tools include user-friendly tools for reporting and information exchange among the stakeholders involved in incident management, through simple dissemination of textual information via a mass notification system, or more complex data dissemination via Web clients and a mobile app, or information sharing via a logical interface (SDK / API).	3.9.4 (Reporting tool) 3.4.1 (Basic functionalities) 3.10.9 (Mass Notification System) 3.11.1 (Mobile devices for the IM / RU staff) 3.11.2 (Web clients)
16	UR-CM-R21 - Reliable communication and early warning	The system-wide installation of the incident and crisis management system by the infrastructure manager / railway undertaking / metro operator enables reliable communication among the various stakeholders while managing the	3.8 (Incident assessment – incident intake, analysis, alerting and handling)

Nr.	Requirements	ICMT Specifications	Referenced to chapter in this document
		incident, including the option of advance alerting to risks.	3.10.9 (Mass Notification System)
17	UR-CM-R22 and UR-CM-R23 - Shared early warning system for the operators of different means of transport	The incident and crisis management system enables handling early warning and suspicious situations via the business process and information dissemination tools, to enable effective management of the threat and mitigation of the potential risks.	3.10.9 (Mass Notification System) 3.12.1 (Business process management notation) 3.12.2 (Workflow planning tool) 3.12.3 (Reusable Modules)
18	UR-CM-R24 - Cross-border exchange with the use of different languages must be considered	This issue can be handled by using the incident and crisis management system's information dissemination tools, the use of the system's Web client application, or the establishment of a joint incident management control centre for operators in the different geographical areas.	3.2.2 (CONOP) 3.10.9 (Mass Notification System) 3.11.2 (Web clients)
19	UR-CM-R25 - Situational awareness	At the foundation of the incident and crisis management system capabilities and implementation are a uniform and shared display of the situational picture pertaining to the incident, when the system is installed in a variety of technological applications at the sites of shareholders relevant to the management of the incident – off- and on-site.	3.4.2 (Situational picture at-a-glance) 3.11.1 (Mobile devices for the IM / RU staff) 3.11.2 (Web clients)
20	UR-CM-R26- Impact and cascading effect simulation	The incident and crisis management system includes different parameters for defining the impact of the incident, such as casualties and effect on system operation. These parameters affect the organisational arrangements for the incident's management, such as establishing a crisis management group, allocating required internal and external resources (manpower and means) and implementing the emergency plan and procedures using the business process tool.	3.8.2 (Incident intake form) 3.12.1 (Business process management notation) 3.12.2 (Workflow planning tool) 3.12.3 (Reusable Modules) 9.2.1 (Intake form structure)
21	UR-CM-R27- Crowd management	The incident and crisis management system, via the business processes in the control rooms (off-site) and the activation of operational personnel (frontline staff, on-site), enables effective crowd management in stations and/or onboard trains.	3.12.1 (Business process management notation) 3.12.2 (Workflow planning tool) 3.12.3 (Reusable Modules) 5.1.5 (Abnormal congestion – overcrowding)
22	UR-CM-R28- Resumption of all operations of the multimodal transport system – complying with mutual interdependencies	The incident and crisis management system is designed to handle all phases of the emergency incident, including the recovery phase. The assimilation of the system at the sites of all the stakeholders, and the use of the business process and information dissemination tools, implement the recovery plan of the railway/metro system in the incident and crisis management system.	3.2.2 (CONOP) 3.8 (Incident assessment – incident intake, analysis, alerting and handling) 3.12.2 (Workflow planning tool)

Nr.	Requirements	ICMT Specifications	Referenced to chapter in this document
23	UR-CM-R29- Evaluation and explanation of common "lessons learned" to be implemented in the next prediction/prevention phase	The incident and crisis management system's logging and debriefing tools enable effective incident debriefing, as well as organisational learning and improvement of the organisation's response processes, by adapting the emergency procedures and updating the business processes in the system.	3.9.1 (Incident log) 3.9.3 (debriefing) 3.9.5 (Business analytics) 3.12.2 (Workflow planning tool) 3.13.2 (Assessment tools)

3.2 Concept of operation

3.2.1 Users

The ICMT serves two kinds of users:

(1) **Users in the control centres (control centre operators).** The system serves various uses in operation, maintenance, security and crisis management rooms, for example:

a. Operation control rooms – regional / national control Centres for incident management and train re-scheduling due to incident impact (RIMC), regional / system operation control centre (OCC) – (regional – in a geographic area; system – of a specific railway system, for example, High Speed Line (HSL) of the RU/IM, security operation centre (SOC).

b. Asset and maintenance management control centre, including also fixed physical assets (passenger stations and terminals, line of route facilities, the track, traction power and more), and rolling stock.

c. Control centres for communication infrastructure and cyber operations – network operation centre (NOC) and/or cyber security operation centre (CSOC).

d. External stakeholder's control room users – Police, Fire & Rescue Services, EMS, etc.

e. Crisis Room for crisis management.

The SAFETY4RAILS Information System S4RIS provides a GUI that is meant to be deployable in all of the above mentioned environments.

(2) **On-site responders** – individuals, teams and subcontractors of stakeholders, responding to crises and disasters on behalf of the RU/IM, maintenance contractors, first responders, etc.

3.2.2 Operating concept (CONOP)

FIGURE 6 visually depicts the operating concept (CONOP) of the railway/metro system incident management system. It includes core operating centres, peripheral control centres and on-site responders.

(1) Core control centres. Core control centres are control centres that are essential to the effective operation of the incident management system. To enable effective system operation, the following core control centres are required, as a minimum:

a. **Railway Incident Management Centre (RIMC) –** responsible for managing incidents on railway infrastructure (its function might also be undertaken by the OCC, as indicated below). The RIMC maintains lines of communication to operation and traffic control centres and is responsible for communication with the RU operation control centres, as well as for communication with the LP, first responders and relevant subcontractors.

b. **Operation Control Centre** – responsible for traffic management in a specific geographic area / line, and for maintaining lines of communication with train drivers, infrastructure maintenance entities (in RU – communication with rolling stock maintenance entities), the LP, first responders and subcontractors.

c. **Maintenance Control Centre/s** – responsible for maintenance of the line infrastructures (electrification, tracks, signalling, communication, operational systems, fire safety, etc.), passenger stations and terminals, line of route facilities and rolling stock.

d. **Security Operation Centre** – responsible for operating the railway system security systems and managing its security operation.

(2) **Peripheral control centres.** These are optional control centres for operating the incident management system, and include:

a. Train stations management control centre.

b. Network operation centre (NOC).

c. Cyber security operations centre (CSOC).

d. Customer Service Centre (CSC).

e. Crisis Room for managing crises.

(3) **On-site responders.** First responders at the incident site, including end users of ICMT mobile devices. These include:

a. Lead Person acting on behalf of the IM/RU.

b. Mobile teams tasked with managing incidents on behalf of the IM/RU.

c. Maintenance teams acting on behalf of the IM/RU.

d. First responders – Police, Fire & Rescue Services, EMS.

e. Various IM/RU contractors.

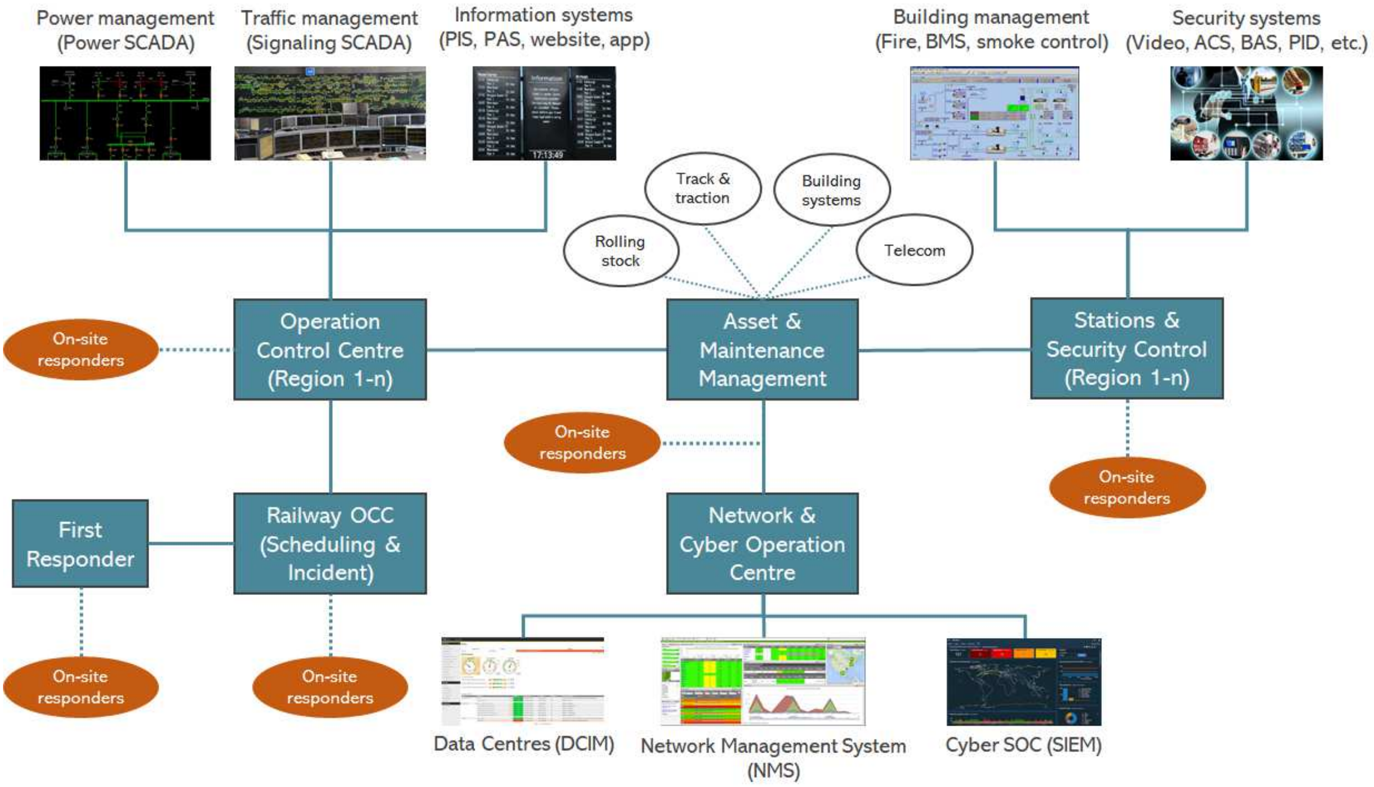

Power management (Power SCADA)
Traffic management (Signaling SCADA)
Information systems (PIS, PAS, website, app)
Building management (Fire, BMS, smoke control)
Security systems (Video, ACS, BAS, PID, etc.)
Track & traction
Building systems
Rolling stock
Telecom
On-site responders
Operation Control Centre (Region 1-n)
Asset & Maintenance Management
Stations & Security Control (Region 1-n)
On-site responders
On-site responders
First Responder
Railway OCC (Scheduling & Incident)
Network & Cyber Operation Centre
On-site responders
On-site responders
Data Centres (DCIM)
Network Management System (NMS)
Cyber SOC (SIEM)

FIGURE 6: OPERATING CONCEPT (CONOP)

3.3 ICMT architecture

The ICMT architecture is displayed in FIGURE 7 below. It includes the following elements:

(1) **User interface.** A user interface in three typical configurations:

a. Control centre client – in an assignee or collaborator configuration, which includes:

- Video management screen
- Business process management screen
- A screen with mapping tools

b. Web client workstation – a browser-based workstation which includes one or more screens with the main control centre functions, in a browser-adapted configuration and capabilities.

c. Application for rolling stock, which includes view viewing and business process management capabilities as a collaborator.

(2) **Functional modules.** Functional modules for realising the following capabilities:

a. Gateways to operational, security and safety subsystems; databases and more.

b. Rule engine for correlation and an events filter.

c. Interface to the Geographic Information System (GIS), for the purpose of managing the ICMT system configuration.

d. Business process management tools, used to create workflows in the system, with automatic actions (automatic activation of sub-systems' functions), semi-automatic actions (operator-activated sub-systems' functions), and manual actions of the operator.

e. Database for logging incidents and operator actions, and business intelligence (BI)-based analysis tools.

f. A system training and simulation module.

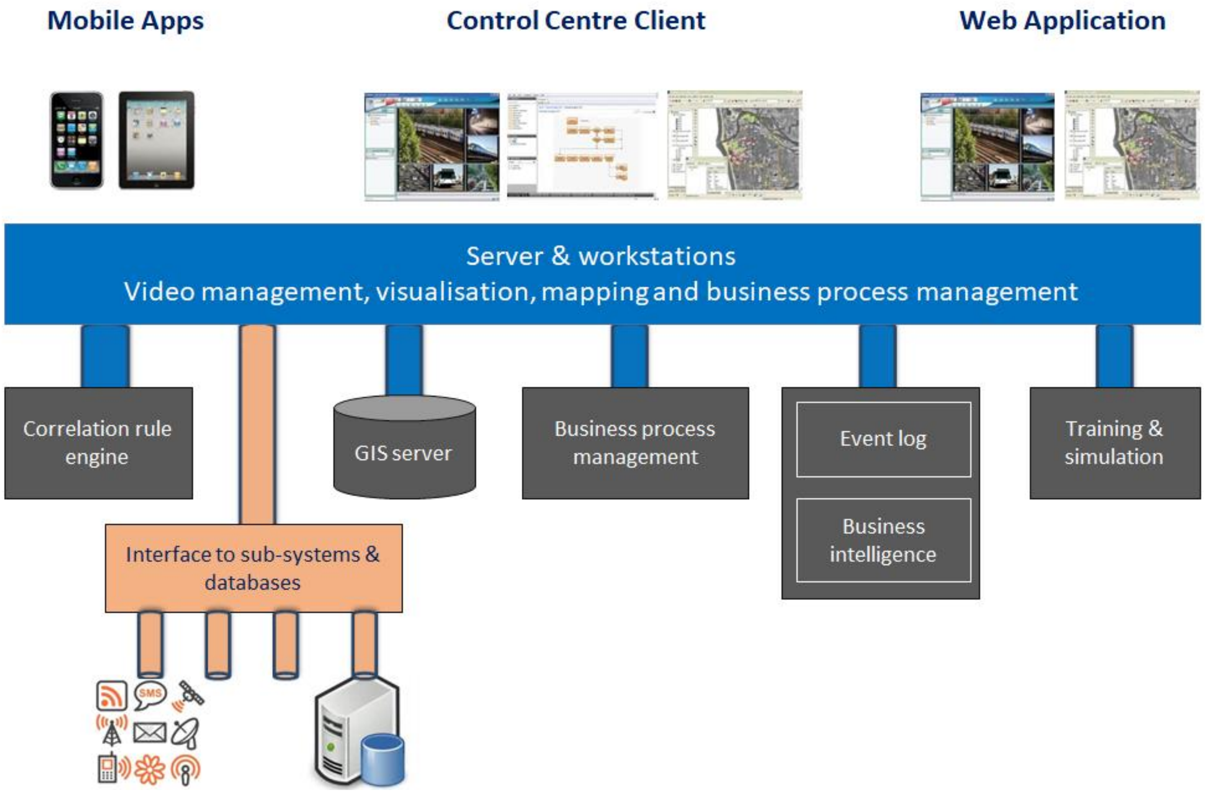


FIGURE 7: ICMT ARCHITECTURE

Within SAFETY4RAILS we addressed the above mentioned two architectural sections also in a two folded way: the S4RIS GUI serves as a gateway to all the individual GUIs of our tools and provides the possibility to be extended regarding the above-mentioned components. The individual tools are (due to the work in SAFETY4RAILS to be connected to the S4RIS GUI) also prepared to be integrated in web-based GUIs. The tools of SAFETY4RAILS already fulfil a subset of the functional modules, mentioned above: RAM² from Elbit provides a rule engine to correlate events, SecuRail provides a GIS based system for modelling and representing railway networks, a centralized database to log events and operator activities is foreseen but not implemented.

3.4 General functional requirements

3.4.1 Basic functionalities

The ICMT should have the following basic functionalities:

(1) Incident management capacity that covers the lifecycle of an incident – monitoring capacities to identify the potential for or an actual incident occurring, incident assessment, incident handling and incident review.

(2) Interfaces with technological systems serving the railway/metro systems, such as Video Surveillance System (VSS) and security systems, Signalling and Train Control (S&TC) system, Railway Scheduling System (RSS), Geographic Information System (GIS), telephony system, Help Points (HP), Mass Notification System (MNS), Enterprise Asset Management (EAM) system, Security Information & Event Management (SIEM) system, Passenger Information Systems (PIS), Building Management System (BMS), power management system, Fire Life Safety Systems (FLSS), weather alerting system and on-board systems, as may be required, and relevant databases.

(3) An intuitive Graphical User Interface (GUI) / User Interface (UI), including mapping tools, which can operate on three different platforms – desktop, Web and mobile applications.

(4) Automated and manual data entry of information on incidents, including updating their status during their entire lifecycle.

(5) Monitoring and debriefing of the operator's actions and of tasks in the system, using the ICMT database.

(6) The ICMT system should support standardised alerting protocols, such as OASIS Common Alerting Protocol (CAP), XML-based data format, JSON, OPC, REST, PSIA, etc. Software Development Kit (SDK) and Application Programming Interface (API).

3.4.2 Situational picture at-a-glance

The ICMT system should provide a clear situational picture for any type of scenario, starting from outputs of the current system / operation monitoring, comprising the following:

(1) Include all the relevant events, alerts and incidents, sorted in a meaningful way, with general information notes.

(2) Reflect only the information that is relevant to the logged in user, such as the operator, supervisor /

(3) Frequent updating of the incident situational picture and details, and their dissemination to all stakeholders.

3.4.3 Support throughout the incident life cycle

The ICMT system should support the entire life cycle of an incident – incident intake, incident handling and incident review, as presented in FIGURE 8 below.

(1) Incident intake, using an adaptive process covering:

  a. Intake and registration, using adaptive forms and a registration process.

  b. Incident analysis mechanism, which defines the severity level and foreseen impact on train / metro operations and generates an appropriate incident handling response.

  c. Alerting different stakeholders that are part of the incident handling scenario, using conventional communication mechanisms and messaging applications and mass notification capabilities.

(2) Incident handling – a business management process documented as an Incident Response Plan and procedures developed by the railway/metro system RU/IM, that identifies the roles, responsibilities and collaborative response to incidents of the system IM, operators and other stakeholders.

(3) Incident review that supports real-time and offline evaluation, debriefing, reporting and auditing of incidents and their management.

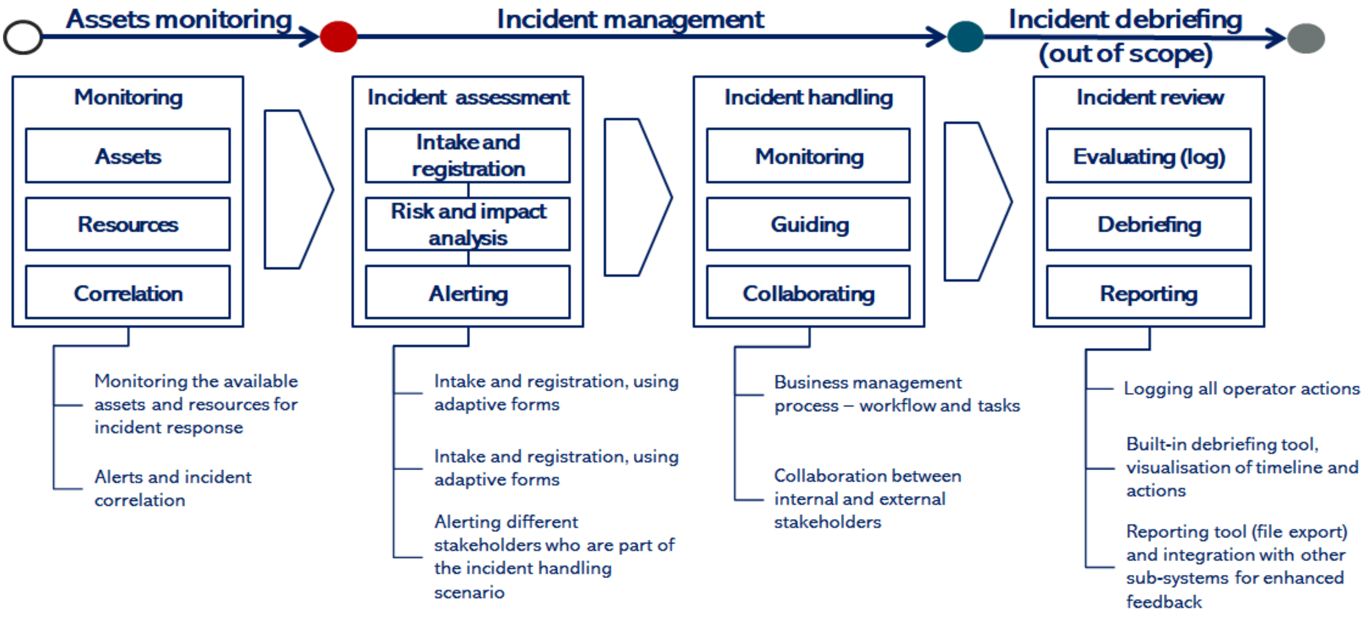

Assets monitoring
Incident management
Incident debriefing (out of scope)
Monitoring
Assets
Resources
Correlation
Incident assessment
Intake and registration
Risk and impact analysis
Alerting
Incident handling
Monitoring
Guiding
Collaborating
Incident review
Evaluating (log)
Debriefing
Reporting
Monitoring the available assets and resources for incident response
Alerts and incident correlation
Intake and registration, using adaptive forms
Intake and registration, using adaptive forms
Alerting different stakeholders who are part of the incident handling scenario
Business management process – workflow and tasks
Collaboration between internal and external stakeholders
Logging all operator actions
Built-in debriefing tool, visualisation of timeline and actions
Reporting tool (file export) and integration with other sub-systems for enhanced feedback

FIGURE 8: TYPICAL INCIDENT LIFE CYCLE

3.4.4 ICMT users and operators

In order to operate in accordance with and support the RU/IM Incident Response Plan and the Emergency Operating Procedures (EOPs), the ICMT should support various types of users at the operational level, including:

(1) **Operator.** The ICMT operator (as an assignee or collaborator) is responsible for incident assessment and for executing tasks in routine and emergency conditions, based on the CONOP, the different use-cases and workflows.

(2) **Control centre supervisor / shift manager.** The ICMT supervisor / shift manager is responsible for managing and supervising the execution of the tasks in routine and emergency conditions, based on the CONOP, the different use-cases and workflows. From a command and control standpoint, the supervisor / shift manager using the ICMT will serve as the senior user in the strategic management of the incident (Gold), as detailed in section 2.2.3 above.

(3) **External stakeholders / Web clients.** External stakeholders / Web clients are the stakeholders in and outside the rail organisation (e.g. first responders, contractors) who are usually not present in the OCC / RIMC and take part in incident management via a Web application. They are responsible for executing tasks as part of the incident response workflow, for collaboration and for communication with the on-site incident command entities (e.g. Lead Person) and the operator or shift manager in the control centre. From a command and control standpoint, the use of the system by stakeholders (usually as Web client) will serve these entities in the strategic management (Gold) of the organisation (Police Gold, Fire & Rescue Services Gold, EMS Gold, etc.).

(4) **Mobile clients.** Mobile clients are the stakeholders assisting on-site incident management, or having managerial authority in the organisation, who take part in incident management via a mobile application. They are responsible for executing tasks as part of the incident response workflow, for collaboration and for communication between different operators (as an assignee or collaborator) in the control room; or alternatively, they receive real-time updates concerning the incident. From a command and control standpoint, the internal and external stakeholders making use of the ICMT mobile applications will serve in a Silver (tactical management) or Bronze (operational management) capacity of the incident, as detailed in sections 2.2.3 – 2.2.5 above.

3.4.5 ICMT roles – assignee and collaborator/s

The terms 'assignee' and 'collaborator' refer to the person assigned to manage the incident – the incident manager – and to those collaborating with him. This is expressed in the Operator's user interface, in the manner in which he displays the incident, and in the business process relevant to the incident.

(1) **Assignee.** Only one person will be appointed assignee in any incident. The rule of thumb to the definition of an assignee in an incident is:

a. In the case of a local and/or low-level incident, an operator in the relevant control room should be appointed assignee.

b. In the case of a system-wide, high-level emergency incident and/or a crisis/disaster, the supervisor / shift manager in the relevant control room should be appointed assignee.

(2) **Collaborator.** All those assisting in incident management as operators of specific systems in the various control centres/rooms should be defined as collaborators. The number of collaborators – from a single collaborator to many – should be determined based on the level of complexity of the incident and the appropriate response, and the functions required to implement it.

3.4.6 Business process management

(1) The business process management (incident handling interface) should be based on the ICMT workflow management user interface. It should be used to manage various use-cases and should have the capacity to distinguish between types of incidents and their levels of severity.

(2) The business process management capabilities should support incident management, including:

a. Viewing the details of all relevant events, alerts and incidents and classifying them according to the severity level of their actual or potential consequences/impact.

b. Event correlation between adjacent and/or related sensors, using a rule engine and/or machine learning tools.

c. Automatic or manual operation of relevant interfaces, using the ICMT interface capacities with relevant sub-systems.

d. Receipt of a list of tasks to be executed as part of incident handling, with acknowledgement once completed.

e. Enabling the escalation of an alert or an incident based on predefined rules – operator handling time for a task, impact on safety and operations.

f. Assigning the workflow to a specific operator, acting as the assignee (incident manager in the workflow) or collaborator (an operator participating).

g. Transferring an incident from one operator to another, when the assigning operator is overloaded with incidents.

h. Adding, assigning and reassigning tasks impromptu to a single user or a group of users, and adding attachments.

i. Adding attachments to tasks and incidents – document in standard format (Word, PDF, etc.), snapshot, video file, plain text file.

j. Recording / time-stamping all procedural actions (business processes) taken when managing the alerts, incidents and workflow tasks.

k. Adding comments, in either a predefined form or as free text, including task comments.

3.5 Configuration and customisation

(1) The ICMT should support an adapted configuration for the Control Centre Client workstations and the Web Client workstations. The mobile application should be uniform for all users.

(2) The ICMT interface configuration should also support the type of the user – operator or control centre supervisor / shift manager, including capabilities to display the dashboard to managers in the control centre and in viewing-only workstations.

(3) Changes in the configuration should be made using two main tools:

a. Operator's user interface, for ad-hoc configuration changes.

b. System administrator and planning tools, for configuration changes adapted to IM/RU requirements.

3.5.1 ICMT workstation configuration

3.5.1.1 Functional usage

(1) The ICMT workstation should support the system functionalities, including video viewing, incident assessment, handling, mapping tools (GIS) and incident review and debriefing, in a flexible configuration, as presented.

(2) A typical ICMT workstation consists of three monitors:

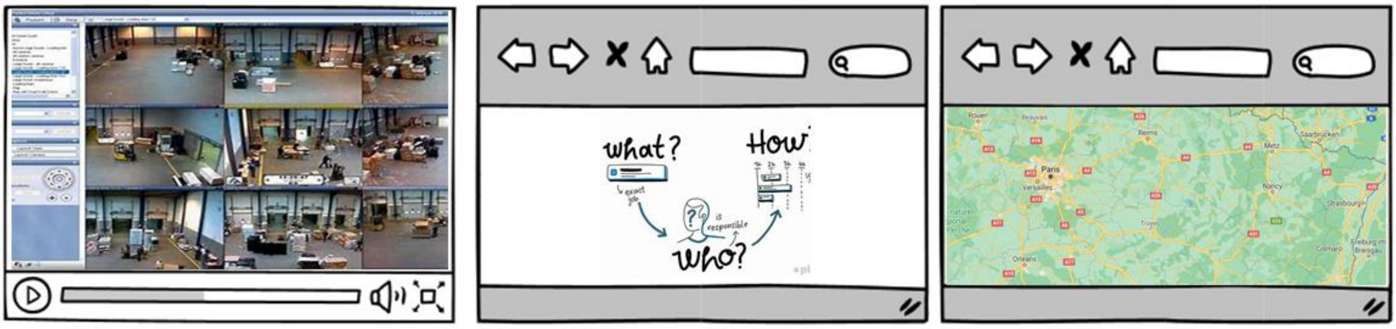
a. A monitor for video surveillance;

b. A monitor for workflow management; and

c. A monitor for GIS and mapping of the railway / metro infrastructure.

This configuration can, of course, be changed based on the features of the ICMT workstation in the specific operations control centre in which it is situated.

(3) These monitors may be a part of the console in the monitoring workstation. When the system is integrated with other operational systems, it is essential to provide a similar user experience (UX) to that of the other applications in the work position.



Video management screen

Workflow management

GIS & mapping

FIGURE 9: ICMT TYPICAL WORKSTATION CONFIGURATION (EXAMPLE)

3.5.1.2 Web clients with secured remote access

(1) Implementation

a. Web clients should be installed for the various stakeholders, based on the IT infrastructure of the IM/RU, responding bodies and contractors, if applicable.

b. The workflows should be configured and assimilated as specified into the incident response plan and relevant incident response procedures (e.g. EOPs).

(2) Web clients' capacities

The implementation of the Web clients should support the following functionalities:

a. Visualisation of events, alerts and incidents, as required by the CONOP and configured by the system administrator.

b. Incident management and sharing of information and of the situational picture of an incident among the OCC/RIMC operators and the various stakeholders.

c. Operation of sub-systems such as VSS, security systems, messaging and GIS.

d. Communication with the ICMT through the Web client.

e. Create a customised user interface that displays relevant information about the incident to the end user – location, description, severity, textual data, notifications and tasks interface.

3.6 Display and monitoring

3.6.1 Display layout

The ICMT should support the following display layout:

(1) Flexible multi-screen setups for the GUI.

(2) Dock/undock multiple views on different monitors and dock all views and manage them from a single screen.

(3) Define and save a specific layout per workstation.

(4) System administrators should be able to define which modules are viewable on a per user basis.

3.6.2 System monitoring

The ICMT should:

(1) Support internal BIT (Built-In-Tests) monitoring with GUI, to automatically identify and recover from application faults. This monitoring service should be configurable by system administrators to take various actions upon failure, such as sending notifications to technical staff, using e-mail and/or SMS, when a service fails or becomes unavailable.

(2) Enable administrators to define the monitoring time interval and number of alerts before a notification is sent.

(3) Manage and create/update applicable logs.

(4) Events, alerts and incidents, generated by other sub-systems

(5) The ICMT should enable alerts visualisation and incident creation from other sub-systems, such as:

a. Fire and smoke detection systems in the railway / metro infrastructure (stations, tunnels, electrical sub-stations, trackside technical rooms, depot facilities, control centres) and on-board systems.

b. Trespassing or unauthorised access incidents, generated by security and railway / metro safety systems.

c. Overcrowding / extreme congestion situations in stations and on-board the trains, generated by video based and/or automatic counting systems, or overweight load detectors (on-board the rolling stock).

d. Extreme weather conditions, generated by a weather alerting system.

e. Assault or threat situation generated by panic buttons in stations and on-board the trains.

f. Critical faults of railway / metro mission critical sub-systems, such as S&TC, FLSS, facility systems, crisis communication systems, etc.

g. A cyber incident with potential to affect safe operation the railway / metro system.

(6) Video and monitoring: The ICMT should enable two options for video viewing:

a. Via video wall display: Video wall requirements as per control centre requirements.

b. Via workstation monitors: High Definition (HD)/Ultra High Definition (UHD) monitors.

3.6.3 Incident visualisation

Visualisation display of an incident should include the following elements:

(1) Visualisation of the incident's location – the location should be displayed via the system's GIS mapping tools (e.g. aerial photo, GIS, city map, raster map, vector map) in the dedicated screen or window of the system's location/mapping display.

(2) Information line/s – a line of text in a separate window, which displays alphanumeric data concerning the incident and a situational overview.

(3) The entered information should be either automated or entered by the operator through use of a pull-down menu, list of values (LOVs) or free text.

(4) Rolling stock data should be extracted from the Signalling & Train Control (S&TC) / Automatic Vehicle Locating System (AVLS) / Railway Scheduling System (RSS), as may be required.

(5) Each incident should be assigned a sequential unique number and time stamp. Related data should be logged-in automatically.

(6) The data should include, as a minimum:

  a. Time stamp.

  b. Logged in operator and the role of the operator (e.g. assignee, collaborator).

  c. Incident type, with its unique ID.

  d. Number of trains affected (including train-specific alpha-numeric ID) and their status, as reported by the S&TC / AVLS / RSS, as may be required.

  e. Impact on railway/metro system infrastructure, operational and safety related systems, as well as environmental impact, if any (e.g. if hazardous materials are involved).

  f. Impact on people – fatalities and injuries, including the severity of injuries.

  g. Projected number of people that will be affected by the incident, e.g. on involved trains.

  h. Available resources: Operator's staff, maintenance personnel, security personnel, engineering and heavy equipment, alternative public transportation, etc.

  i. Resources dispatched, informed.

  j. Stakeholders involved in the incident.

(7) The information line and situational picture should be constantly updated as the incident progresses.

(8) An at-a-glance operational overview that indicates important / critical information, such as open incidents, tasks that still require attention, escalations and other outstanding matters. The summary screen display should be organised and configurable to hold a large amount of information at a high-level view. It should be easy to read and provide only the necessary details.

(9) Classification of the severity of the incident – this should be carried out using different coloured 'flags' or a similar method in the incident line, in accordance with the incident's level of severity. The higher the priority attributed to the incident, the higher it should appear in the incident screen. Incidents classified in the same level should appear in their order of occurrence (an incident occurring earlier should be displayed higher on the screen or vice versa, as chosen by the ICMT operator).

3.6.4 Incident handling interface

(1) The incident handling interface should be based on the ICMT workflow management user interface. It should be used to manage various use-cases and should have the capacity to distinguish between types of incidents and their levels of severity.

(2) The user interface for the Web and Mobile clients should be based on each user's specific role. It should present these users with information that is relevant to the incident and to their role, enabling them to execute tasks in their specific workflows.

3.6.5 Dashboards

(1) The ICMT should have built-in capacity to display the dashboards for the workstations serving the various management positions.

(2) The dashboard design should comply with human engineering requirements.

(3) The dashboard should allow displaying the following parameters:

a. Status of incidents in the railway/metro system, covering all its assets.

b. General information about alerts in sub-systems.

c. Display of quality of service (QOS) parameters and key performance indicators (KPIs) for incidents in which QOS plays a role (usually measured in time) in the handling of the event.

(4) Display of any divergence from Service Level Agreements (SLAs) / KPIs with third parties (Contractors, Police, Fire & Rescue Services, etc.), for events in which SLA parameters are applicable.

(5) General information about users and system workstations should be provided in regard to personnel working in the railway/metro system at any given time, workstations currently in operation, cross-section of events by railway/metro system assets and the like.

3.7 Use-cases and incident levels

3.7.1 Use-cases

The ICMT should enable the management of all railway/metro system incidents, classified into the following three categories:

(1) Safety, operational, natural disasters and critical faults incidents.

(2) Security incidents.

(3) Cyber security incidents.

Chapter 5 in this document lists the specific use-cases included in the above categories.

3.7.2 Incident levels and categorisation by delay time

(1) Incident classification should be performed based on the level of severity and delay time categories. The classification of incidents should be based on the potential severity for determining command, control and response purposes.

(2) Incidents are classified into either four or five severity levels, as detailed in Table 2 below containing suggested delay levels with RU/IMs deciding their criteria based on the type of operation and physical circumstances.

TABLE 2: INCIDENT CLASSIFICATION LEVELS

Incident level	Classification into 5 levels	Classification into 4 levels
Level 1	Incidents that do not affect the safety of people, railway / metro system assets and operational capability, but with a potential to produce such impact if escalated.	Incidents that do not affect the safety of people, railway / metro system assets and operational capability, or result in short delays (a few minutes up to half an hour) in railway/metro system traffic, without threatening the safety of people.

Incident level	Classification into 5 levels	Classification into 4 levels
Level 2	Incidents resulting in short delays (a few minutes up to half an hour) in railway/metro system traffic, without placing the safety of people at risk.	Incidents with concrete risk to the safety of people (injuries and/or fatalities) and/or damage to physical and/or logical infrastructure, causing moderate delays (half an hour to several hours) in railway/metro system traffic, without placing the safety of people at risk.
Level 3	Incidents with concrete risk to operations, the safety of people (injuries and/or fatalities) and/or damage to physical and/or logical infrastructure, causing moderate delays (one hour to several hours) in railway/metro system traffic.	Incidents with several casualties (fatalities/ injuries) and/or significant damage to physical and/or logical (cyber) infrastructure, causing significant delays (half a day to several days) in railway/metro system traffic.
Level 4	Incidents with several casualties (fatalities/ injuries) and/or significant damage to physical and/or logical infrastructure, causing significant delays (half a day to several days) in railway/metro system traffic.	Crisis involving multiple casualties, resulting in significant damage or destruction of physical and/or logical infrastructure and/or rolling stock, which critically affects the operation of the railway/metro system for a significant period, with partial or full shutdown of the railway/metro system line's service and functionality.
Level 5	Crisis involving multiple casualties, resulting in significant damage or destruction of physical and /or logical infrastructure and/or rolling stock, which critically affects the operation of the railway/metro system for a significant period, with partial or full shutdown of railway/metro system service and functionality.	

It is also possible to classify incidents by system shut-down time, as presented in Table 3. The shut-down time in this context refers to the system's shut-down time as a direct result of the impact of an incident on the ability to manage traffic according to the operation plan.

TABLE 3: INCIDENT CATEGORIES BY DELAY

Delay of minutes	Delay of hours	Delays of days to months
M1 – delay < 30 min	H1 – delay of 3-4 hours	D1 – partial or full system shut-down for 1 day (24 hrs)
M2 – 30 min < delay < 60 min	H2 – delay of 4-6 hours	D2 – partial or full system shut-down for 2-3 days
M3 – 60 min < delay < 90 min	H3 – delay of 6-12 hours	D3 – partial or full system shut-down for 4 days - 1 week
M4 – 90 min < delay < 120 min	H4 – delay of 12-18 hours	D4 – partial or full system shut-down for more than 1 week to 1 month
M5 – 120 min < delay < 150 min	H5 – delay of 18-24 hours	D5 – partial or full system shut-down for months

3.8 Incident assessment – incident intake, analysis, alerting and handling

Incident assessment takes place when an incident in any of the railway/metro system sites, assets or infrastructure (e.g. stations, tunnels, bridges, line of route, electrical sub-stations, trackside technical rooms, stabling areas, depot, trains) is reported to the OCC / RIMC by frontline staff, a passenger or an external stakeholder (e.g. Police dispatch, customer service centre or triggered by a sub-system. This incident assessment phase encompasses three steps: Incident intake, incident analysis and incident alerting.

3.8.1 Incident intake and analysis process

Incident intake should use predefined drop-down menus and LOVs, as well as complementary free-text field. The ICMT should:

(1) Support the intake, registration and data identification of all incidents in the railway/metro system, using a dedicated adaptive intake interface.

(2) Based on the alpha numeric location data entered into the intake form, the system, through its mapping tools, should automatically zoom into the incident location and present relevant information layers and data on the affected train/s, including its/their location.

(3) Assess the incident based on the use-cases and determine the appropriate incident workflows (Reusable Modules) developed specifically for the type, severity, impact and location of the incident.

(4) Using a predefined set of parameters, enter the estimated, reported or potential consequences of the incident – immediate safety issues, harm to people, number of trains affected, number of people involved or stranded on train/s, cyber issues, physical damage or impact to the railway/metro system infrastructure and/or mission critical systems, operational impact and anticipated shut-down time of the railway/metro system.

(5) Receive ongoing updates on the incident and enter new information as it becomes available.

(6) Relevant stakeholders to be notified should be automatically determined based on the specific scenario, and incident information should be automatically disseminated to them via the mass notification module. The receiving party should be able to determine the medium through which the information will be delivered (e-mail, SMS, etc.). Message acknowledgment should be logged in the system.

(7) The option of concluding an alert as a false alert should be provided, using a dedicated UI. Alerts concluded as false alerts should be logged into the system as events and as reported cases of false alerts.

(8) The incident intake should include incident no-action time-out (configurable), notification to the operator (periodicity and period should be configurable).

(9) The operator should have the option of transferring the incident to another operator (assignee or collaborator) if they are busy and handling another incident. The transfer of the incident to an operator should be a simple process, executed via the UI and the system log tools.

3.8.2 Incident intake form

3.8.2.1 General functional requirements

(1) The ICMT should provide the administrative tools to define the incident intake data fields (mandatory and / or optional) and execute the associated pre-requisites.

(2) The administrative Incident Form tool should support form configuration for the ICMT server, Web and Mobile clients.

(3) The intake process should facilitate the registration and classification of all the incidents. The various use-cases should be adapted to each installation site and each area of the railway/metro system infrastructure to create an adaptive intake process.

3.8.2.2 Intake form specific fields

The form should be compatible with the railway/metro system Incident Response Plan and should include the following fields and functionalities, as a minimum:

(1) Real-time synchronisation of all workstations, so that all ICMT client, Web and mobile users who share a certain incident view with its related form, will always see the most current data when they open the form.

(2) Storage of all data in the ICMT database in a clear and consistent manner, to enable their use for producing customer-specific reports for post-incident debriefing purposes.

(3) Identification of the name and role of the person reporting the incident, their position (unless a passenger), the relevant area, and the traffic control centre from which the report was received.

(4) The incident heading, to include the type of incident, its location and its expected conclusion time ('time to finish').

(5) Adaptation of the nature of the incident – the incident category and type, according to the specific use-case, in a number of ways:

   a. Search field with the option of entering free text, showing the relevant use-cases in each search field.

   b. Selection of fields (incident number, incident category, incident type, specific characteristics).

(6) Definition of the incident's level of severity and delay category, with the option of raising or lowering the level during the course of the incident.

(7) Setting key indicators of the incident, such as harm to people, operational mode, critical faults and evacuation.

(8) A specific field referring to casualties, including the number of fatalities and injured persons and additional data, to support an effective response by EMS.

(9) An incident stage management field – selection and operation of the incident stages, according to the progression of the incident in the field, which enables automatic operation of business processes through the activation of ReMos based on the following incident stages:

   a. Stage 1 – Immediate Actions (IA): A stage that is automatically activated once an incident is entered into the intake form and the data is processed.

   b. Stage 2 – Ongoing actions: The full range of actions that take place during the course of the incident, in order to support the immediate responders of the IM/RU and external first responders – police, fire & rescue services, EMS, RU/IM external contractors and more.

   c. Stage 3 – Recovery actions: The full range of actions required for business continuity and restoration of the operational routine.

   d. Stage 4 – Conclusion of the incident: Summarises the actions required to conclude the incident, document it and execute actions to support internal / external debriefing and investigation.

(10) Analysis of the operational effects on the railway/metro system, including:

   a. Definition of the area affected by the traffic operation according to the railway/metro operational plan.

   b. The system's operating method, as detailed in the railway / metro operational plan.

   c. Estimated system shutdown time.

   d. Option of entering, editing and/or updating the Intake Form during the incident, so that the Form will be 'live' throughout its duration.

(11) A specific field for stranded trains, including specific data:

   a. Train ID, as defined in the S&TC / RSS System.

   b. Train point of departure and destination.

   c. Train location.

   d. Number of passengers on the train (if available from any database).

   e. Train status with respect to passenger evacuation.

   f. Train status with respect to technical aspects.

   g. Identification of access point to rail infrastructure for responders

(12) A field with the estimated ‘time to finish’.

(13) Automatic display of geolocation data based on the various geographic database sources, including:

  a. Incident location, based on the details of the reporting party.

  b. Incident location on the train data (real-time data from the S&TC; forecasted location data from the RSS).

  c. Incident location based on an infrastructure element that is identified in the GIS system.

  d. A location may be a specific point, a ‘from to’ indication, or a section of an area.

  e. Various identifiers may be used (km of the track, train number, etc.) to display the geographic location, so that different identifiers may be used to display the same location on the mapping tools.

(14) Notification and reporting list, arranged by role (RU / Metro driver, frontline staff, maintenance staff, management, responding bodies, contractors, externals, etc.).

(15) Adaptive and intelligent capacities supporting the following:

  a. Showing only the fields / data relevant for the incident type.

  b. Enabling input of text concerning the incident.

  c. Enabling input of geographical data of the incident location, such as ‘track access points’, etc.

(16) Sub-forms – will be developed based on the ICMT concept of operation, for example:

  a. A form for reporting on the status of the first responders’ response.

  b. A form covering the response of maintainers and of maintenance sub-contractors.

  c. A Human resources form, covering the available personnel and their competences.

  d. A Welfare and logistics form, covering the available equipment and engineering IM / RU resources.

3.8.3 Alerting

The ICMT system should enable disseminating alerts to various users – Web and Mobile clients, mobile phones and e-mail recipients, in the case of emergency and crisis situations, through integration to the MNS. The alert dissemination module should include the following functionalities:

(1) Disseminating an incident alert with the incident data, as defined in the intake form.

(2) The generation of an incident alert will enable defining the following fields:

  a. The organisation, department, person receiving the alert, according to their position.

  b. Time stamp indicating when the alert was sent.

  c. Incident information – category, type location, impact.

  d. Drive to location or nearest access point link, activating a Web browser or standard navigation App for mobile devices (e.g. Waze, Google Maps, Here, etc.).

  e. Specific actions and check-list to be executed by the organisation, department, person receiving the alert.

  f. Required response to the alert – confirmation of receipt; confirmation that the alert has been read; confirmation that action has been taken; alert closure.

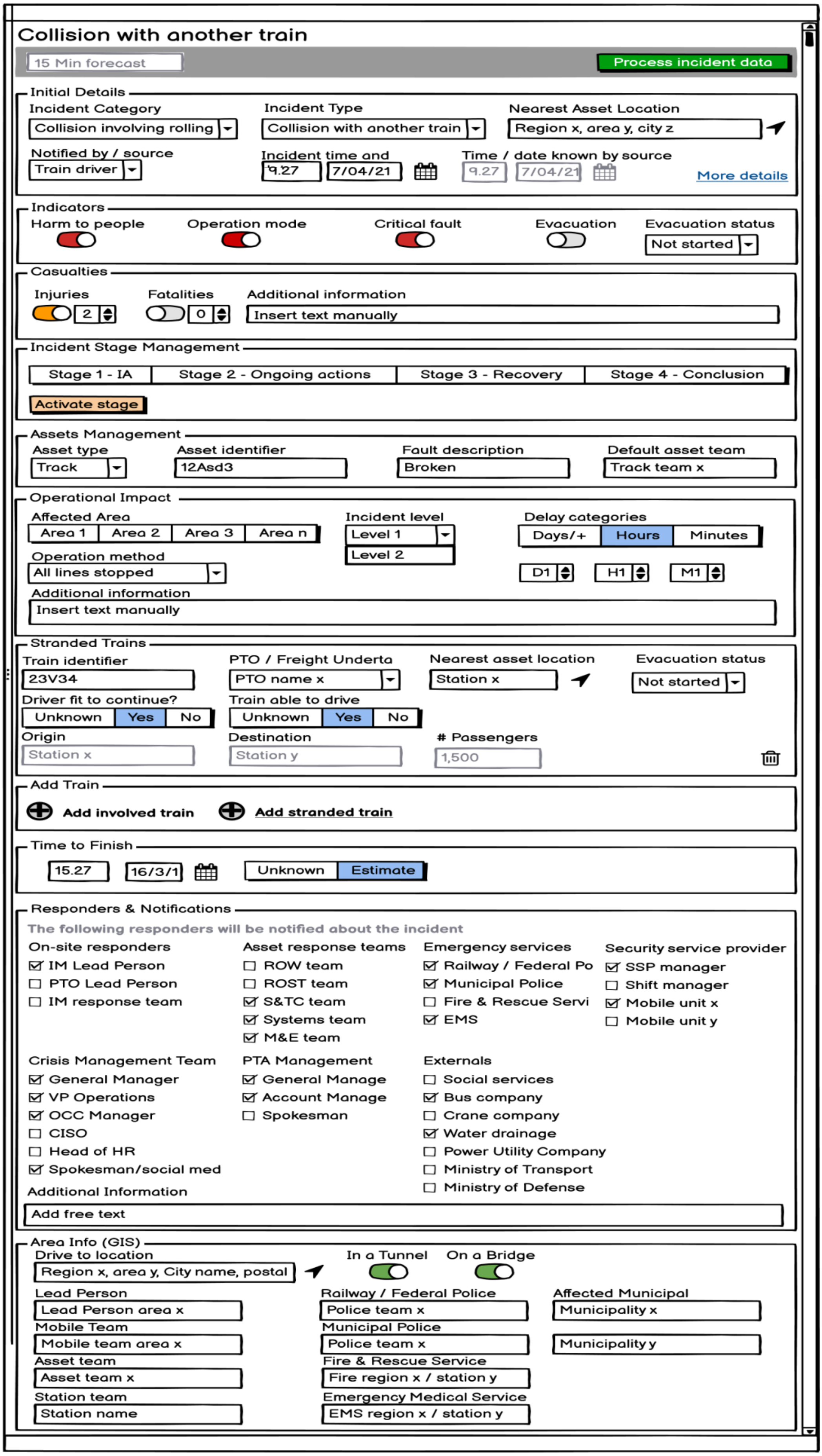
  g. Time reminder – time in which an action assigned to a recipient must be signed off; if not the recipient will receive a reminder, with the pre-set default to be set per group / staff member / message type.

  h. The importance and priority of the message.

(3) Based on scenario classification during the incident intake/registration process the system should be able to determine the business process/tasks that must be executed and messages/alerts that must be sent.

(4) The system should have the capacity to define the entities responsible for executing tasks based on a specific use-case.

(5) The system should enable Alerts generation when new information is entered, updated or edited, based on specific definitions.



Collision with another train

15 Min forecast | Process incident data

Initial Details

Incident Category: Collision involving rolling

Incident Type: Collision with another train

Nearest Asset Location: Region x, area y, city z

Notified by / source: Train driver

Incident time and: 9.27 | 7/04/21

Time / date known by source: 9.27 | 7/04/21

More details

Indicators

Harm to people | Operation mode | Critical fault | Evacuation | Evacuation status: Not started

Casualties

Injuries: 2

Fatalities: 0

Additional information: Insert text manually

Incident Stage Management

Stage 1 - IA | Stage 2 - Ongoing actions | Stage 3 - Recovery | Stage 4 - Conclusion

Activate stage

Assets Management

Asset type	Asset identifier	Fault description	Default asset team
Track	12Asd3	Broken	Track team x

Operational Impact

Affected Area: Area 1 | Area 2 | Area 3 | Area n

Incident level: Level 1 | Level 2

Delay categories: Days/+ | Hours | Minutes

D1 | H1 | M1

Operation method: All lines stopped

Additional information: Insert text manually

Stranded Trains

Train identifier: 23V34

PTO / Freight Underta: PTO name x

Nearest asset location: Station x

Evacuation status: Not started

Driver fit to continue?: Unknown | Yes | No

Train able to drive: Unknown | Yes | No

Origin: Station x

Destination: Station y

Passengers: 1,500

Add Train

Add involved train | Add stranded train

Time to Finish

15.27 | 16/3/1 | Unknown | Estimate

Responders & Notifications

The following responders will be notified about the incident

On-site responders
- ☑ IM Lead Person
- □ PTO Lead Person
- □ IM response team

Asset response teams
- □ ROW team
- □ ROST team
- ☑ S&TC team
- ☑ Systems team
- ☑ M&E team

Emergency services
- ☑ Railway / Federal Po
- ☑ Municipal Police
- □ Fire & Rescue Servi
- ☑ EMS

Security service provider
- ☑ SSP manager
- □ Shift manager
- ☑ Mobile unit x
- □ Mobile unit y

Crisis Management Team
- ☑ General Manager
- ☑ VP Operations
- ☑ OCC Manager
- □ CISO
- □ Head of HR
- ☑ Spokesman/social med

PTA Management
- ☑ General Manage
- ☑ Account Manage
- □ Spokesman

Externals
- □ Social services
- ☑ Bus company
- □ Crane company
- ☑ Water drainage
- □ Power Utility Company
- □ Ministry of Transport
- □ Ministry of Defense

Additional Information: Add free text

Area Info (GIS)

Drive to location: Region x, area y, City name, postal

In a Tunnel | On a Bridge

Lead Person: Lead Person area x

Mobile Team: Mobile team area x

Asset team: Asset team x

Station team: Station name

Railway / Federal Police: Police team x

Municipal Police: Police team x

Fire & Rescue Service: Fire region x / station y

Emergency Medical Service: EMS region x / station y

Affected Municipal: Municipality x | Municipality y

FIGURE 10: INCIDENT INTAKE FORM (EXAMPLE)

3.8.4 Incident handling – monitor, guide & collaborate

3.8.4.1 General

Incident handling in the ICMT should be represented by the incident workflow, which includes predefined tasks that operators are required to execute, based on a pre-prepared plan. The workflows and the tasks should be designed based on the Railway/Metro System Incident Response Plan and also on the rules and regulations applicable to system operation, as part of the configurations defined in this document and as per the specific procedures Standard Operating Procedures (SOPs) and EOPs) and the operational and safety policies of the railway/metro system managing organisation.

3.8.4.2 Incident handling capacities

(1) With respect to incident handling capacities, we refer to tasks and workflows, where a task is an individual action within a process. A process, in this context also refers to the manner of operation of the interfaces in the ICMT.

(2) Incident handling capacities are supported by workflows, which include a predefined number of tasks.

(3) The workflows should support both manual and automatic actions:

a. A manual action should be represented by lines of text with an explanation of the action to be performed by the operator or by another entity.

b. A semi-automatic action should be represented by lines of text with an explanation of the action, which will be automatically executed upon receipt of operator approval, by clicking the line of text.

3.8.4.3 Workflows and tasks management capacities

The ICMT system should provide the following workflows and task management capacities:

(1) Creating a predetermined workflow that will include various tasks and actions for all the stakeholders involved in the management of the incident, including options for cooperating, sharing information and responding jointly in a coordinated manner.

(2) Automatically defining the entities involved in the incident based on geolocation data, so that different geolocation data will affect the identity of the stakeholders involved in the workflow.

(3) Presenting the status of each incident and changing the status of any incident using visual tools.

(4) Opening incidents and tasks automatically triggered by forms, sub-forms, sub-systems alerts or scheduled triggers, or on-demand via 'quick launch' buttons.

(5) Selecting the workflow to deploy – a specific business process (ReMo) and/or tasks.

(6) Assigning a severity level category to incidents, either automatically or on-demand; group incidents in the incident log by site, owner, or category.

(7) Adding comments to incidents and tasks, in either a predefined form format or free text format.

(8) Enabling users to accept incidents and tasks assignment upon acknowledgement and escalate them.

(9) Presenting the sequence of the tasks and determining their level of importance, urgency and schedule for executing each action.

(10) Generating colour-coded pop-up notifications when an incident is created and escalated, with the colour reflecting the severity of the incident.

(11) Viewing and editing forms and sub-forms related to incidents and tasks. The forms and sub-forms with the most updated information should be saved and remain accessible at any time.

(12) Providing the possibility to assign a status, priority and deadline to actions. This status, priority and deadline should be visually represented to each user.

(13) Enabling the creation of sub-incidents to which sub-workflows and tasks are associated, and which are also associated to a 'parent incident'.

(14) Enabling the operator to edit, define a distribution list and send notifications (text, video files, other attachments, navigation instructions) manually or automatically to the various stakeholders during the incident, and also receive notifications, indications of their receipt and handling.

3.8.4.4 Escalation mechanism and interface

(1) It should be possible to implement an incident escalation mechanism when the incident consequences become or are expected to become more severe. The escalation interface should be part of the incident handling interface.

(2) The incident escalation mechanism should be based on the severity of actual or foreseen consequences/impact. Such an escalation should be covered by a procedure, and should lead to one of the following:

a. The incident continues beyond a duration that has been predefined in the system.

b. The impact of the incident expands.

c. Additional incidents, which are at least as severe as the initial incident, occur.

3.8.4.5 Incident correlation

The ICMT should provide the following correlation capacities:

(1) Possibility to add an existing incident as a sub-incident of another opened incident, when the operator determines that they are in fact the same incident.

(2) Possibility to break down complex incidents into sub-incidents that are all inter-related, where each sub-incident must be resolved in order for the overall incident to be closed. It should be possible to handle each sub-incident independently by a different user in the OCC / RIMC.

3.8.4.6 Incident prognosis (summary) tab / window

The ICMT should include an incident prognosis tab and window, enabling:

(1) Visual presentation of the incident status, with its key indicators and data.

(2) Anticipated incident termination time based on a history of incidents, system input and an advanced incident management time prediction algorithm.

3.9 Incident log, search, debriefing, reporting and business analytics

The incident review capabilities of the ICMT should be based on an incident log with log search and filter functions, a reporting module, a debriefing module and a business analytics module.

3.9.1 Incident log

The ICMT should support and provide the following functionalities to manage the incident log:

(1) Incident log manager, with the ability to import custom forms containing data retrieved from a wide range of data sources.

(2) Provide an integrated log containing views of all incidents and tasks, with automatic sorting of new incidents according to their pre-defined severities and creation time.

(3) Associated incident log forms with incident types, automatically retrieve them in real time, and relate them to specific tasks and incidents.

3.9.2 Search and filter capabilities

The system should support search and filter capabilities to provide the following functionalities for the incident handling process:

(1) Search to find incidents and tasks that share similar characteristics. Each similar incident type, opening and registration time, closure time, cyber assets, related sensors, related sub-systems, resource types, location, rolling stock ID, 'opened by' field, and deployed procedures should be displayed.

(2) Provide the ability to 'hide' closed incidents in the active incident log, yet search for closed incidents according to filtered properties, and also support the ability to search for active incidents.

(3) Search and filter should support several search and filter criteria.

3.9.3 Debriefing

(1) The ICMT should include debriefing capabilities based on the capture and analysis of incident data for the purpose of debriefing incidents occurring in the operational environment, as well as incidents generated by the training workstation.

(2) The debriefing module should allow displaying the actions of all the operators by their role in the response synchronously on a time axis. The UI should allow running the recorded segment at different rates, stopping and replaying.

(3) The operator's actions should be visually indicated on the debriefing module UI.

(4) Free text written by the operator during the incident should be available, but the data displayed should remain clear and easily comprehensible, not overburden the debriefing module UI.

(5) The debriefing module should enable analysing the different operators' response times according to the settings of the workflow and the specific tasks.

(6) The debriefing module should enable interfacing with an external recording solution (e.g. video recording, voice recording, screen recording), in a manner enabling the display of all the actions of each workstation for each incident individually and in detail.

(7) The debriefing module should allow exporting debriefing files to an external file, to enable the saving the files for an extended period of time in a standard file server. It should be possible to run the files with standard tools (Windows Media Player, VLC Media Player, etc.), or alternatively, with a proprietary tool that is attached to the exported file.

3.9.4 Reporting tool

The ICMT should include an integrated reporting tool that enables generating reports automatically and on-demand. The built-in reporting tool should support the following functionalities and capacities:

(1) The reports should enable comprehensive evaluation of incidents.

(2) The reports generator should enable the access and use of each of the fields and records in the database, and also enable the creation of templates, tables or forms in formats to be determined by the authorised operator / administrator.

(3) The system should be able to deliver the following management reports as a minimum:

(4) Detailed incident reports, which include incident summary, all the tasks that were executed during the handling of the incident, relevant snapshots and maps.

(5) Evaluation report based on previously set KPIs.

(6) Snapshot report, based on the status at a specific moment.

(7) Automated generation and dissemination of reports to users, according to incident progress and a pre-defined schedule.

(8) Printing and saving in various standard file formats, including Word, Excel, MHTML, and PDF.

3.9.5 Business analytics

The ICMT should support a business analytics module. The business analytics module should use the report generator tools, customised queried and OLAP (Online Analytical Processing) tools using database cubes with incident and service analytics capabilities.

3.9.5.1 Incident analytics

(1) The ICMT GIS tools, forms and database should comprise the infrastructure for this module.

(2) Allows analysing incidents based on time, location, incident category and incident type, in order to detect patterns of incidents and 'hot spots' on the railway/metro system infrastructure.

(3) The analysis should be performed offline.

(4) Running incident analytics should not affect ICMT performance and response times.

3.9.5.2 Service analytics

(1) Enabling analysing the level of service of service-oriented activities, incident activities and traffic restoration.

(2) The analysis of the level of service should be based on the period of time that elapses until the problem is resolved, taking into account all the factors involved.

(3) The analysis should be performed offline.

(4) Running service analytics should not affect ICMT performance and response times.

(5) Service analytics should be used for evaluation of Reliability, Availability and Maintainability (RAM) requirements as well.

3.10 Interfaces with sub-systems

Interfaces with sub-systems provide the ICMT with two main functionalities:

(1) **Event monitoring.** Monitoring events from the sub-systems and displaying them in the operator's user interface as alerts which may develop into incidents depending on the sub-system and nature of the alert.

(2) **Business process / workflow.** Through the interfaces with the sub-systems and a rule-based engine, the ICMT can realise business processes via automatic or semi-automatic workflows, such as:

When alert A_n is received from system S_n, device D_n, function F_n

As an example: When a 'fire detection' alert is received from the 'fire detection system (FLSS)', activates the 'display a live picture' function of camera X, which is part of the video surveillance system.

In the context of cyber-physical threats, when the SIEM system identifies an attack on the trackside S&TC systems, such as point machine/switch, a pre-set of the Pan Tilt Zoom (PTZ) camera of the relevant device can be activated in order to see whether it is being manipulated.

(3) **One unified and simplified user interface.** Realising the interfaces via the ICMT enables monitoring and operation of a large number of sub-systems using a single user interface that simplifies the monitoring function and operation of the different systems for the operator's benefit.

3.10.1 Video surveillance and recording system

The ICMT system should support the following functionalities for the interfaces with the Video Surveillance System (VSS):

(1) The ICMT should have an embedded Video Management System (VMS) module and Video Recording and Playback module, which enable supporting all API functions provided by the VSS software provider.

(2) The VMS and recording functions should be applicable for stationary cameras (fixed and PTZ cameras installed in the Railway / Metro system assets) and for the On-board VSS (the VSS installed onboard the rolling stock).

(3) The ICMT and VSS interface should provide the capability to manage and control VSS cameras, video matrix and video wall display, and to operate according to camera pre-sets and Video Analytics (VA), in association with an event.

(4) The ICMT and VSS interface should provide the tools and facilities to manage and control video recording and playback with the use of VA, according to predefined workflows.

(5) The ICMT should provide the facilities and embedded tools to integrate and execute workflows to include the following:

a. Cameras pre-set by a security related device (e.g. Access Control System (ACS), Burglar Alarm System (BAS), Perimeter Intrusion Detection (PID).

b. Cameras pre-set by a safety related device (e.g. fire and smoke detector, heat detector, blue light phone, etc.).

c. Cameras pre-set by a passenger related system (e.g. help point, fare collection system, etc.)

(6) Display and manage live and recorded video based on predefined workflows and rules, including multiple opened video views on the ICMT workstation and on the VWD (Video Wall Display).

(7) Display live and recorded video from single or multiple cameras on the VWD, including simultaneous display of multiple video matrices on multiple screens and digital zoom In, zoom out, pan, drag & drop, PIP of displayed video with different screen divisions (e.g. 1, 2, 4, 8, 16, etc.).

(8) VSS VA discovery module, to automatically recognise sensors and scenarios associated with video monitors routing and settings, VSS camera pre-sets, VSS camera virtual tours and video favourites; search capabilities enabling users to quickly and easily locate any camera connected to the system; and the ability to create and launch virtual tours, automatically or on-demand.

(9) HMI/GUI interactive map layers.

(10) Maintain the last video display matrix setup and return to it following an initiated change in the setup, operator's command (e.g. 'Home' button selection) or a workflow.

(11) Display protected zones and polygons' confined areas.

(12) Allocate a PTZ camera for defined display settings, upon receipt of an alert generated by a sensor, subsystem or external database, based on user settings or a workflow.

(13) Indication of geographical information regarding the video footage displayed in the ICMT and GIS mapping tools – active cameras (in display), information layers and information from the alerting sensor.

(14) Indication of the mode of the video display stream – live or recorded.

(15) Definition of individual video sources according to their supported logical functionality.

(16) Support mobile video sources (smartphones, tablets, drones, etc.).

(17) Control camera operations from the map layers (e.g. CAD, JPEG, GIS) view, and provide a software PTZ controller for controlling all integrated PTZ enabled cameras and controlling PTZ cameras, using a joystick.

(18) The PTZ software controller should enable full control and operation of a PTZ camera using a standard mouse, enabling the following functionalities:

a. Scrolling – for typical zoom-in and zoom-out functions, using the scroller for:

- Scroll up – zoom in.
- Scroll down – zoom out.

b. Right click and move – move PTZ camera in all directions.

(19) Open/close all VSS cameras in a specific geographic or logical zone and provide a "panoramic" view of an environment by opening all surrounding cameras adjacent to a particular camera with a single click; enable users to display zones related video favourites.

(20) Select a location on a map and automatically bring up video feeds from the cameras that have visibility of the selected location, and easily slave supported cameras to targets, such as those detected by perimeter protection technologies, to enable the users to continuously track moving targets visually; video pursuit capability enabling users to easily track moving objects or people in real time by opening the selected adjacent camera, as the object or person moves out of camera view.

(21) Define camera FOV (Field of View) optimal range and show or hide the FOV on a map for a particular camera, or for all cameras on a map.

(22) Provide the following functionalities for the interfaces of the VMS with the GIS mapping service capabilities:

a. View a particular area by selecting a specific camera or several cameras by clicking an area on the graphical map which is covered by one or more cameras.

b. Select a multi-camera view by drawing a polygon on graphical map.

(23) The ICMT should interface to the Network Video Recording (NVR) module of the VSS and provide the following capabilities, facilities and tools:

a. Save and export video surveillance footage recorded for post-event distribution and analysis, including Video Analytics.

b. Video playback functionality, such as fast forward, rewind, frame by frame, forward slow motion, forward fast motion, real-time display of one or more cameras in the matrix, resulting from an alert generated by a sensor and / or subsystem.

c. Playback of recorded video surveillance footage from one or more VSS cameras, resulting from an alert generated by a workflow, data fusion, sensor, subsystem or external database, based on user and system settings.

d. Save and recall multiple matrix favourites, automatically or on-demand; single-click ability to open and view video within context; ability to lock individual video slots and the overall display to prevent newly opened streams from replacing previously opened streams.

3.10.2 Security systems (access control, burglar alarm, perimeter intrusion, electromechanical)

3.10.2.1 Access Control System (ACS)

The ICMT should support the following functionalities for the interfaces with the Access Control System (ACS):

(1) The ICMT should have an embedded access control module which enables support of all API functions provided by the ACS software provider.

(2) The ICMT's access control management interface should be fully integrated with the rule-based engine and defined workflows.

(3) The ICMT's access control management interface should enable users to easily access the map layers for locations of access events, fully integrated with the VSS for viewing, allocate a PTZ camera to an event, playback, etc.

(4) Manage and control ACS reported events via the ACS management system in association with an event as per predefined workflow, to include VSS.

(5) Receive alerts from and control all connected ACS end devices under a single user interface, regardless of the ACS vendor; open video VSS video feeds related to a specific ACS point; query an ACS user or point, and access control events for readers and/or users; and associate access control events to the users who had triggered them.

(6) Filter/query the ACS to find the relevant access badge holders.

(7) Generate customisable access control reports, on-demand directly from the access control view; including filtering by ACS device, user, time stamp, event number, location or incident type.

(8) Support the correlation between ACS events and video recording from VSS cameras nearby.

(9) Automatic loading of readers and inputs from the ACS system, including a discovery module to probe ACSs and automatically import the badge holders and their associated photos into the system.

(10) Tools for easily placing ACS readers on the GIS map layers.

(11) Prevent duplicate logging by providing a spam filter to fuse data from several sources associated with the same event.

(12) Provide access to associated operation user's details as per access privileges.

(13) Enable users to view user badge ID photos directly from the access control view, as well as user and door access history, including filtering capabilities as per access privileges.

3.10.2.2 Burglar Alarm Systems (BAS)

The ICMT system should provide the following functionalities for the interfaces with the BAS:

(1) Manage and control BAS reported events via the BAS management system in association with an event, as per predefined workflow, to include VSS utilisation.

(2) Receive and process alerts and alarms, including an indication on the geographical map.

(3) Online indication of the status of the BAS sensors.

(4) Online indication of the status of the BAS controllers.

(5) Initiation of a workflow.

3.10.2.3 Perimeter Intrusion Detection (PID)

The ICMT system should provide the following functionalities for the interfaces with the PID system:

(1) Manage and control PID reported events via the PID management system in association with an event, as per predefined workflow, to include VSS utilisation.

(2) Receive and process alerts and alarms, including an indication of perimeter zone / section on a geographical map.

(3) Online indication of the status of the PID zone / section / sensors.

(4) Online indication of the status of the PID controllers.

(5) Initiation of a predefined workflow.

3.10.2.4 Electromechanical devices (pedestrian and vehicles gates and barriers)

The ICMT system should provide the following functionalities for the interfaces with the electro-mechanical devices (pedestrian and vehicle gates and barriers):

(1) Operation of the system via a graphic user interface that includes adapted icons, and also visual and audio indication of opening, stopping (if relevant) and closing.

(2) Indication of system malfunctions – motor and controller malfunctions.

(3) System status indication – open, closed, in motion, malfunctioning.

(4) Logging of the number of times the gates/barriers had been opened and closed and its work hours, in order to alert to the need for preventive maintenance based on the manufacturer's instructions.

3.10.3 Signalling and train control (S&TC) / AVLS)

The ICMT should interface with the S&TC. The interface should be unidirectional, supported by content filter and should provide the following functionalities as a minimum:

(1) Rolling stock / vehicle ID, driver's details (if known).

(2) Train location.

(3) Train origin and destination.

(4) Train permitted maximum speed.

(5) Train cars configuration direction of travel, final destination, actual speed.

(6) Critical malfunction incident from the S&TC, which affects traffic circulation in the railway/metro system.

(7) RSS scheduling and driver shift management roster.

(8) Other data, as may be required.

3.10.4 Railway scheduling system (RSS)

The ICMT should interface with the RSS database, as a complementary or replacement service to the S&TC interface. The interface should be unidirectional and should provide the following functionalities as a minimum:

(1) Display of the passenger trains in service and their planned location at any given time.

(2) For each passenger train, it should be possible to display the following data:

a. RU identifier.

b. Rolling stock / vehicle IDs.

c. Train configuration – Electric/Diesel Multiple Unit (EMU/DMU), locomotive, number of cars, cars configuration.

d. Train origin and final destination.

e. Train maximum permitted line speed.

f. Number of forecasted passengers (if available).

(3) For each freight train, it should be possible to display the following data:

a. FU (Freight Undertaking) identifier. Number of freight car and vehicle IDs.

b. Freight cargo characteristics – containers, bulk, HazMat (UN number), steel, automobiles, food, refrigerated containers, etc.

c. Train configuration – Locomotive or multiple locomotives, number and order of freight cars, position of HazMat in train.

d. Train origin and final destination.

e. Train maximum permitted line speed.

3.10.5 Geographic information systems (GIS)

3.10.5.1 General requirements

(1) The GIS should provide the ICMT with mapping, analytics, and data management capabilities, publish services, host layers and support OGC Web.

(2) The GIS should enable users to open a new incident in the maps view, automatically and on-demand, and associate the incident with its geographic location.

(3) The GIS should provide the tools to define a VSS camera's field of view (FOV) and show or hide the FOV on a map for a particular VSS camera, or for all cameras on a map.

(4) The ICMT should utilise the GIS to provide the sensor management module with the relevant information and functions, including viewing, activating, disabling, neutralising, managing the status of the edge devices, and providing search capabilities, to enable users to quickly and easily locate any sensor connected to the system.

(5) The GIS should be OGC and support KML as per Digital Geospatial Metadata ISO 19115, WCS, WMS.

3.10.5.2 Sub-systems representation and activation

The ICMT should provide the following capabilities related to the interface between GIS layers to sub-systems' edge devices (e.g. video cameras, smoke detectors, etc.) and mobile assets and devices (e.g. cars or personnel equipped with mobile and/or GPS devices):

(1) Create and manage virtual geo-fencing polygons or lines on the GIS map and define a set of geo-location rules (e.g. enter into, exit from, cross line, etc.) and time rules (from time, until time, time intervals, etc.) and alerts for mobile assets.

(2) Correlate between entities, incidents, alarms, alerts and zone related edge devices, to perform zone-based response operations, by implementing predefined workflows.

(3) Request a map image at any scale in a variety of image formats and provide the ability to automatically bring up or 'fly to' map views or locations relevant to events, alerts and incidents.

(4) Add visual markers to the GIS: The marker's image/icon should be customisable; the markers should have the ability to trigger a variety of automatic actions in compliance with scenarios and workflows.

(5) Provide the ability to customise sensor / controlled or monitored equipment icons over the GIS layers, to present the state of each sensor/sensor-group, mobile units, Rolling Stock AVLS; toggle labels that display the name of sensors and assets on the GIS, and add customisable labels to the GIS.

(6) Provide a common operational picture enabling information sharing between different users, and automatic synchronisation of all relevant GIS information (such as markers, zones), across all relevant OCC and RIMC workstations.

(7) Manage geo-location information received from external sources, telemetry or any device that provides geographic locations (e.g. S&TC, AVLS) and is installed in a train or in mobile devices carried by personnel.

(8) Support visual display of the historical path of the movements of chosen geo-location devices on demand.

3.10.5.3 GIS Geographic Data Layers

The presentation of geographic layers in the ICMT system should fulfil the following requirements:

(1) City maps and orthophotos, including street names, building numbers, municipal authority boundaries, etc. should be indicated.

(2) Police stations, hospitals, Fire & Rescue Services stations, Emergency Medical Services stations.

(3) Boundaries of local authorities and areas of jurisdiction.

(4) Boundaries of rail/metro infrastructure.

(5) Transport systems (public buses, metro/railway stations, etc.).

(6) OCC / RIMC and the area for which they are responsible.

(7) Stations and their surrounding area.

(8) Bridges, including access points for maintenance and emergency services.

(9) Tunnels, including access points for maintenance and emergency services.

(10) Depot, stabling area and their surrounding area.

(11) Traffic arrangements.

(12) Tracks (e.g. tracks, intersections), including access points for maintenance and emergency services.

(13) Electrical sub-stations and trackside technical rooms.

(14) Trackside equipment – point machines, etc.

(15) Overhead / 3rd rail conductor traction system and equipment.

(16) Signalling equipment – axle counters, Euro Baliese, interlocking equipment, GSM-R equipment, fixed signals, etc.

3.10.6 VoIP telephony systems

The ICMT should provide an interface to a Voice Over Internet Protocol (VoIP) telephony system, and should support built-in VoIP communication with the following capabilities:

(1) Automatic and on demand phone-to-phone dialling.

(2) Electronic phone book with search capability.

(3) Enable users to make outbound calls from the phone dialler, or to initiate a call to a user directly from a telephone icon located on a map.

(4) Initiate a workflow for automatic messaging to a single device or to a group.

3.10.7 Help points

The ICMT should provide an interface with the stations' emergency HPs function, enabling the following functionalities:

(1) Manage and control HP-triggered events, to include VSS and the video module of the URS.

(2) Receive and process HP alerts, including an indication of the location on the geographical map.

(3) Duplex communication via the intercom system at the HPs.

(4) Online indication of the status of the HP terminals.

(5) Initiation of scenario or script workflow.

3.10.8 Enterprise asset management (EAM) system

(1) The integration between the ICMT and an EAM system should allow exporting from the ICMT to the EAM system incidents associated with preventive or required maintenance, resulting from incidents occurring in the railway / metro system and managed by the ICMT. These incidents should be managed by the EAM system.

(2) Information concerning the relevant incidents should also include the incidents' severity and on their effect on railway / metro system's physical assets (infrastructure).

(3) The information transferred from the ICMT to the EAM system should include the following data, among others:

a. Identification number of the incident in the ICMT.

b. Data on the incident – incident name, location, time identifiers.

c. Effect on physical and logical assets resulting from the incident, in a manner enabling the creation of a suitable workflow in the EAM system.

d. Effect on rolling stock resulting from the incident, in a manner enabling the RU to create a suitable workflow in the EAM system.

3.10.9 Mass Notification System (MNS)

The ICMT system should include broad mass notification capabilities, to be integrated with edge devices used by the IM / RU, internal and external responding bodies and other stakeholders. These capabilities should allow the system to carry out the actions listed below during the workflows and tasks execution, among others:

(1) Definition of a group of message recipients, based on the incident characteristics.

(2) Definition of the means of communication with each recipient and group of recipients – mobile phone (audio, text message), smartphone (audio, text message, e-mail), workstation (landline phone, email).

(3) Sending messages and mass notification messages via e-mail, SMS, landline phone, smart phone (mobile devices application) and instant messaging application.

(4) Sending messages with attachments – snapshots, audio, video and geographic data.

(5) System definitions for messages allowing operators to define which messages they send, as well as when and to whom they can send them.

(6) Sending incident reports via the system, which should include the following incident fields as a minimum:

a. Local time stamp

b. Unique incident ID number

c. Incident characteristics

d. Incident location and nearest track access point

e. Incident indicators and prognosis

f. Description of the incident's consequences, criticality and priority

3.10.9.1 SMS messaging

The ICMT SMS messaging module will be part of the MNS. It should provide a built-in crisis communication mechanism, providing the following capabilities:

(1) Manually sending messages (free text or predefined messages).

(2) Automatically sending mass notification messages (free text or predefined messages).

(3) Message tracing capabilities that can be filtered by a number of parameters, such as time of creation, message sender/user, driver or message status.

(4) Initiation of a workflow for automatic messaging to a single person or a group.

3.10.9.2 E-mail messaging

The ICMT e-mail messaging module should be part of the MNS and/or an embedded module of the ICMT. It should provide a crisis communication mechanism with the following capacities:

(1) Manually sending messages (free text or predefined messages).

(2) Automatically sending mass notification messages (free text or predefined messages).

(3) Message tracing capabilities that can be filtered by a number of parameters, such as time of creation, message sender/user, driver or message status.

(4) Initiation of a workflow for automatic messaging to a single person or a group.

3.10.10 Security information & event management (SIEM)

The integration between the ICMT and the SIEM system should allow receiving information about cyber incidents that affect the safety of passengers and/or personnel, and/or the QoS on the railway/metro system, in the context of the following systems:

(1) Cyber incidents that affect the S&TC system and may potentially place the passengers' and /or personnel's safety at risk.

(2) Cyber incidents that affect power supply to the railway/metro system and to the traction power management system.

(3) Cyber incidents that affect facility management systems in stations / terminals and FLSS, which may potentially affect the safety and health of the passengers.

(4) Cyber incidents that may potentially shut down the GSM-R and mission critical radio crisis communication system.

(5) Cyber incidents that may potentially shut down data centres and control centres (e.g. OCC, RIMC).

Note: Curix (IC) and RAM[2] are SIEM solutions which can be integrated into the C-SOC in railway and metro systems, and can also be integrated with an ICMT solution.

3.10.11 Passenger information systems (passenger information display and public address systems)

3.10.11.1 Passenger information display system (PIDS)

The ICMT should allow triggering predefined messages to the PIDS, which can then be displayed on the passenger information system screen at a single site or in several sites:

(1) PIDS messages should be sent to the PIDS management system in association with an incident, as per a predefined workflow.

(2) The ICMT should support the creation of a free text message and / or select a message from a bank of messages and / or from an LOV menu message and send it to a particular station or group of stations.

3.10.11.2 Public address system

The ICMT should provide the following functionalities through an interface with the PAS:

(1) Send announcement messages to the PAS via the PAS management system in association with an incident, as per a predefined workflow.

(2) Broadcast announcements directly from the ICMT interface to a specific station / area.

3.10.12 Building Management System (BMS)

The ICMT should provide the following functionalities for the bidirectional interfaces with the BMS system:

(1) A general system status indication – in good order, local malfunctions, system-wide malfunction.

(2) Receipt of alerts of critical technical malfunctions in the following systems:

a. Lighting.

b. Heating, Ventilation and Air Conditioning (HVAC), Lifts (elevators) / escalators.

c. Drainage pumps (in locations with a high risk of flooding).

(3) Operation of specific functions in the following systems:

a. Lighting – operation of the lighting and emergency lighting systems, as required for the evacuation of passengers from a station / tunnel / bridge, taking into account legal requirements and the environmental conditions.

b. HVAC – switching off the system, changing the fresh/recycled air mix (according to functions existing in the systems), switching on the system.

c. Lifts (elevators) / escalators – defining the state of operation, to comply with legal requirements during passenger evacuation from a station.

3.10.13 Traction power management system

Using a unidirectional interface the ICMT should provide the functionality of indicating a critical fault of the traction power management system.

3.10.14 Fire life safety systems (FLSS)

The ICMT should provide the following functionalities for the unidirectional interfaces with the FLSS system:

(1) Manage and control incidents which are associated with SFDS reported incidents.

(2) Receive and process alerts and alarms, including an indication of the zone / section on a geographical map for stations, tunnels (including chambers), siding electrical sub-stations, trackside technical rooms, OCC, SCC, Depot, DCs, etc.

(3) Online indication of the status of the SFDS zone / section / location sensors.

(4) Online indication of the status of the SFDS controllers.

(5) Initiation of scenario or script workflow.

(6) Interface with facility SCADA to receive reported actions (e.g. sprinkler system, HVAC status, smoke dampers, door magnets bypass, etc.).

3.10.15 Weather alerting system

The ICMT should provide the following functionalities for the unidirectional interfaces with the weather alert system:

(1) Receiving an alert of extreme weather, based on the following categories:

a. Heavy rain.

b. Thunderstorm / lightning storm

c. Snowstorm / blizzard.

d. Strong wind.

e. Extreme cold.

f. Extreme heat.

(2) For each of the above situations, the interface should enable receiving the following data:

a. The geographic area of the alert.

b. Anticipated development of the weather condition.

c. Alert duration – date and time of its beginning and end.

d. Quantitative data of the extreme weather conditions – temperature, quantity of precipitation, wind speed, storm category, lightning activity level (LAL), anticipated flooding.

3.10.16 On-board systems

3.10.16.1 On-board video surveillance system

The ICMT should support and provide the following functionalities and capabilities supporting the on-board video surveillance system for real time viewing, audio transmission, playback of and receipt of alerts from one or more cameras, according to the selection of the following:

(1) Rolling stock ID number.

(2) Rail/metro car ID number.

(3) Management and control of a specific camera or cameras over an onboard-wayside wireless communication interface in association with an event, as per a predefined workflow.

(4) Playback search capabilities of the images recorded by one or more cameras, based on metadata, including:

a. Search by rolling stock ID, vehicle ID.

b. Vehicle data.

c. Geographical and time variables (e.g. all the rail/metro cars found in a defined area between the hours X and Y).

d. By data on alerts found in the database.

(5) The ICMT should have the capability to interface on-demand to the on-board VSS via the onboard-wayside wireless communication interface.

3.10.16.2 Train Control Management System (TCMS)

(1) The ICMT should support an interface with the TCMS for reporting critical faults, potentially create an immediate safety hazard or service disruption.

(2) The interface should cover events indicated by any of the following on-board sub-systems, potentially creating an immediate risk to the safety of passengers or service disruption:

a. On-board signalling system.

b. HVAC system.

c. Traction power system.

d. Braking system.

e. Door system.

f. On-board fire detection system.

g. On-board VSS.

3.11 Mobile Devices and Web Clients

3.11.1 Mobile devices for the IM / RU staff

3.11.1.1 Mobile device – operating system and interfaces

The ICMT should provide native mobile, based on the latest and optimised technology for mobile devices. The native mobile App should provide the following functionalities:

(1) Support Commercial off the Shelf (COTS) smart-phones and tablets.

(2) Be based on a common, standardised operating system, such as Android or iOS.

(3) Interface to the IM / RU backbone communication network via an LTE / 5G (public or private) network.

(4) Fully support geo location functionalities, enabling the location of the device on standardised mapping and GIS layers in the ICMT.

(5) Support text messaging, including sending SMS and MNS messages and e-mails that are standard to the manufacturer and the operating system provider.

3.11.1.2 Video monitoring via the mobile App

The mobile application should support the following video capabilities and functionalities in mobile devices:

(1) Viewing real time video.

(2) An adaptive system, which updates the frame rate and resolution according to the network provider's level of service.

(3) The possibility to view the images transmitted from four (4) cameras at half real-time and at a resolution equal to the highest resolution that the network carrier is able to supply on the mobile device (smartphone and tablet).

(4) The ICMT mobile device user, should have the option to select a camera using the mapping tool, a matrix or other interface, which should be simple and easy to use.

3.11.1.3 Mapping / GIS functionalities

The mobile application should support the following mapping / GIS capabilities and functionalities on mobile devices:

(1) Display the railway/metro system map.

(2) Display maps of all assets of the railway/metro system – stations, tunnels, bridges, tracks, stabling areas, depots, etc.

(3) Display relevant emergency layers in the mapping / GIS tool.

(4) Display icons of the cameras on the mapping tool.

3.11.1.4 Incident visualisation

The mobile application should support viewing capabilities of information of incidents, relevant to stations, depots and line or route infrastructure.

3.11.1.5 Business process management

The mobile application should support business process management capabilities for mobile devices to support event management, including:

(1) Receiving and sending messages.

(2) Receiving tasks and sending an indication confirming task execution (acknowledgement function).

(3) Transmitting video image files.

3.11.2 Web clients

Web clients are the stakeholders in the organisation who are usually not present in the OCC / RIMC and take part in incident management via a Web application as in section 3.4.4. They are responsible for executing tasks as part of the incident response workflow, for collaboration and for communication with the operator or supervisor of the operators in the control centre.

3.12 Planning and administration tools

3.12.1 Business process management notation (BPMN) tool

We propose using BPMN 2.0 as a notation method for describing the processes referring to alerts and incidents in the SAFETY4RAILS incident related planning activities. In the context of the ICMT, the notation method is relevant for alerts and incidents.

BPMN is a standard for business process modelling, which provides a graphic notation for specifying business processes in a Business Process Diagram (BPD), based on a flowcharting technique very similar to activity diagrams in Unified Modelling Language (UML). The objective of BPMN is to support business process management, for both technical users and business users, by providing a notation that is intuitive to business users yet is able to represent complex process semantics.

The scope of BPMN includes:

- Organisational structures
- Functional breakdowns
- Data models

The elements of BPMN includes:

- Flow objects – events, activities, gateways
- Connecting objects – sequence flow, message flow, association
- Swim lanes – pool, lanes
- Artifacts – data object, group, annotation

An example of a notation method is presented in FIGURE 11 below.

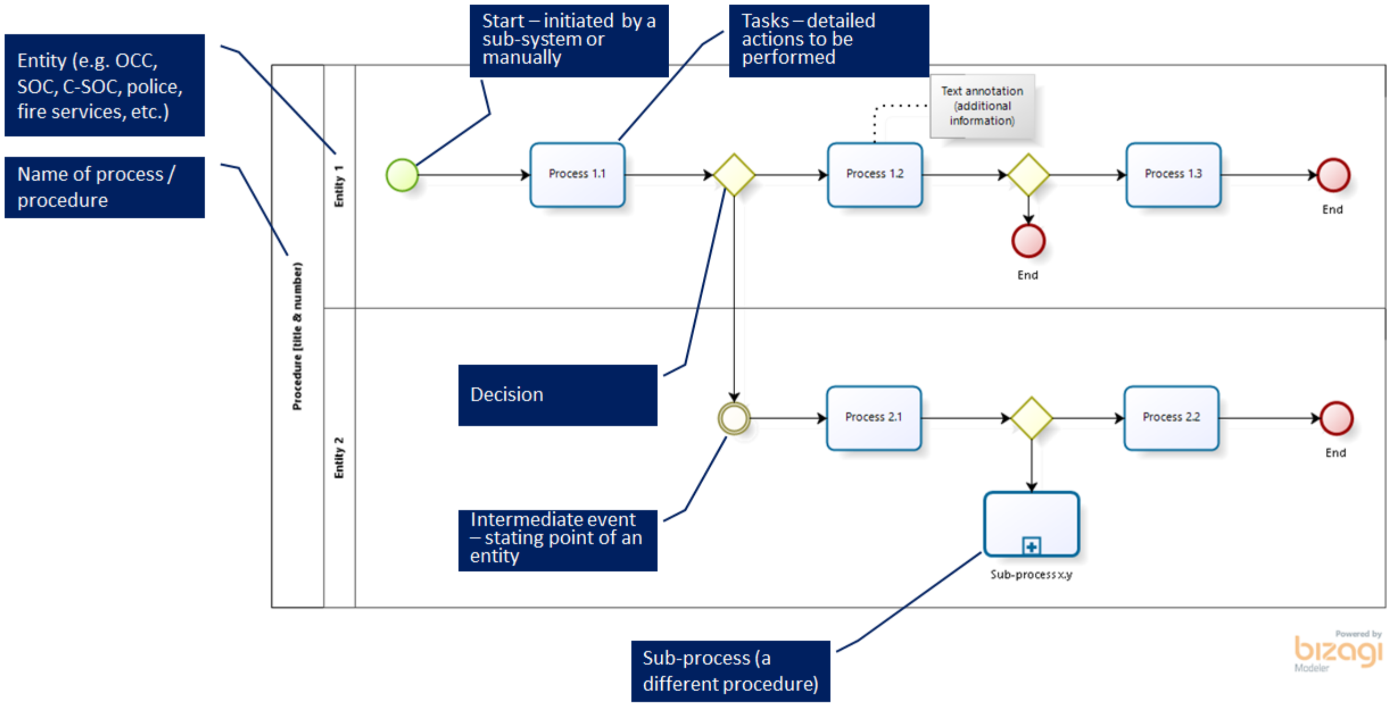

Entity (e.g. OCC, SOC, C-SOC, police, fire services, etc.)
Name of process / procedure
Start – initiated by a sub-system or manually
Tasks – detailed actions to be performed
Text annotation (additional information)
Procedure (title & number)
Entity 1
Entity 2
Process 1.1
Process 1.2
Process 1.3
End
End
Decision
Process 2.1
Process 2.2
End
Intermediate event – stating point of an entity
Sub-process x.y
Sub-process (a different procedure)
Powered by bizagi Modeler

FIGURE 11: BPMN EXAMPLE

3.12.2 Workflow planning tool

3.12.2.1 Planning tool functionalities

The ICMT incident planning tool should support the following functionalities:

(1) Define workflows that will ensure that incidents will be handled consistently and safely, including predefined tasks that will be presented to the users in run time.

(2) Define automatic workflows and tasks that execute various actions when they are reached at run time. The ICMT should enable multiple actions, including sending messages, displaying video, popping up pre-configured GIS map views, adjusting incident details (such as raising the severity or modifying its name, for example) and more.

(3) Associate predefined forms and attachments with incident types, procedures and tasks at planning time, for use while handling an incident in run time.

(4) Define task escalation triggers so that, in run time, escalation will take place if a task is not completed within a predefined period of time. In such a case, incident response managers should be able to define the various actions that will take place, such as raising incident severity, moving it up in the hierarchy, re-assigning it to someone else, etc.

(5) Define conditional workflows with branching options. At run time, these tasks will present the pre-configured options to the users. Procedures and response plans will change dynamically at run time, according to users' selections.

(6) Define or modify each workflow only once, even though it may be applicable to and launched in many cases. It should be possible to define 'procedure call' tasks that initiate the execution of another procedure into action.

(7) Assign tasks to a 'special' predefined group of job titles so that the first person who completes the task completes it for all.

(8) Configure 'quick launch' options according to the enterprise required workflows (procedures), including default categories per workstation.

(9) Enable users to export, save and print out the entire procedure book.

3.12.2.2 BPM planning tool

The ICMT should include embedded COTS business process modelling and planning tool and notations, supporting the following functionalities and capacities for planners:

(1) User-friendly visual tool for creating response workflows (procedures, business processes) offline, which are then activated and presented automatically or on-demand (during run time). This tool should have a graphic environment that enables designing complex, yet easy to build business processes (workflows).

(2) The GUI should support standard notation (e.g., flow charts, BPMN), where steps and actions can be dragged and dropped into the canvas in order to design the business process.

(3) Provide the ability to define activation rules based upon a wide array of parameters enabling complete flexibility and customisation.

(4) GUI to define the different stakeholders within the owner's and the operator's organisations (participants in the workflow), including those who use Web and mobile clients.

(5) Conditional definition of different branching steps, parallel activities, intermediate workflows, events, actions, timers, start, if-then-else steps, end, etc.

(6) Define sub-processes and workflows associated with the main workflow.

(7) Associate attachments with incident types and procedures.

(8) Specify escalation policies per incident type.

(9) Activate different actions according to the task status.

(10) Export the entire procedures book.

(11) Upload any icon set to an icon repository, including customised icon display behaviour through rule-based configurations.

(12) Support OLAP and database / data warehouse cubes tools.

3.12.3 Reusable Modules (ReMos) concept

Some operational and technical workflows which are relevant for a particular incident, based on its characteristics and the incident response phase, are also relevant for various other incidents. We call these workflows Reusable Modules, or ReMos.

The activation of ReMos is determined by the advance planning of the incident and by dynamic variables, according to the incident definitions in the intake form.

When we define or change parameters in the intake form, we activate a specific ReMo, for example:

- When we indicate in the intake form that there are casualties → we will activate the 'incident casualties' ReMo.
- When we define an operational change/adjustment in the system, which results from an incident (for example, train stopping, single line of operation) → we will activate the relevant operational ReMo in the specific section of the line.

The use of Reusable Modules is a huge advantage as it enables us to easily maintain and develop the business processes and workflows during operation, because any adjustment only requires updating a single workflow in the database.

We have classified the ReMos for responding to emergencies and crisis/disasters in the railway / metro system into five categories, as detailed below:

(1) **Group 1 - Sub-system alerts.** The objective of the ReMos in this group is the workflow for handling a sub-system alert, including a protocol verifying the alert and its classification (real alert, false alert, malfunction).

(2) **Group 2 - Immediate actions group.**

This group is relevant for all the immediate actions taken by off-site control centres in coordination with the immediate actions taken on site. It includes, for example, actions executed in sub-systems, evacuation management, attending to casualties of incidents, crisis communication with the public, dissemination of messages, traction power (electricity) cut-off and isolated, cyber security mitigation actions, coordination of the entry of vehicles and/or pedestrians into the track, ad-hoc maintenance actions, evidence gathering and investigation.

(3) **Group 3 - Train movement and operational modes ReMos group.**

This group includes the actions that the OCC implements to manage traffic due to the effects of the incident. It includes, for example, stopping traffic in a line / area / system, reducing speed, initiating degraded mode operation, single line operation, skipping a station, fall back operation and more.

(4) **Group 4 - Incident resolution and aftercare group.**

This group includes all the actions required to resume routine operation, as well as welfare support during the course of the incident. It constitutes a continuation of the immediate actions described in point (2) above, and includes, for example, traffic restoration activities, welfare support for passengers and staff, IM/RU support provided to external bodies investigating the incident, announcement of incident conclusion and more.

(5) **Group 5 - CMG (Crisis Management Group) establishment.** This group includes all the organisational and logistical processes associated with the establishment of a crisis room, when an incident is defined as a disaster, and its handling requires the involvement of a CMG.

Figure 12 depicts the realisation of the ReMo method, and the connection between the ReMos and the incident characteristics in the intake form.

On the vertical axis, the relevant ReMo groups are indicated – immediate actions, train movement / operation mode, incident resolution and aftercare, and CMG establishment. On the horizontal axis, the incident phases are indicated – immediate actions, incident handling, incident recovery, and incident conclusion. In any specific incident, we include fixed ReMos in the pre-set definition, according to the incident characteristics. In the diagram, they are shown as dark-coloured rectangles. Conditional ReMos are shown as light-coloured rectangles. The top part of the diagram includes an example of the indicator components in the incident form, and when an incident with casualties is defined in this part of the form, requiring adjustments in the operation method of the railway/metro system and evacuation, the relevant ReMos – casualties, stranded train, degraded mode and evacuation – are activated.

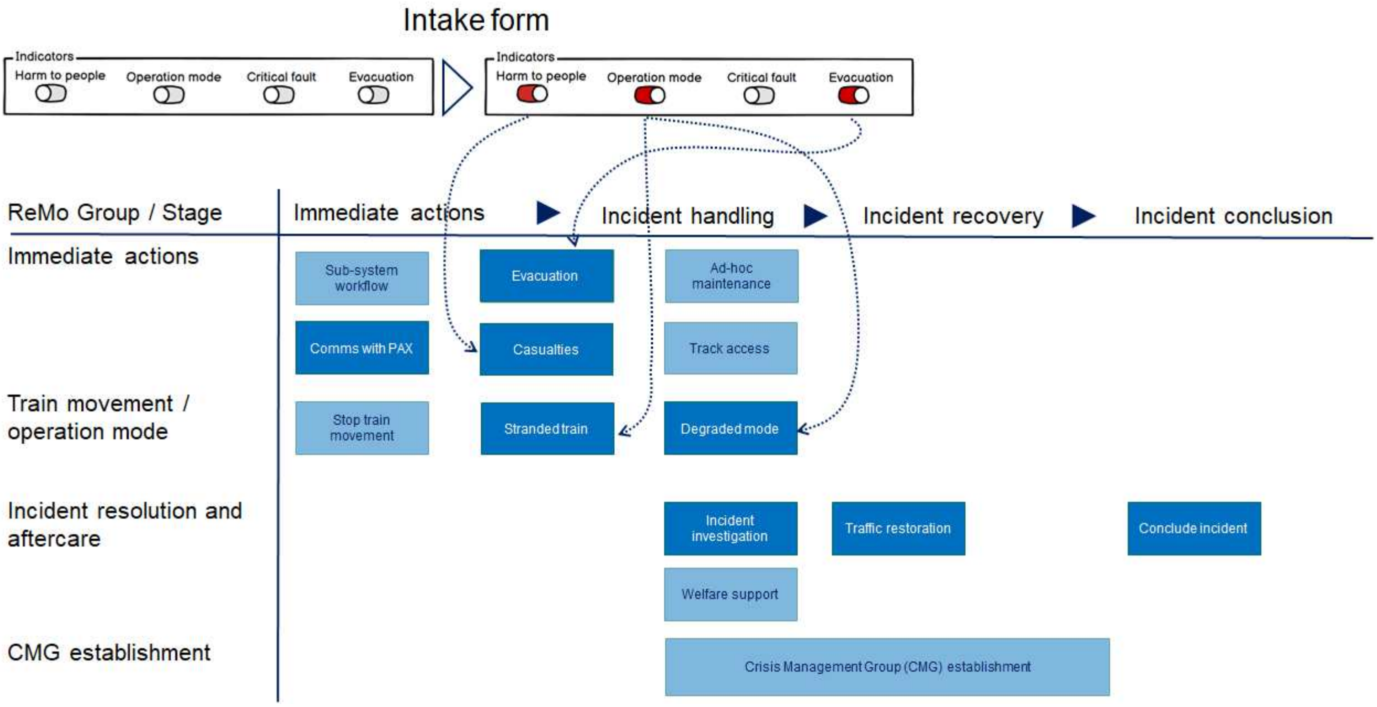


FIGURE 12: REMO CONCEPT IMPLEMENTATION

3.13 Emergency and crisis exercise tool

3.13.1 Management of emergency / crisis exercises

The ICMT should provide the capacity to manage emergency / crisis exercises through an exercise generator module that assists the trainer to manage the exercise.

(1) The exercise generator should integrate all the scenarios in an exercise.

(2) The exercise generator should include all the exercises that are managed by local generators, for all the control rooms and all the operators.

(3) The exercise generator fields and parameters should display the full range of possible scenarios for trainees to the trainer conducting the exercise, and should incorporate additional relevant parameters, including:

a. Exercise identifiers – system, exercise name, stage of the exercise, exercise participant (entity, control room, position), exercise date.

b. Incident identifiers – ID, exercise participant, time of simulation, simulation process, details of the simulation for the participating party.

c. An indication whether the exercise participant has received the incident simulation, the time of receipt, the receiving entity.

d. The progression of the incident in the local generator via a progress bar:

- An indication of all the actions that were executed through the local generator, in relation to all the actions in the same generator's exercise.
- An indication of all the actions that were executed in all the generators, and of all the actions in the exercise of all the generators.

3.13.2 Assessment tools

The ICMT should provide assessment tools and support the operator’s actions via the following capacities:

(1) Recording of the operator's workstations screen (operator’s business process).

(2) Assessment of the operator’s actions (business processes) by time and order of actions.

(3) Assessment of the operator’s knowledge by embedding questions into the business process.

(4) Assessment of decision making – incident classification for manually chosen incidents using the ‘quick launch’ tool.

(5) Assessment tools for hierarchical operation in the control room, for business processes where more than one operator is involved (e.g., crisis situation).

4. Safety and Security Management Platform – LDOs SC2

The SC2 platform (FIGURE 13), developed by Leonardo is based on the OODA (Observe, Orient, Decide, Act) methodology, and built upon a robust Service Oriented Architecture (SOA) and Web Services organisation. SC2, described in this chapter, is an example of the ICMT approach used in SAFETY4RAILS to increase the efficiency and effectiveness of incident handling, and can be considered as a benchmark in this respect.

SC2 is the platform designed to provide a common, constantly updated situational and operational picture for command and control, to support effective incident and crisis management and coordinate the response of all internal and external stakeholders and on-site responders.

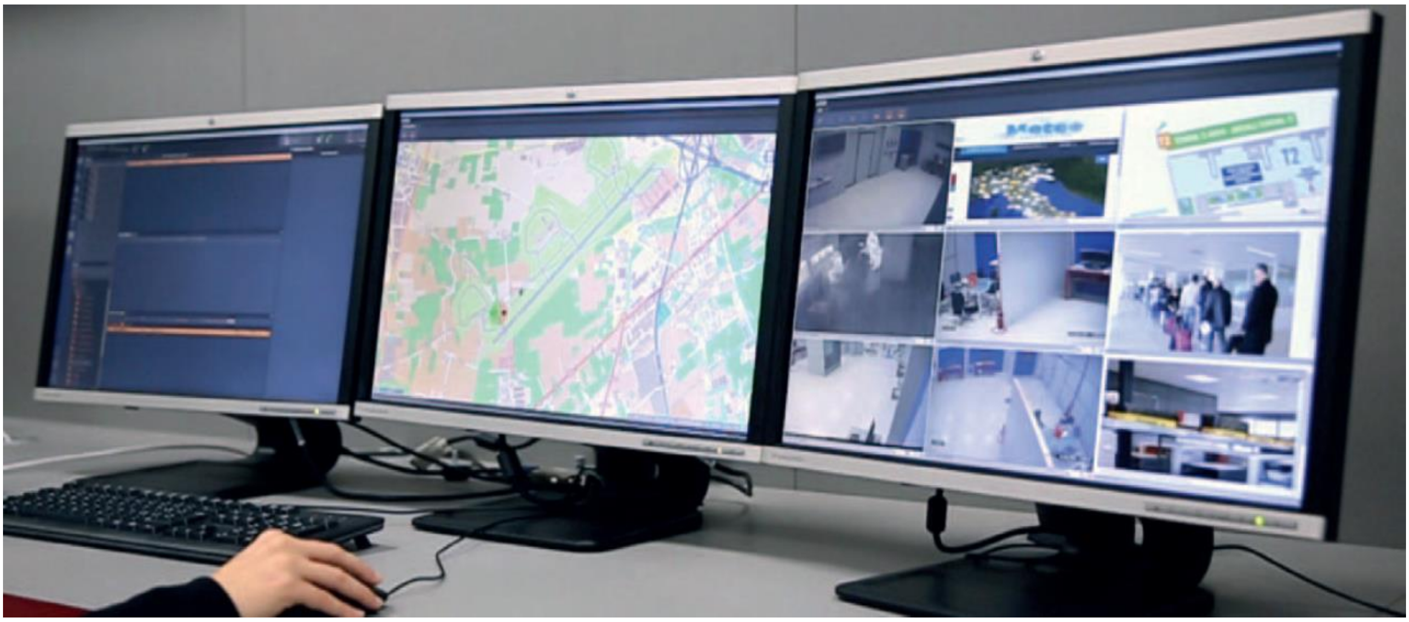


FIGURE 13 : LDO'S SC2

4.1 SC2 Key Features

4.1.1 Integration of heterogeneous systems

The core of this system integration is a comprehensive platform able to manage information from multiple sources, to provide a view of all operations on a single screen. With an integrated control centre solution, incident managers and security personnel benefit from situational awareness and can quickly assess and proactively respond to an incident, as with ICMT based on predefined business processes, before it escalates into a serious security incident. Enterprise service bus-based architecture facilitates the subsystem integration, regardless of its complexity.

4.1.2 Data acquisition and correlation

The integration of different systems and the correlation of heterogeneous information in an innovative way, providing useful support for better situational awareness, are the main features of the platform. SC2 enables collecting, normalising and correlating all relevant information from all sources and highlighting "situations" that would otherwise be difficult to detect in advance.

4.1.3 Event management

Thanks to a Complex Event Processing (CEP) rule-based engine, SC2 can define relationships between heterogeneous events generated by various subsystems, even if apparently unrelated, in order to generate new entities (e.g. assets, sub-systems and devices), new alarms (smart alarms) or identify possible false alarms. With ICMT these are then entered into the input form to set in motion the predefined business processes appropriate for the situation.

4.1.4 Workflow configuration

The workflow engine included in the platform is an extremely effective tool for the security management of critical infrastructures. Through an easy-to-use graphical interface, it is possible, for example, to introduce into the system all the encoded business processes, Standard Operating Procedures (SOPs), that are used to implement the security plan for a specific asset. The system can thus ensure that the actions executed in response to an alarm incident/event are always linked to a codified process associated with the specific incident/event.

4.1.5 Cartography and geo reference

The integrated management of cartography provides the user with a geo-referenced integrated view of all the resources and information in the system. It is thus possible to understand the situation and determine the recommended actions to carry out - predefined as in the ICMT. SC2 cartography is Geoserver based and is fully compliant with Open Geospatial Consortium (OGC) standards, such as Web Feature Service (WFS) and Web Coverage Service (WCS).

4.1.6 Communication interoperability

SC2 supplies complete integration with professional radio systems leveraging the Leonardo communications interoperability platform. Narrowband technologies (TETRA, DMR), as well as broadband technologies (Wi-Fi, LTE), can be used to exchange data with the system and coordinate on-site resources.

4.1.7 Resource management

Sophisticated resource management enables identifying, visualising, tracking and administration of sensors, cameras, radio terminals and on-site responders.

4.1.8 Federation

Multiple instances of SC2 can be hierarchically structured federations allowing alarm escalation, and, in general, more flexibility in security management.

4.1.9 Intelligent video management

Operating as an ICMT, SC2 provides native video management functions of ONVIF based cameras, including recording and investigation capabilities. A third-party video management system can be integrated as well.

Either on the camera or on the server, video analytics capabilities are included in the system, with the possibility to implement a number of algorithms applicable to different business domains.

OCR for license plate number recognition and face recognition are examples of existing integrations.

4.1.10 Investigation

In its capacity as an ICMT, SC2 enables querying events video and information recorded in the system with a sophisticated browsing interface for post-event investigation.

4.1.11 Enterprise data management

Data and multimedia contents can be securely exchanged through the integration of a secure data management function that can trigger events and be part of a SC2 workflow, increasing operational efficiency and effectiveness.

4.1.12 Visualisation and user interface (UI) presentation

The presentation layer is entirely based on Web technologies, guaranteeing greater simplicity in the distribution of applications, and above all, the capability to render accessibility to all content more flexible. The typical client configuration includes three monitor workstations, but videowall, tablet and flat multitouch monitor (tactical table). Client configurations are available as well.

4.2 Application Domains

The SC2 platform provides a flexible solution to the security requirements of different domains through a unified answer to the need for:

(1) Sensors and subsystems management.

(2) Sophisticated events and alarms management.

(3) Enhanced situation awareness.

(4) Automation in response.

(5) Workforce coordination.

SC2 flexibility allows different types of installation, including deployable and mobile configurations.

HA (High Availability) characteristics may be exploited using software redundancies and virtual architecture features.

SC2 constitutes a valuable tool for the security of:

(1) Critical national infrastructures (ports, airports, railways).

(2) Energy and utilities.

(3) Enhanced situation awareness.

(4) Cities and territories.

(5) Major events.

5. Use-cases

The following use-cases are provided to assist, as in Section 2.1.4, the process of planning for incidents, hence risks, that could affect safety, operations and security. As such, they represent circumstances where the solutions provided by SAFETY4RAILS could be applied. The list is based on MTRS's experience as a subject matter expert in previous projects, also involving RUs and IMs on actual response planning and incident management.

5.1 Safety, Operational, Natural Disasters and Critical Faults Incidents

5.1.1 Collision involving rolling stock and derailment

(1) Collision with a person

(2) Suicides / attempted suicide of persons on the tracks

(3) Collision with a vehicle (bicycle or motorcycle, small / large vehicle)

(4) Collision with another train

(5) Collision with an infrastructure element

(6) Collision resulting from excessive impact in coupling vehicles

(7) Derailment

(8) Third party vehicle collision with rail infrastructure

(9) Fire or other incident in an adjacent area/building, which may affect operations

5.1.2 Interference with operations, disruption and stranded train / maintenance vehicle

(1) Assistance to passengers, emergency medical assistance, passenger health issue.

(2) Logistical problem - employees transportation to work, provision of food and water, sanitary issues in welfare facilities

(3) Object on / near track

(4) Passenger train (powered, loss of power, with / without voice contact)

(5) Non-passenger train (powered, loss of power), Maintenance vehicle

5.1.3 Natural disasters and severe weather conditions

(1) Earthquake

(2) Tsunami

(3) High water / flooding / heavy rain

(4) Earth slips / mud slides

(5) Heavy snow

(6) Strong wind / lightning

(7) Extreme cold temperatures

(8) Extreme high temperatures

5.1.4 Fire, including arson

(1) Fire or smoke alert in a station

(2) Fire or smoke alert onboard rolling stock - at-grade, tunnel, station

(3) Fire or smoke alert in a tunnel

(4) Fire or smoke alert in an electrical sub-station / technical room

(5) Fire or smoke alert in a depot

(6) Fire or smoke alert in a stabling area

(7) Fire or smoke alert in the OCC

(8) Lineside fires

(9) Fire or smoke alert in other rail property

5.1.5 Abnormal congestion (overcrowding)

(1) In stations

(2) Onboard trains

5.1.6 Infrastructure failure (Critical Faults)

(1) Signalling and Train Control (S&TC)

(2) Track equipment, bridges, culverts, etc.

(3) Landline and Wireless Communication Networks

(4) Information Management Systems (Control Centres Applications)

(5) Traction Power & Power Distribution

(6) Fire & Life Safety Systems

(7) Tunnel & Stations Electro-mechanical Systems

(8) Passenger Related Systems

(9) Building Systems

(10) Rolling Stock

5.1.7 Safety accidents

(1) Electrocution

(2) Falling from a height

(3) Being struck by mechanical equipment

(4) Accident between road vehicles in rail facilities

(5) Road accident

5.2 Security Incidents

5.2.1 Offences against persons and/or property

(1) Theft without assault

(2) Behavioural and public disorder offences

(3) Assault with physical violence and/or theft

(4) Attack with non-lethal means

(5) Violence from groups – gang fights, mass demonstrations, riots

(6) Assault with weapon – injury or fatality

(7) Vandalism

(8) Graffiti

(9) Burglary

(10) Interfering with signalling or power equipment

(11) Arson

(12) Throwing objects at trains

5.2.2 Illegal activities

(1) Consuming illegal substances, illegal sales, sale of counterfeit tickets, drug trafficking

(2) Trespassing

(3) Intrusion into secured facility / room

(4) Access violation into secured facility / room

5.2.3 Misuse of safety and passenger related systems

Misuse of safety and devices - fire extinguisher, fire break glass, Automatic Fare Collection (AFC) gates emergency opening, escalators stop push button, lift (elevator) stop/call, Help Point, Public Address, Access Control System (ACS) break glass

5.2.4 Attacks with weapons and/or explosives

(1) Hostage taking

(2) Standoff weapon / active shooter

(3) Improvised Incendiary Device (IID)

(4) Improvised Explosive Device (IED) / Person Borne IED (PBIED)

(5) Vehicle borne IED (VBIED)

5.2.5 Attack with unconventional weapons

Dispersion of toxic materials

5.2.6 Sabotage of tracks, infrastructure, power, telecom or mission critical systems

(1) Sabotage of rail track systems in order to cause train collision or derailment

(2) Deliberate sabotage of infrastructure to harm persons

5.2.7 Threats causing hindrance, with potential risk people and assets

(1) Suspicious item

(2) Suspicious person

(3) Anonymous call

5.2.8 Incidents external to the IM / RUs that affect operation

Power failure in a utility company

5.3 Cyber security incidents

5.3.1 Incidents involving computer hacking / cyber-attacks, affecting the following sub-systems

(1) Signalling & Train Control (S&TC).

(2) The power supply to the Mass Transit System and its control system (P-SCADA).

(3) Fire safety, facility management and tunnel ventilation control systems (F-SCADA).

(4) The communications of the Mass Transit operation via the radio system or wideband wireless system.

6. Conclusion

Mainline rail and metro systems include a very large number of stand-alone information systems and software platforms, which are used for monitoring, controlling and managing alerts and incidents in their operating, safety and security systems. The situation today is that most Infrastructure Managers (IMs) and Railway Undertakings (RUs) make use of the capabilities of the existing operating systems to manage incidents associated with their existing management system, without a central software platform, which would enable the management of all the incidents in all the operational environments, in a variety of applications (desktop, Web and mobile). From our knowledge and experience in working with RUs and IMS, we believe that less than 10% of the end users, and particularly the IMs and metro operators, have a central incident management application that enables collaborative and effective incident management, as described in this document.

As detailed in this document, we have identified that RUs and IMs can prepare response plans and management arrangements to respond to the various risks to safety and security that their operation may face. To support these basic needs, we have outlined the structure and content of an ideal Incident & Crisis Management Tool (ICMT) which, as a desktop, Web or mobile application, would provide an all-embracing overview and coordination of all the issues necessarily and potentially involved both on and off site in these circumstances. Use of this tool would support those involved in what are often stressful situations whilst helping ensure the most effective and safe resolution of the circumstances. It would also complement established crisis management systems, such as the Leonardo SC2 tool.

From a functional viewpoint, the ICMT supports IMs, RUs, first responders and contractors, in three main functions:

(1) **System-wide solution.** Provide a system-wide solution for real-time operational monitoring and incident management off and on site (Gold, Silver & Bronze), to ensure safe and effective incident response and railway or metro operation.

(2) **Single source for information collection and collaboration.** Optimise situational awareness with a single source of truth, pro-actively manage incidents, and enable incident planning, response and debriefing.

(3) **Collaborative and adaptive platform.** A tool suited for command and control applications, and for the use of external bodies and on-site responders, via a variety of platforms – desktop, Web and mobile, enabling information sharing and tasks execution, and adaptive to varying incident situations.

The ICMT is essentially an information management tool serving operators in operational control centres (OCC), incident management control centres, building management centres, asset management and network operation centres (NOCs), Data Centres, Cyber Security Operation Centres (Cyber SOCs) and on-site responders, for effective management of railway incidents. Through implementation of the tool, IMs and RUs will improve incident management, based on the tool capabilities in four main aspects:

(1) **Integration and automation.** The capacity to integrate a large number of systems (operational, safety, security, information and more) in one user interface, and the capacity to automatically execute tasks in sub-systems, based on the protocol of the sub-system's interface with the ICMT.

(2) **Dynamic and adaptive response workflows.** An adaptive and dynamic response to the incident, based on real-time incident data. Reusable Modules (ReMos) are used in a way that enables maintenance and straightforward adaptation of the system during its operation.

(3) **Collaboration and information sharing.** Effective collaboration (single source of truth) between internal and external stakeholders – on and off site (Gold, Silver & Bronze), with a unified and clear situational picture.

(4) **Log and debrief.** Logging of all actions enables effective incident debriefing and investigation, including KPI analysis.

Within SAFETY4RAILS the current S4RIS implementation and the collaborative architecture that connects all contributing tools together into one platform already now delivers functionalities that partially cover ICMT capabilities. Yet, not complete, S4RIS forms can be seen as a starting point to build upon a full-featured ICMT or to be integrated in one.

Future work in the context of SAFETY4RAILS and the ICMT will focus on analysing the capabilities detailed in this document and comparing them with existing information management systems, in order to evaluate any gap functionalities that must be addressed in order to enable them to effectively manage mainline and metro incidents in a variety of control centres using diverse platforms. We identify four product categories that can serve as a benchmark for the development of the capabilities described in this document. These systems include the following product categories:

(1) **PSAP (Public Safety Answering Point)** – a product category found in call centres of first responders (police, fire services, emergency medical services (EMS), through which the call centre directs the responders to the emergency incident in the field.

(2) **Physical Security Information Management (PSIM)** – a product category for managing security means, which mainly focuses on the integrative aspect of a large number of sub-systems to one HMI and enables displaying the incidents in a mapping tool and initiating workflows for handling security and safety alerts and incidents. The SC2 solution of LDO is compatible with the PSIM definition and can serve as a benchmark for the fulfilment of ICMT functionalities.

(3) **Supervisory Control and Data Acquisition (SCADA)** – a product category for monitoring, command and control of operational and industrial systems, through which one can monitor and operate multiple sub-systems for the management of traffic, building and energy systems, and of industrial processes. The SecureWings solution of WINGS is a SCADA solution, which can serve as a benchmark for the fulfilment of ICMT functionalities.

(4) **Command, Control and Communication (C3)** – military command and control systems for forces operating in the field, used to manage sub-systems and means, control and manage forces executing operations in a diverse range of areas / terrains. Both ELBIT and LDO have C3 platforms serving a variety of defence applications. They can serve as benchmarks for the fulfilment of the ICMT functionalities. These applications were not demonstrated by the partners in the various project demonstrators.

Future work is required in analysing the architecture and functionality of each of the product categories indicated above, in order to examine the suitability of the system architecture and its existing capacities, for use as a platform for the future development of the ICMT.

8. Bibliography

1. SECUR-ED (FP7 GA no. 261605), D37.1 – Emergency and Crisis Preparedness Handbook, Parts 1-3
2. RESTRAIL (FP7 GA no. 285153), D4.2 - Information, Situation Management and Decision Support Platform, Including Functional Specifications
3. SAFETY4RAILS (H2020 GA no. 883532), D1.4 – Specification of the overall technical architecture

9. Annexes

9.1 Annex I. Glossary and Acronyms

TABLE 4: GLOSSARY AND DEFINITIONS

Term	Definition
Alert	A visual and/or audio expression of an event in the information management system which indicates a risk, or information that is significant for the information management system operator in aspects relating to operation or safety.
Attack	A hostile action resulting in the injury or death of persons, or the damage or destruction of physical and/or logical governmental, public and/or private property.
Concept of Operation (CONOP)	A written document describing an overall picture of an operation or series of operations, frequently covering operational strategies, methods, principles, plans, policies, and also organisation and command structures.
Crisis / disaster	A situation, derived from natural or man-made causes, 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.
Cyber attack	Damage, unauthorised use, exploitation or destruction of electronic information by means such as viruses, worms, Trojan horses, phishing, denial of service (DoS) attacks, unauthorised access and control system attacks**.**
Cyber Security Operation Centre (C-SOC)	A command and control centre for managing cyber incidents.
Edge device	An electronic device which provides an entry point into a network.
Emergency	An unforeseen or unplanned situation that has implications on the safety of persons and assets and requires immediate attention.
Emergency Operating Procedure (EOP)	A pre-planned documented arrangement for managing or executing a set of actions in an emergency situation, to ensure the safety of people and assets, and to maintain a pre-identified level of operation and/or services.
Emergency services / First responders	The external bodies, including, but not limited to fire services, police and emergency medical units arriving on-site to provide initial services when incidents occur.
Event	An output of an actuator, edge device or sub-system of an information management system, or alternatively: A notification of a person to the information management system operator of an occurrence in the railway / metro system.
Frontline employees	Members of IM/RU, usually at stations or onboard trains, who interface directly with passengers when executing tasks related to operational arrangements.
Immediate Actions (IA)s	Pre-planned actions taken immediately by the frontline employees to address an emergency; or when an incident occurs; or when notified in advance – before the occurrence; and also actions taken by arriving emergency services or other responding bodies.
Incident	An occurrence which negatively impacts, or may negatively impact the safety of persons, and/or the method of operation, and the level of service of the railway / metro system.
Incident response plan	A plan detailing the response to an incident or an emergency situation.

Term	Definition
Information management system	An information system used to support decision-making, coordination, control, analysis and visualisation of information in a system and/or an organisation.
Lead Person (LP)	An identified qualified person appointed in an organisation and assigned responsibility for the overall on-site incident command and control of its response (may also be referred to as "Emergency Management Coordinator" or "Person in Charge – PIC").
Mission critical system	Any element of a system (equipment, process, procedure, software, etc.), the failure of which would result in the stoppage or impossibility to fulfil the main functionality (i.e. mission) of the railway / metro system in question.
Logical (IT) infrastructure	All of the hardware, software, networks, facilities, etc., that are required to develop, test, deliver, monitor, control or support IT services. The term IT infrastructure covers all the information technology, but not the associated people, processes and documentation.
Network Operations Centre (NOC)	A control centre from which operational communication networks (wired, wireless) are managed.
Operation	Operation of the railway / metro system, also covering the training of the operational personnel and the maintenance of the facilities and the rolling stock, as required for transporting passengers.
Operation Control Centre (OCC)	A general name for a facility from which the train traffic in the lines is managed.
Reusable Module (ReMo)	A response procedure that is implemented when responding to incidents and may be combined as a secondary response procedure to that of a main incident.
Risk	The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome); the effect of uncertainty on objectives (ISO 31000).
Safety	The state of being free of risk or danger (natural or accidental); being in control of recognised hazards and reducing risk of harm or damage as low as reasonably practicable. The term 'safe', when used as an attribute, encompasses all measures, actions or systems aiming to ensure the state of safety.
Safety incident	An accidental event, of internal or external causes, that is likely to lead to some negative consequences and compromise safety.
Security	The degree of protection against intentional danger, damage or loss Also: The set of means / actions through which safety is ensured, in particular against intentional threats. Thus, the term 'security' encompasses all measures, actions or systems aiming at preventing intentional threats from compromising safety.
Security incident	A deliberate act intended to harm persons, damage equipment and infrastructure, disrupt operations and compromise safety.
Security Operation Centre (SOC)	A command and control centre from which security systems are managed, security arrangements are implemented, and the response to routine and emergency security incidents are managed.
Site (of an incident)	The area in which the response to an incident is managed.
Standard Operating Procedure (SOP)	A pre-planned documented arrangement for safe and effective management of a task during routine conditions.

TABLE 5: GLOSSARY AND ACRONYMS

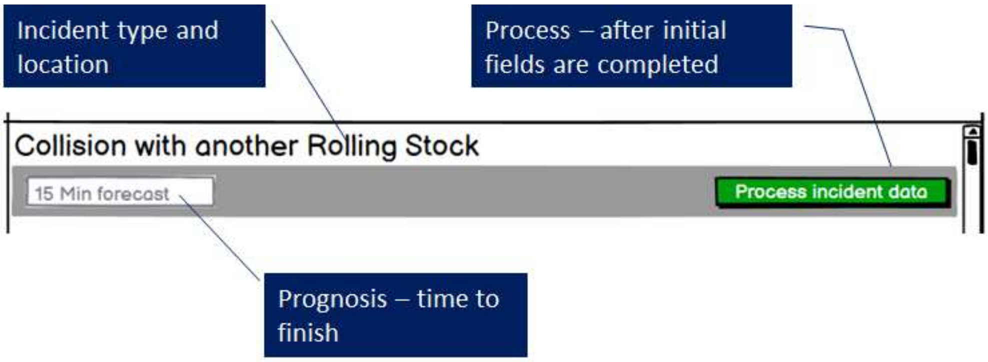
ACS	Access Control System
AFC	Automatic Fare Collection
AVLS	Automatic Vehicle Location System
BAS	Burglar Alarm System
BI	Business Intelligence
BIT	Built-In-Tests
BMS	Building Management System
BPD	Business Process Diagram
BPMN	Business Process Management Notation
CMG	Crisis Management Group
CONOP	Concept of Operation
COTS	Commercial off the Shelf
CSC	Customer Service Centre
CSOC	Cyber Security Operations Centre
DMU	Diesel Multiple Unit
DoA	Description of Action
EAM	Enterprise Asset Management (system)
EMS	Emergency Medical Services
EMU	Electrical Multiple Unit
EOP	Emergency Operating Procedure
ERP	Enterprise Resource Planning
ETA	Estimated Time of Arrival
FLSS	Fire Life Safety Systems
FOV	Field of View
F-SCADA	Facility Supervisory Control and Data Acquisition
GIS	Geographic Information System
GUI	Graphical User Interface
HP	Help Point
HSL	High Speed Line
HVAC	Heating, ventilation, air conditioning
IA	Immediate Action
ICMT	Incident and Crisis Management Tool
IED	Improvised Explosive Device
IID	Improvised Incendiary Device
IM	Infrastructure Manager
IT	Information Technology
KPI	Key Performance Indicator
LAL	Lightning Activity Level
LOV	List of Values

LP	Lead Person
MNS	Mass Notification System
MOU	Memorandum of Understanding
HD	High Definition
UHD	Ultra-High Definition
NOC	Network Operations Centre
NVR	Network Video Recorder
OCC	Operation Control Centre
OLAP	Online Analytical Processing
PAS	Public Address System
PBIED	Person Borne IED
PID	Perimeter Intrusion Detection
PIDS	Passenger Information Display System
PIS	Passenger Information System
P-SCADA	Power Supervisory Control and Data Acquisition
PTA	Public Transport Authority
PTZ	Pan Tilt Zoom
QoS	Quality of Service
RAM	Reliability Availability Maintainability
ReMo	Reusable Module
RIMC	Railway Incident Management Centre
RSS	Railway Scheduling System
RU	Railway Undertaking
S&TC	Signalling and Train Control
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information & Event Management (system)
SLA	Service Level Agreement
SOC	Security Operation Centre
SOP	Standard Operating Procedure
TCMS	Train Control Management System
UI/UX	User Interface / User Experience
UML	Unified Modelling Language
VBIED	Vehicle Borne IED
VMS	Video Management System
VoIP	Voice over IP
VSS	Video Surveillance System
VWD	Video Wall Display

9.2 Annex II. Intake Form Structure and Sub-Forms Examples

9.2.1 Intake form structure

An example of the incident heading, to include the type of incident, its location and its expected conclusion time ('time to finish').



Incident type and location

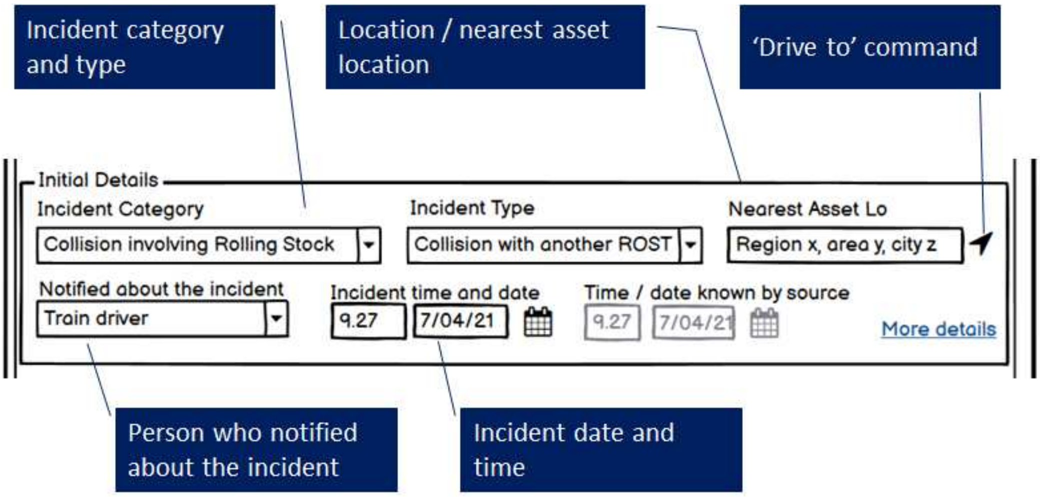
Process – after initial fields are completed

Collision with another Rolling Stock

15 Min forecast

Prognosis – time to finish

An initial detail field, with all relevant information of the incident – category, type, location, the identification of the person who had notified the incident, time and date (taken by the OCC and in real time).



Incident category and type

Location / nearest asset location

'Drive to' command

Initial Details

Incident Category: Collision involving Rolling Stock

Incident Type: Collision with another ROST

Nearest Asset Lo: Region x, area y, city z

Notified about the incident: Train driver

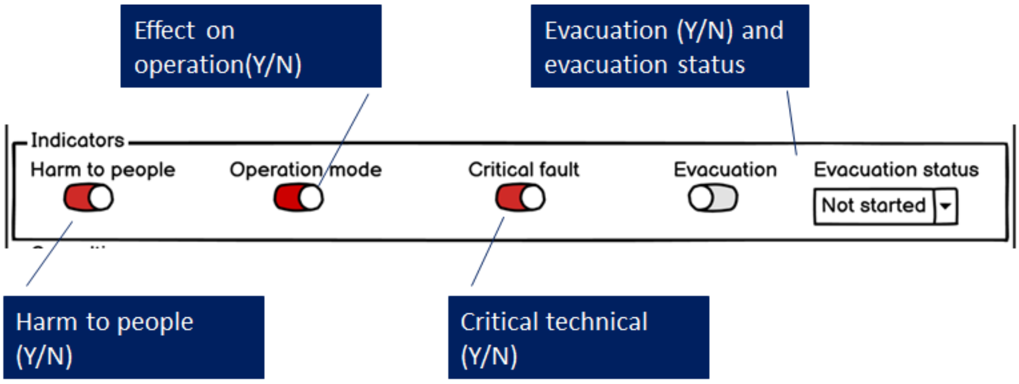
Incident time and date: 9.27 7/04/21

Time / date known by source: 9.27 7/04/21

Person who notified about the incident

Incident date and time

The key indicators of the incident, which affect incident command and control, operations and the involvement of responding bodies – harm to people, effect on operation, critical faults and evacuation.



Effect on operation(Y/N)

Evacuation (Y/N) and evacuation status

Indicators

Harm to people

Operation mode

Critical fault

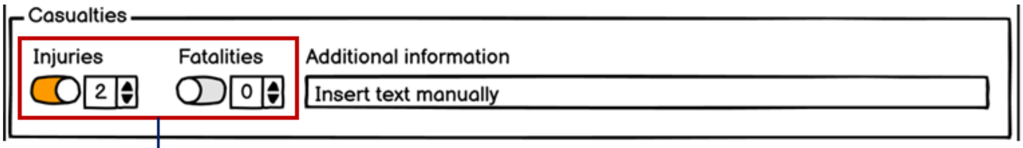
Evacuation

Evacuation status: Not started

Harm to people (Y/N)

Critical technical (Y/N)

A specific field referring to casualties, including the number of fatalities and injured persons and additional data, to support effective response by EMS.

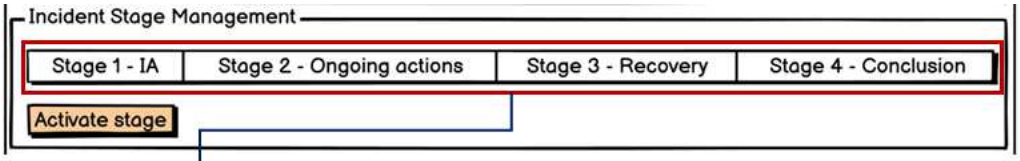


Casualties

Injuries	Fatalities	Additional information
● 2	○ 0	Insert text manually

A number > 0 here will activate the 'casualties' ReMo

Incident stage management, enabling activation of relevant workflows (ReMos), by each specific stage of the incident.

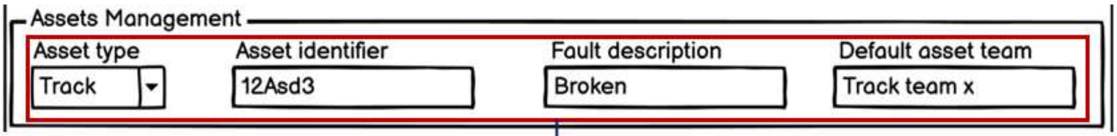


Incident Stage Management

Stage 1 - IA	Stage 2 - Ongoing actions	Stage 3 - Recovery	Stage 4 - Conclusion

Selection of stages and activation will execute the relevant pre-defied ReMos

Assets management field, indicating the affected mission critical and operational systems, including the fault specifications.

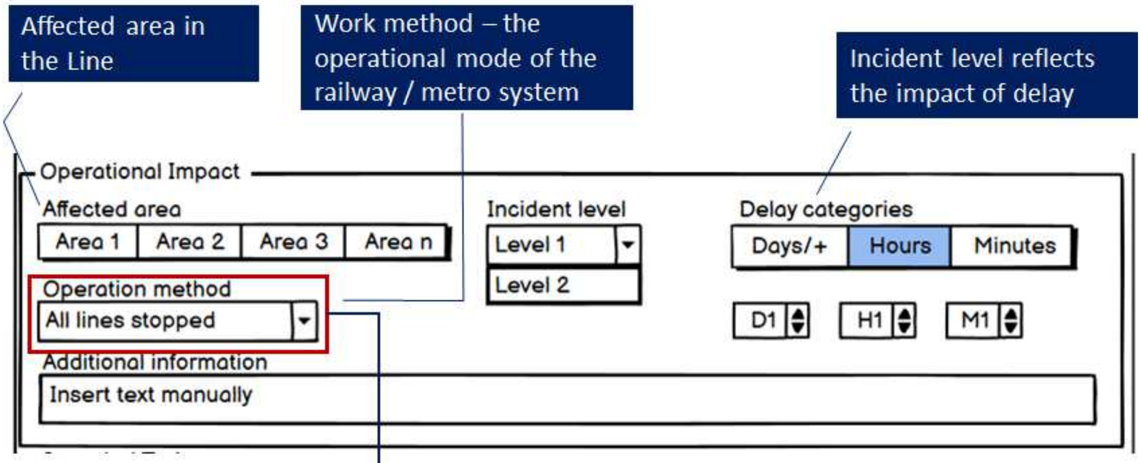


Assets Management

Asset type	Asset identifier	Fault description	Default asset team
Track	12Asd3	Broken	Track team x

The selected values will define the ad-hoc ReMos

Analysis of the operational effects on the railway/metro system and the chosen mode of operation, the severity level of the incident and the delay category, which affects the command and control arrangements.



Affected area in the Line

Work method – the operational mode of the railway / metro system

Incident level reflects the impact of delay

Operational Impact

Affected area: Area 1 | Area 2 | Area 3 | Area n

Operation method: All lines stopped

Additional information: Insert text manually

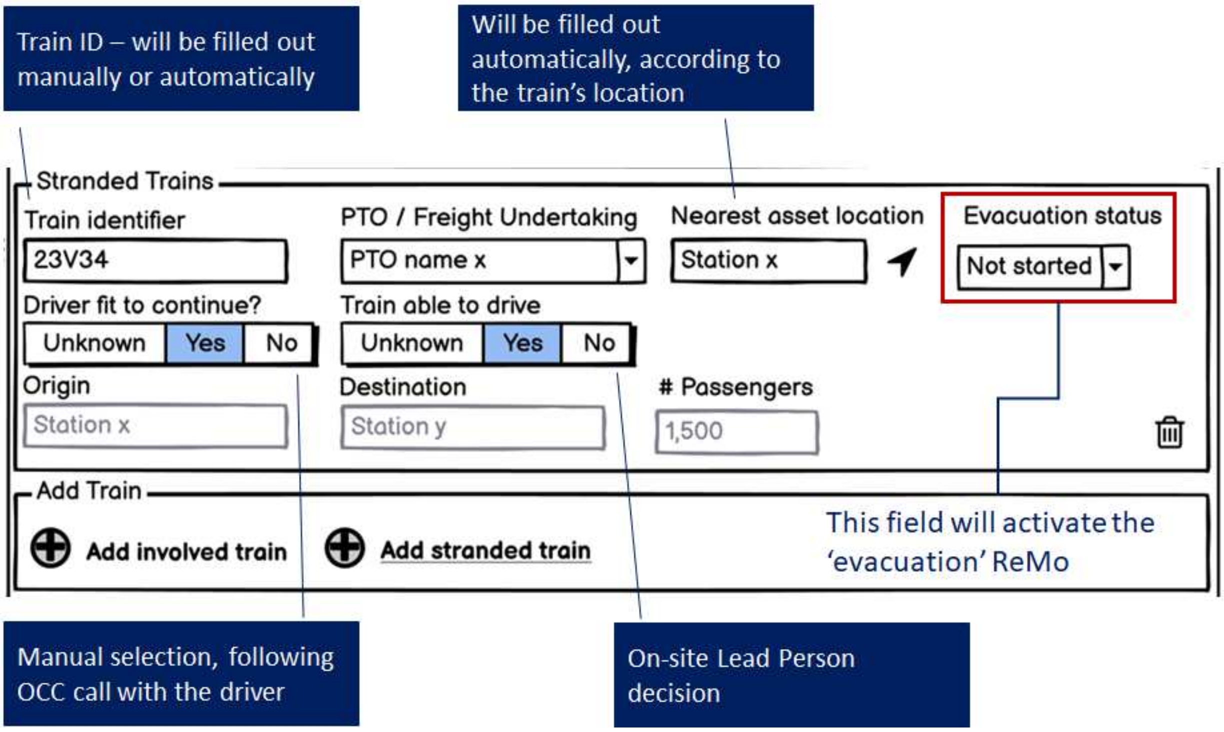
Incident level: Level 1 | Level 2

Delay categories: Days/+ | Hours | Minutes

D1 H1 M1

The selected 'work method' will activate the relevant 'train movement and operational modes' ReMo

A specific field for stranded trains with relevant details, the train' operating status and the driver's fitness to drive.



Train ID – will be filled out manually or automatically

Will be filled out automatically, according to the train's location

Stranded Trains

Train identifier: 23V34

PTO / Freight Undertaking: PTO name x

Nearest asset location: Station x

Evacuation status: Not started

Driver fit to continue? Unknown / **Yes** / No

Train able to drive: Unknown / **Yes** / No

Origin: Station x

Destination: Station y

Passengers: 1,500

Add Train

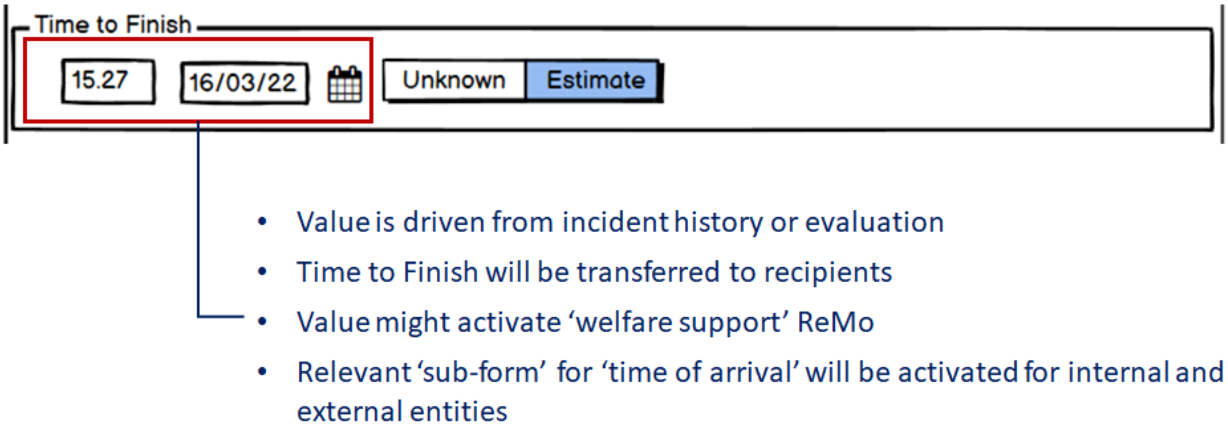
⊕ Add involved train ⊕ Add stranded train

This field will activate the 'evacuation' ReMo

Manual selection, following OCC call with the driver

On-site Lead Person decision

The incident 'prognosis' area, indicating the estimated 'time to finish' and resumption of normal or degraded operation.



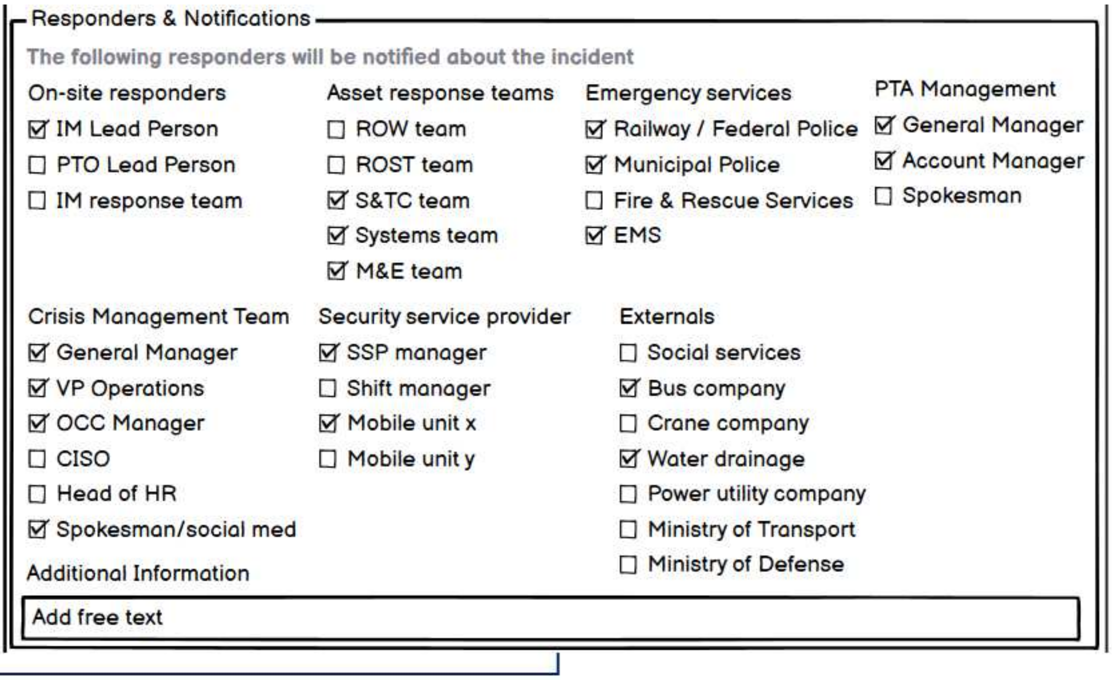
Time to Finish

15.27 16/03/22

Unknown / **Estimate**

- Value is driven from incident history or evaluation
- Time to Finish will be transferred to recipients
- Value might activate 'welfare support' ReMo
- Relevant 'sub-form' for 'time of arrival' will be activated for internal and external entities

The mass notification and reporting list, arranged by role (IM/RU / Metro driver, frontline staff, maintenance staff, management, responding bodies, contractors, externals, etc.).



Responders & Notifications

The following responders will be notified about the incident

On-site responders
☑ IM Lead Person
□ PTO Lead Person
□ IM response team

Asset response teams
□ ROW team
□ ROST team
☑ S&TC team
☑ Systems team
☑ M&E team

Emergency services
☑ Railway / Federal Police
☑ Municipal Police
□ Fire & Rescue Services
☑ EMS

PTA Management
☑ General Manager
☑ Account Manager
□ Spokesman

Crisis Management Team
☑ General Manager
☑ VP Operations
☑ OCC Manager
□ CISO
□ Head of HR
☑ Spokesman/social med

Security service provider
☑ SSP manager
□ Shift manager
☑ Mobile unit x
□ Mobile unit y

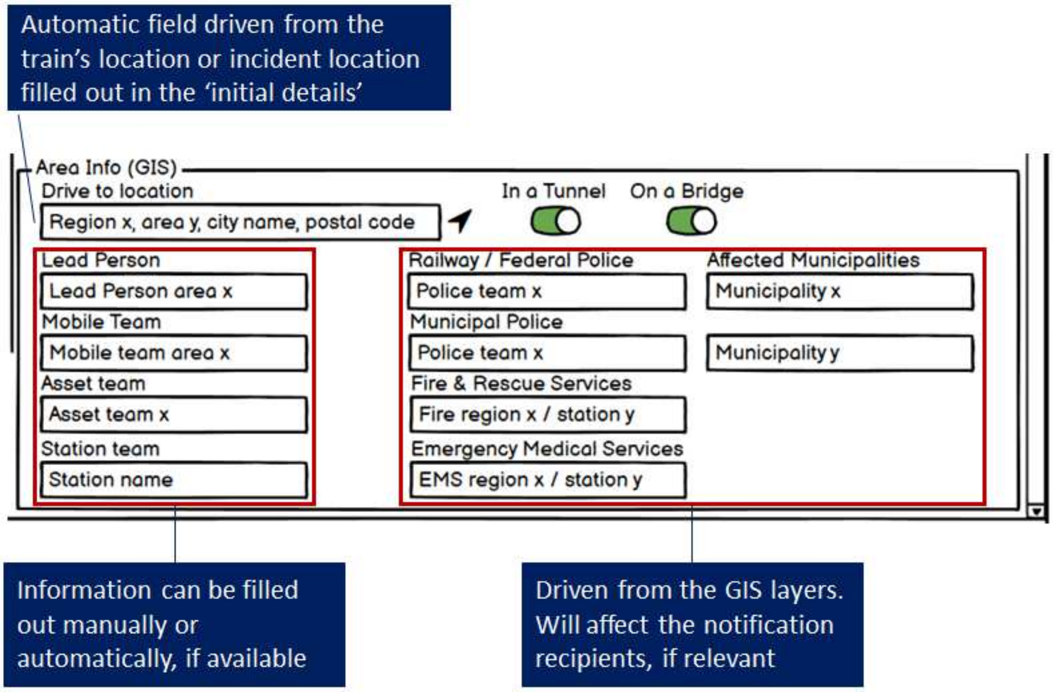
Externals
□ Social services
☑ Bus company
□ Crane company
☑ Water drainage
□ Power utility company
□ Ministry of Transport
□ Ministry of Defense

Additional Information

Add free text

- Fields affect the 'mass notification' ReMo and will be reflected in the incident message
- All recipients will be indicated automatically, according to the incident characteristics
- The operator can add recipients and free text

The geo-location related data, which determines the relevant position of holders, first responders and municipalities affected by and associated with the incident.



Automatic field driven from the train's location or incident location filled out in the 'initial details'

Area Info (GIS)

Drive to location: Region x, area y, city name, postal code

In a Tunnel ●
On a Bridge ●

Lead Person: Lead Person area x
Mobile Team: Mobile team area x
Asset team: Asset team x
Station team: Station name

Railway / Federal Police: Police team x
Municipal Police: Police team x
Fire & Rescue Services: Fire region x / station y
Emergency Medical Services: EMS region x / station y

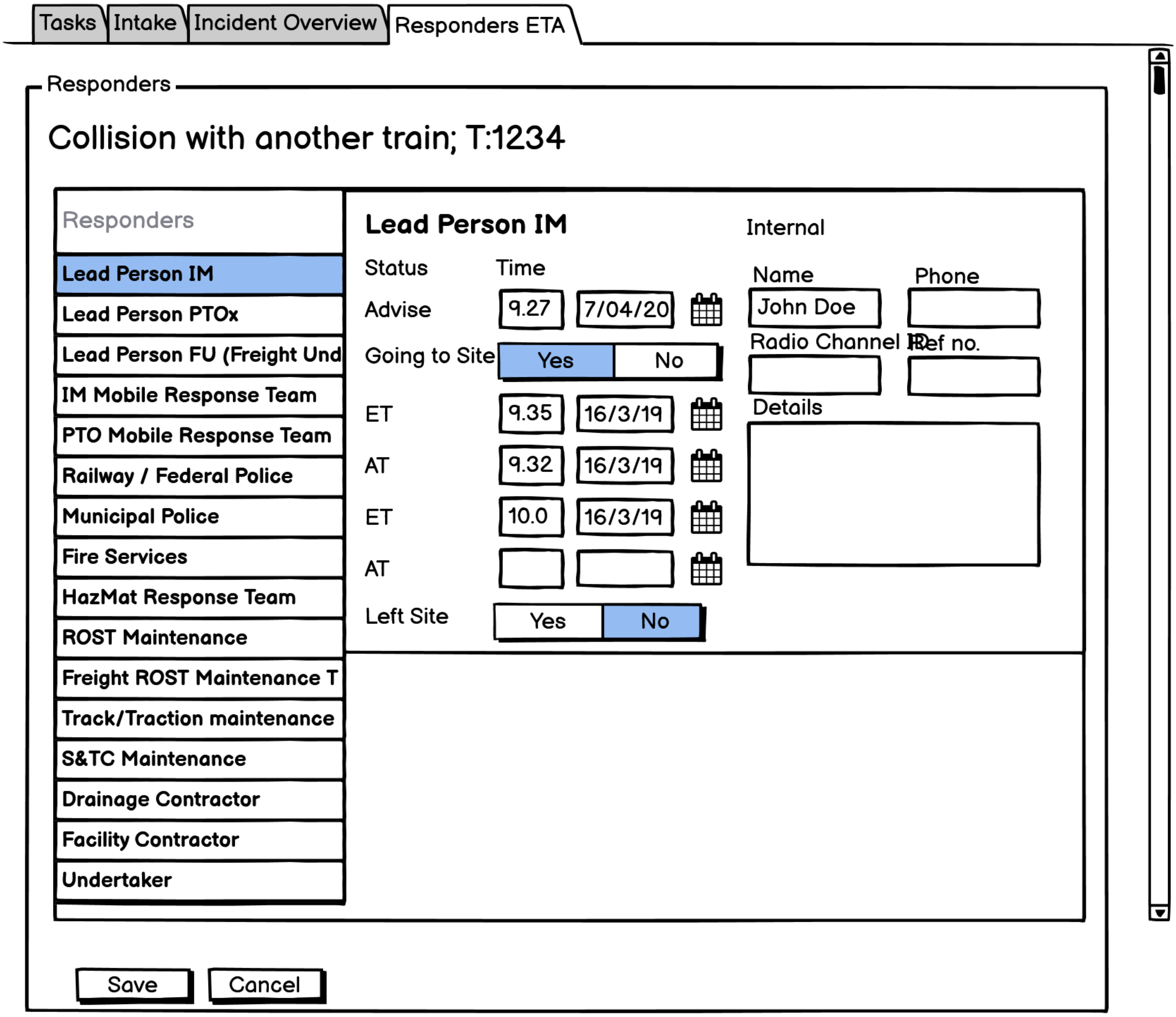
Affected Municipalities: Municipality x
Municipality y

Information can be filled out manually or automatically, if available

Driven from the GIS layers. Will affect the notification recipients, if relevant

9.2.2 Sub-forms examples

An ETA sub-form, which enables real time reporting and tracking of the on-site responding entities and their arrival time.



Responders

Collision with another train; T:1234

Responders
- Lead Person IM
- Lead Person PTOx
- Lead Person FU (Freight Und
- IM Mobile Response Team
- PTO Mobile Response Team
- Railway / Federal Police
- Municipal Police
- Fire Services
- HazMat Response Team
- ROST Maintenance
- Freight ROST Maintenance T
- Track/Traction maintenance
- S&TC Maintenance
- Drainage Contractor
- Facility Contractor
- Undertaker

Lead Person IM

Status	Time	
Advise	9.27	7/04/20
Going to Site	[✓ Yes]	No
ET	9.35	16/3/19
AT	9.32	16/3/19
ET	10.0	16/3/19
AT		
Left Site	Yes	[✓ No]

Internal

Name: John Doe

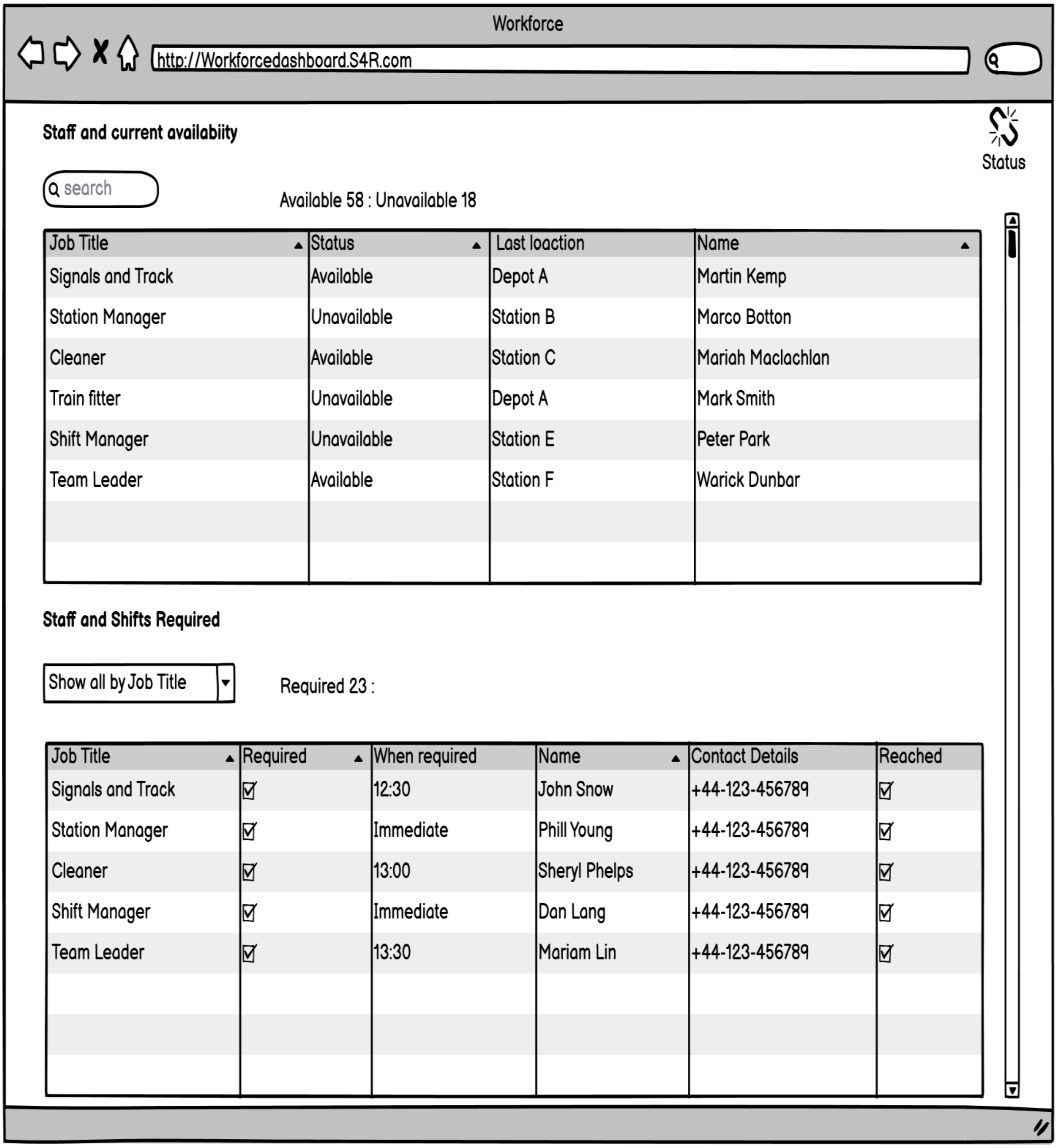
Phone:

Radio Channel ID:

Ref no.:

Details:

A workforce management sub-form, indicating the available and required personnel, according to specific competencies required, depending on the incident characteristics.



Staff and current availabiity

Available 58 : Unavailable 18

Job Title ▲	Status ▲	Last loaction	Name ▲
Signals and Track	Available	Depot A	Martin Kemp
Station Manager	Unavailable	Station B	Marco Botton
Cleaner	Available	Station C	Mariah Maclachlan
Train fitter	Unavailable	Depot A	Mark Smith
Shift Manager	Unavailable	Station E	Peter Park
Team Leader	Available	Station F	Warick Dunbar

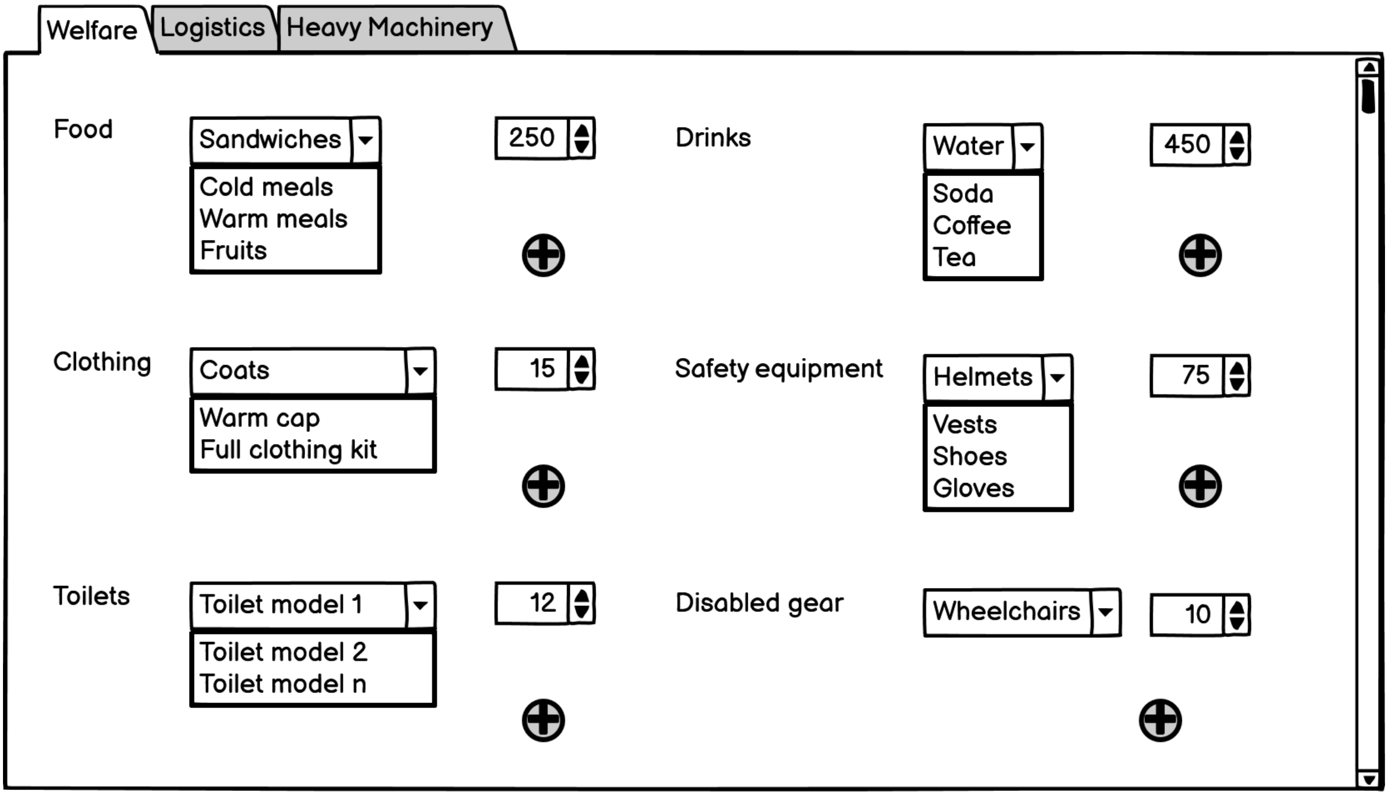
Staff and Shifts Required

Show all by Job Title ▾

Required 23 :

Job Title ▲	Required ▲	When required	Name ▲	Contact Details	Reached
Signals and Track	☑	12:30	John Snow	+44-123-456789	☑
Station Manager	☑	Immediate	Phill Young	+44-123-456789	☑
Cleaner	☑	13:00	Sheryl Phelps	+44-123-456789	☑
Shift Manager	☑	Immediate	Dan Lang	+44-123-456789	☑
Team Leader	☑	13:30	Mariam Lin	+44-123-456789	☑

Welfare and logistics sub-form, specifying the required welfare and logistical support on-site and off-site.



Food: Sandwiches, 250

Drinks: Water, 450

Clothing: Coats, 15

Safety equipment: Helmets, 75

Toilets: Toilet model 1, 12

Disabled gear: Wheelchairs, 10

SAFETY4RAILS

Partners:

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