Budget simulation module of S4RIS

Deliverable 7.3 – Public version

Lead Author: UMH

Contributors: UMH, NCSRD, ETRA, RMIT, EGO, MDM, PRO, UREAD, RFI, ELBIT, UNEW, LAU, FGC, UIC, ERARGE

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.

D7.3 Budget simulation module of S4RIS		
Deliverable number:	7.3	
Version:	3.5 Public version	
Delivery date:	13/01/2023	
Dissemination level:	PU - Public	
Nature:	Report	
Main author(s)	Nacho Díaz Castaño Fernando Miró-Llinares	Jesús Aguerri Dévica Perez
Contributor(s)		
Internal reviewer(s)	Artur Krukowski Stephen Crabbe Mohsen Moshrefzadeh Antonio De Santiago Laporte	ICOM Fraunhofer RMIT MdM
External reviewer(s)	n/a	

Document control			
Version	Date	Author(s)	Change(s)
v0.1	14/04/2021	Nacho Díaz	Methodology for the Matrix
v0.2	04/04/2022	Nacho Díaz	Matrix
V1.1	06/07/2022	Nacho Díaz	General changes
V1.2	14/07/2022	Nacho Díaz	General changes
V1.3	19/7/2022	Nacho Díaz	Content review
V2.2	28/07/2022	Nacho Díaz	Updates following partial consideration of RMIT and Fraunhofer feedback.
V3.1	29/09/2022	Nacho Díaz	Updates following partial consideration of RMIT and Fraunhofer feedback.
V3.2	07/10/2022	Stephen Crabbe	Creation of V3.2 from V3.1. Update of this table to reflect version numbering and updates. Removal of all comments in order to allow for Security Assessment before submission to EC in time for Final Project Review.
V3.3 Confidential	11/10/2022	Stephen Crabbe	Following Security Assessment, the full V3.2 planned as a Public report was re-classified as a Confidential report. In addition, section 6.1 was revised because of security concerns and there were some further minor typing corrections.
V3.4 Public	11/10/2022	Stephen Crabbe	Creation of the V3.4 Public version from the V3.3 Confidential version with redaction of content to enable the Public version.
V3.5 Public	13/01/2023	Nacho Díaz, Stephen Crabbe	Addition of new section 8 and extension of last sentence under section 9.1 in response to request for revision following project review. Update of this table, footers and minimal update to section 1.2.

DISCLAIMER AND COPYRIGHT

The information appearing in this document has been prepared in good faith and represents the views of the authors. Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authors 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 authors. Neither the authors nor the Research Executive Agency nor 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 have to ensure that mitigation steps are taken and communicated to travellers and other users. **SAFETY4RAILS will improve the handling of such events through a holistic approach.** It will analyse the cyber-physical resilience of metro and railway systems and deliver mitigation strategies for an efficient response, and, in order to remain secure given everchanging novel emerging risks, it will facilitate continuous adaptation of the SAFETY4RAILS solution; this will be validated by two rail transport operators and the results will support the re-design of the final prototype.

TABLE OF CONTENT

TABLE OF FIGURES

Executive summary

The budget simulation module identifies and classifies physical and cyber threats potentially relevant to the railway environment, generating a catalogue of phenomena associated with threats. Each threat (e.g. vandalism or explosions) has been divided into phenomena, (e.g. different acts of vandalism such as graffiti, fire, breaking of elements, or different types of explosion; in the station, in the tunnel, outside, etc). The document is structured into several threat categories, considering their nature as well as the potential sources of incidents, including physical attacks, cyber-attacks, natural hazards, physical incidents and cyber/technological incidents and data-related human error.

The phenomena have been analysed in relation to the assets of the railway infrastructure that may be affected by this phenomenon if it occurs, considering the probability of the asset being affected and the expected impact on it. The result is a two-axis matrix (phenomenon-asset) that allows the identification of the different assets that may be affected by each phenomenon and the level of damage. The matrix provides a total expected impact for each phenomenon from the expected impacts for each asset, which allows to grade all phenomena, to make comparisons between them independently of their nature (physical attacks, digital, natural catastrophes, etc.) and to select different intensities for the same threat.

The main objective of the budget simulation module is to serve as a basis for the CAMS tool by collecting and describing the profile of threats, characterised by different levels of intensity and the impact of each of these events on the assets so that the CAMS tool can subsequently analyse the costs of threats according to a specific intensity. In addition, the catalogue of phenomena serves as an input for the identification of vulnerabilities, making it possible to generate a vulnerability matrix associated with the catalogue of events (D7.2.).

1. Introduction

1.1 Overview

Estimating the costs and consequences of major disasters is a complex task, even when analysing events that have already occurred, as estimating the economic costs incurred on the assets of the affected facility requires knowledge of the size and exact location of the facilities where the event occurs and the inventory levels of existing supplies [1]. In addition to the economic costs incurred directly by the company, other types of direct costs can be incurred in relation to users, such as costs resulting from injuries and fatalities or the loss or damage to users' property. In relation to the health of users, mental health is another aspect to be taken into account and it is difficult to estimate the impact an event will have on each individual [2]. In addition to the direct costs, there are indirect costs such as loss of earnings as well as administrative costs resulting from the intervention of the administration (rescue, police investigation and legal costs). The number of assets and people affected will not only be determined by the location, inventory and occupation at the time of the event but also by the intensity of the event.

Most studies that attempt to approximate the costs of various calamities usually do so on the basis of real cases (see for example [3], although in some cases there are models of potential hazards [4, 5, 6]. Most models that analyse the economic costs of a disaster use input-output (I-O) models to estimate the economic consequences of shocks [3, 8]. I-O models describe the interdependent relationship between industries in terms of what one industry needs from another to produce its goods and services. Disruption can directly affect people's health, destroy infrastructure and property. Direct economic losses result from the reduction in final demand due to lost wages or fatalities and the rendering of facilities unusable. I-O models measure the system-wide effects of these direct losses because the directly affected industries reduce their demand for goods and services from other industries, referred to as indirect losses. Total economic losses are the sum of direct and indirect losses. I-O models are supported by extensive data collection around the world. Approximating the costs of an event that has happened or of a hypothetical scenario is complex but possible, but it is not possible to make calculations for potential events that have not been concretely defined [4, 5, 6], taking into account each of the characteristics of the event. To make this approach we would be talking about a scenario case. The effects of an explosion resulting from a terrorist attack at a particular location at a particular time would be totally different from the effects of an explosion of the same intensity at another location and/or time.

When carrying out the budgetary analysis of a simulated scenario, it is first necessary to establish the intensity of the event and the consequences of the scenario, in order to be able to measure the economic impact of these consequences. The budget module provides a basis for CAMS, establishing a broad catalogue of events and indicating the expected effects on assets for each event, through a matrix indicating the expected risk and impact for each asset for each phenomenon. Phenomena can combine with each other, generating complex scenarios. Through the budget simulation module, the different assets that would be affected by the scenario as a whole can be identified. This allows the intensity of a threat to be graded, and therefore generate concrete simulation scenarios. CAMS can associate the expected damage to assets for each phenomenon provided by the Budget Simulation Module with other data entered into the system such as the number of elements of each type present in the environment in which the simulation is generated, repair times and repair costs to perform the economic analysis. The generated matrix is therefore an input for the analysis of the costs of a threat that is carried out by the CAMS tool. In accordance with the deliverables of Work Package 7 under the leadership of RMIT, the complete system specification for the enhancement of current capabilities of CAMS for rail assets, including all the scenarios and vulnerable asset components, can be developed in D7.5.

1.2 Structure of the deliverable

This document includes the following sections:

- Section 1: This section outlines the objectives of Task 7.3 and the interrelationship of the deliverable within WP7, especially its relationship with the CAMS tool.
- Section 2: In this section, the concept of a threat profile and phenomenon concept (around which the budget simulation module revolves) are presented. The methodology used for the analysis of threats and the construction of the profile of threats and their budgetary implications, the scales used and the equations for the assessment of the phenomena are presented.

- Sections 3, 4 and 5 introduces the threat profile and the budgetary implications for, physical, natural and cyber threats, respectively. Each section shows the catalogue of phenomena associated with the different hazards in the section and the associated hazard intensity scores.
- Section 6 shows an example of the use of the methodology applied to a simulated scenario in which different phenomena are combined and the total impact of the event on the assets can be known.
- In section 7 results from the analysis of threats assets are presented and discussed, establishing the most impactful threats and the most vulnerable assets. The connection of the module matrix with the CAMS tool is discussed.
- In section 8 the budget simulation module of S4RIS as an integral part of the CAMS tool is discussed.
- In section 9 the main conclusions and future lines of work are presented.

2. Conceptualizations and methodology

2.1 Overview of profile of threats and budgetary implications

In deliverable 3.1, an extensive taxonomy of threats that can affect the railway system and metros was drawn up. However, a particular threat, such as an act of vandalism, can present very different phenomenologies (graffiti, fires, destruction of objects, obstruction, etc.) and the consequences of each of these particular forms of attack will also be different. Attacks can also be directed against different targets (e.g. attacks with explosives in the station, wagons, rails) or have different intensities (earthquakes of different magnitudes or different magnitudes of an explosion among others). Taking into account the particularities that a threat can present, they have been divided into phenomena. Each phenomenon will have a particular impact on certain assets. Depending on the number of assets likely to be affected, the impact on the asset (damaged, disabled or destroyed) and the priority of the asset for the service, each phenomenon will have a score, which makes it possible to 1) measure the intensity of an event, 2) identify the events or phenomena that pose the greatest risk to the service and 3) identify the assets that will be affected by the phenomenon and the degree to which they will be affected. This allows guiding Asset Management and budgeting strategies under extreme events. The profile of threats is therefore defined as the different possible phenomena within the threat and the budgetary consequences are conceptualised as the impact on assets for each phenomenon.

2.1 Characterization of the profile of threats and budgetary implications

In order to develop the profile of threats, the first step was to carry out a literature review to identify the main forms or phenomena that can present the same threat. The taxonomy developed in deliverable 3.1. was used as a starting point and a series of phenomena were established based on the review of the academic literature and incidents on the groups of threats in the taxonomy. Natural events such as earthquakes, wind, floods, etc. are structured and graded in the academic literature according to the intensity of the event (e.g. Ritcher scale or Beaufort scale for earthquakes and wind respectively). These threats can be measured objectively and therefore generate scales, but these scales are not comparable with each other. Other threats, such as physical or digital attacks, cannot be measured in a simple way and therefore no scales exist. An explosion will depend on the type of explosive used, the charge, the pressure, the location, the oxygen level, etc. To make a scale of explosions according to the power of the event is complex, but to make a scale from the measurement of a variable for other attacks, such as acts of vandalism, sabotage or armed attacks, is impossible, as it is the particularities of the event that shape the result. The way to identify the different phenomena of a threat that we have used is to identify frequent particularities, in order to create an extensive but parsimonious catalogue.

Depending on the threat, we have considered particularities that have been identified as relevant in the literature for that specific threat, such as the number of attackers or the type of weapon for armed assaults, or the type of target for vandalism or explossions, in order to establish the different phenomena that make up each threat. This does not, however, provide information on the intensity of the phenomenon in comparison with other phenomena. Some kind of impact measurement or estimation is necessary to compare the intensity of the different phenomena.

The full catalogue includes 228 phenomena and is presented in the subsequent sections, organized by each type of threat.

2.2 Intensity of threats and budgetary implications

Once the catalogue of phenomena was developed, it was necessary to measure their intensity in some way in order to be able to graduate the intensity of threats and associate different effects according to the different varieties and intensities they could present. The intensity of natural threats such as earthquakes or wind is widely developed and standardised in the scientific literature, however, comparisons cannot be made between hazards of different nature, e.g. the scale used to measure the intensity of an earthquake cannot be compared to the intensity of a wind storm. On the other hand, there are no intensity scales for human attacks, whether physical, such as vandalism or armed terrorist attacks, or cyber-attacks. Given the absence of objective scales to measure the intensity of threats of human origin such as different types of attacks. In this deliverable, a model has been developed that allows the intensity of an event to be graded taking into account two fundamental parameters: On the one hand, the intrinsic characteristics of the event or attack vector in the context of metro and railway networks; for this purpose, different elements found in the literature have been taken into consideration for each threat and they are represented in the catalogue of phenomena. In the case of an explosion, for example, the explosive charge or the place where the detonation occurs (in a carriage, in the station, outside, etc.) will produce a different impact of different intensity on the service. On the other hand, the assets that can potentially be affected and their relevance to the service, according to the expected impact on the railway infrastructure. For this purpose, we have developed a two-axis matrix. One axis contains the complete catalogue of phenomena, organised into threats. The other axis is made up of a list of 44 assets (see table 35) provided by EGO and organised in sections according to location (station, command centre, wagon, tracks). Each combination of phenomenon and asset is given a value for the probability that the asset will be affected or impacted by a phenomena (PI) and another value for the expected impact (EI) (see table 1 and 2). The product of both values is the risk posed by the phenomenon to the asset (individual risk value).

TABLE 1: LEVEL OF THE PROBABILITY OF PHENOMENA AFFECTING AN ASSET

0 – Impossible	For example: it is impossible or at least highly unlikely that a power failure would damage the structure of the tunnels. The possibilities of a direct impact of the threat profile have been considered and not the consequences resulting from it. For example, an object on the tracks could pose a risk of damage to the wagon and its components, even to some track elements. The train could derail as a result of such an object, causing much greater damage. This damage has not been considered in the profile of objects on the track, and therefore it has been determined that there is no possibility of impacting assets such as the CCTV, which could be affected in the event of a derailment. There is a specific profile for derailment where the potential impact of this threat profile is established, which can be a consequence of multiple profiles (explosions, objects, inadequate speed, etc.).
1 – Low	A low probability level but higher than zero. Referring back to the example of the threat of small objects on the tracks, the impact on wagon assets such as wheels is unlikely but possible. The presence of larger objects has a higher risk of affecting these assets.
2 – High	This level of probability of affecting the asset is proposed for an impact that is likely but there is a certain level of uncertainty. For example, in the case of earthquakes, structural elements are likely to be damaged, but there is considerable uncertainty.
3 – very high	At this level, impacts on assets are considered for each threat when there is a virtual certainty of impact on the asset. It should be understood that this certainty considers that the specific threat and the asset coincide in the same space, that there is a "contact". The clearest case to explain this level and the aforementioned deliberations is that of vandalism. An act of vandalism of property destruction, for example with a blunt object, can affect almost all the assets of a station, but this does not mean that all assets are affected by a single act of vandalism.

This probability should therefore not be understood as the probability of the occurrence of the phenomenon to which the probability is associated. It refers to the probability that in the event of the occurrence of the phenomenon the asset will be directly affected by that phenomenon, regardless of how probable or improbable the occurrence of the analysed phenomenon is.

TABLE 2: LEVEL OF THE IMPACT OF THE PHENOMENA ON EACH ASSET

0 - Non-Affected	The asset does not suffer directly from the threat. This level is reserved for cases where the asset has a zero probability of being affected score

1 - Minor damage	This level reflects impacts on assets that reduce their condition but are still functional or where damage is merely cosmetic. Since CAMS assesses the ageing of assets, this score is of interest for calculating the deterioration curve after an incident when the asset has not needed to be replaced.
2 - Compromised	This level refers to assets that are temporarily out of service and require minor maintenance to bring them back into operation.
3 - Severe damage	Asset needs severe repairs and replacement of parts
4 - Destruction	This level is reserved for cases where the most likely effect of the threat is the destruction of the asset making its replacement necessary.

The result is a matrix indicating the risk of each asset being affected by each phenomenon and the expected impact.

The individual risk values (IRV) are divided by 3 to keep a 5 levels scale (from 0 to 4) and then modulated by the criticallity of the asset (AC). Each AC was rated on a scale of 1 to 5 by two end-users. The scores for each asset were similar between the two samples. In case of discrepancy, the mean of the two scores was used. The sum of the Modeulated IRVs indicates the overall risk of the phenomenon for the infrastructure and takes into consideration the number of assets affected, the degree of impact and the priority of the asset. To keep the scale from 1 to 5, the values are divided by 5.

There are threats that can be directed against a wide variety of targets, e.g. graffiti or destruction of assets. This does not mean that all assets identified as susceptible to the consequences of the attack are involved in the particular event. On the contrary, there are other threats, such as explosions or fires that have the capacity to damage all identified assets in a single event. Assuming that the probability and impact of these two threats on the assets were the same (i.e., maximum probability and level of damage for the same assets), the sum of the risks of each asset would give the same score and therefore the two threats would have the same score. A threat can have events with the same intensity. This is why the sum of the modulated IRV is again modulated according to the amplitude or spectrum of the phenomenon (PS), i.e. the number of assets that can be affected in a single event of the phenomenon analysed. In this way, phenomena such as vandalism and explosions, both of which can affect almost all assets, would have different final scores, as the former will usually target a single asset per event, while the latter will affect a wide variety of assets in a single event.

TABLE 3: LEVELS FOR PHENOMENA SPECTRUM

0 - No component affected	This category is reserved forphenomena that do not directly affect any asset. For example, hostage-taking does not directly affect physical or digital assets, although it obviously has an impact on people and service and can facilitate other attacks with direct implications on assets. In this case the total score will be 0
1 - One component affected	This category refers to phenomena that normally have a single target, or a limited number of targets. For example, the graffiti sub-threat. In this case the score will be multiplied by 0,33
2 - Few components affected	This level refers to all those phenomena that will potentially affect several assets, such as a localised fire or a small flood, a landslide or most cyber-attacks. In this case the score will be multiplied by 0,66

3 - Several components affected	This category is reserved for phenomena that affect virtually all assets of a facility or the system as a whole. Examples would be a major earthquake or a large explosion. In this case the score will be multiplied by 1.

The modulated sum of each asset for each phenomenon is the overall intensity of the phenomenon (OIP). The threats intensity scale will be composed by the OIPs of each event that are part of a threat. In short: each asset has an individual risk constructed on the basis of the probability of being affected and the impact that the phenomenon would have on the asset. The value is modulated according to the importance of the asset. The sum of the individual risks modulated by the importance of the asset is again modulated according to the level of extent of the threat.

EQUATION 1: INTENISTY INDEX FOR PHENOMENA AND ASSET

$$IRV = PI * EI / 3$$

$$\text{Modulated } IRV = IRV * AC /5$$

$$OIP = \sum IRV * PS$$

The OIP scores are normalised to obtain values on a scale with homogeneous values by multiplying the OIP value by 100 and dividing by the maximum possible score, 176 (an IRV value of 4 for the 44 assets, 44*4=176).

Once the instrument was designed, two researchers were instructed on how to score the relationships between the asset and the phenomenon. In testing the results, it became apparent that, although the assets identified as likely to be affected were moderately similar between the researchers, there were statistically significant differences between the scores that each researcher had associated with risk for each phenomenon-asset pair. To overcome this problem, it was decided that three researchers would jointly establish scores using group techniques to pool the scoring criteria and obtain similar scores for each phenomenon-asset pair.

Further content in this section redacted.

The full description of this section is included in the none redacted report attached to another confidential deliverable due to security reasons.

3. Catalogue of physical attacks and their budgetary implications

Chapter redacted.

The full description of this chapter is included in the none redacted report attached to another confidential deliverable due to security reasons.

4. Profile of natural threats and their budgetary implications

4.1 Natural events

Unlike physical attacks, most natural events are measurable. Such events usually occur in a larger environment than physical attacks. An earthquake or flood will not normally occur in a localised area such as a depot or the control centre, but will affect the entire station. For this reason, we have ignored the location when setting up the case phenomena. It is possible, however, to identify the assets that will be affected by the location. The score is therefore a score assuming an overall effect on the network, but since the assets are categorised by location (station, command centre, wagon, tracks) it is possible to select the location of interest and recalculate the score.

TABLE 4: PHENOMENA FOR EARTHQUAKE THREAT AND INTENSITY SCORES

NH1	Earthquake	Score
EA1	Minor Earthquake (1-2 Richter)	0,60
EA2	Moderate Earthquake (3-4 Richter)	7,51
EA3	Severe Earthquake (5+ Richter)	28,10

The earthquake threat has been divided according to the power of the earthquakes from the Richter scale [53]. Due to the impossibility of finding differences between each of the levels of the scale, it was decided to merge some degrees, leaving 3 sub threats according to the literature of earthquake consequences [54, 55]. As the only variable in this case is intensity, the greater the intensity of the earthquake, the greater the budgetary implications. Heavy snowfall, ice storm and heavy wind phenomena are based on common meteorological classifications.

TABLE 5: PHENOMENA FOR FLOOD THREAT AND INTENSITY SCORES

FL	Flood	Score
FL1	Minor flood	1,88
FL2	Moderate flood	8,76
FL3	Major flood	27,10

Floods do not depend just on the level of rainfall or water leakage, but also on the geography of the location. They can also be caused by non-meteorological phenomena including vandalism. In order to maintain the internal coherence of this type of threat and to have a parsimonious graduation, we have decided to divide the threat profile into three phenomena, according to flood literature [56-59]: minor floods, moderate floods and major floods. The first ones refer to waterlogged areas. The latter refer to a level of flooding that makes access to the location difficult. The third level does not allow access to the location. As in the case of earthquakes, the higher the intensity, the more assets affected and the more likely they are to be damaged.

TABLE 6: PHENOMENA FOR HEAVY SNOW / ICE THREAT AND INTENSITY SCORES

NH2	**Heavy snowfall / ice**	**Score**
HS1	Extremely cold temperatures (congelation)	3,24
HS2	Severe snow	1,03
HS3	Medium ice balls (hail)	3,01
HS4	Big ice balls (hail)	6,40

Cold can affect various assets, accelerating the deterioration process and impacting on their proper functioning. Snowfall will affect in a similar way but unlike cold will only affect those assets affected in a more direct way. Hail will impact in a similar way to snow but its destructive potential is greater.

TABLE 7: PHENOMENA FOR HEAVY WIND THREAT AND INTENSITY SCORES

NH3	**Heavy wind**	**Score**
HW1	High wind to moderate gales (up to 88 km/h)	1,83
HW2	Whole gales (up to 102 km/h)	4,63
HW3	Violent Storm (up to 117 km/h)	6,89
HW4	Hurricanes (118+ km/h)	14,95

The wind threat has been divided according to the power of the wind from meteorological classifications (Beaufort scale) [60]. Due to the impossibility of finding differences between each of the levels of the scale, it was decided to merge some degrees, leaving 3 threat phenomena. As the only variable in this case is intensity, the greater the intensity of the wind, the greater the budgetary implications.

TABLE 8: PHENOMENA FOR LANDSLIDE THREAT AND INTENSITY SCORES

NH4	**Landslide**	**Score**
LS1	Minor rockslides	1,09
LS2	Moderate rockslides	6,01
LS3	Major rockslides	24,94
LS4	Minor soil slides	1,24
LS5	Moderate soil slides	11,78
LS6	Major soil slides (avalanche	37,38

The landslide threat has been divided according to geological classifications. Due to the impossibility of finding differences between each of the levels of the scale, it was decided to merge some degrees, leaving 3 phenomena. As the only variable in this case is intensity, the greater the intensity of the landslide, the greater the budgetary implications.

4.2 Physical incidents

Content in this section redacted.

The full description of this section is included in the none redacted report attached to another confidential deliverable due to security reasons.

5. Profile of cyber threats and their budgetary implications

Chapter redacted.

The full description of this chapter is included in the none redacted report attached to another confidential deliverable due to security reasons.

6. Selected scenario

As mentioned above, the potential phenomena proposed for each threat can interact with each other, facilitating, for example, the commission of physical attacks from other digital attacks. and the scenarios that have been depicted throughout the project are a clear example of some of the possible combinations that can occur.

Chapter redacted.

The full description of this chapter is included in the none redacted report attached to another confidential deliverable due to security reasons.

7. Results

The literature review has allowed the development of a catalogue with a total of 228 phenomena related to the threats previously identified in the SAFETY4RAILS project (D3.1). The phenomena present particular characteristics in which a threat can occur, in addition the phenomena can be combined among them, which allows generating simulated scenarios that respond to the wide variety of ways in which an event could occur while doing so in a standardised way, thanks to the extensive catalogue of proposed phenomena that can be selected when configuring the scenario, and the parsimony and flexibility of the proposed catalogue. Each hazard is composed of several phenomena, which normally have different impacts in relation to the assets they affect and the intensity with which they affect them, which allows the development of scenarios with similar hazards but different intensities.

The risk of the phenomenon on each asset and the expected impact have been presented in a matrix that allows the identification of the assets involved in an event, the impact to the asset and to the service. Knowing the type of assets that will be involved, the CAMS tool can make budget estimates for critical events, using the data provided by the end-user regarding the amount of assets, their cost or repair time. One of the impact levels of the matrix indicates that the asset is still functional but has suffered damage, which allows identifying assets that are still functional but need to be overhauled or whose service life expectancy may be affected. That is, the individual data in the matrix, i.e. the data for each asset, informs CAMS of the assets concerned and the level of adequacy. The present module allows different intensity levels to be selected for the same threat in order to generate degradation curves according to the incident characteristics. The individual data in the matrix, i.e. the data for each asset, informs CAMS of the assets concerned and the level of adequacy.

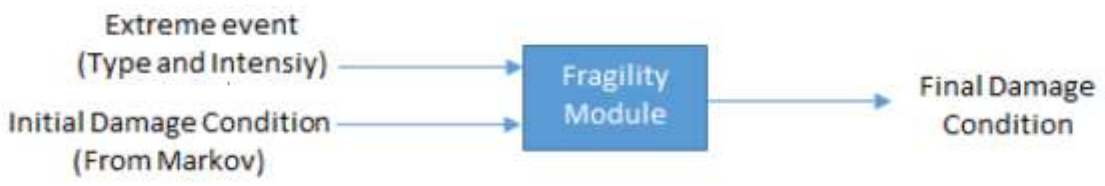

FIGURE 1: FRAGILITY MODULE FROM CAMS

The matrix provides CAMS with the type of extreme event and the intensity of the event, in order to determine the damage after a disruptive element.

Chapter redacted.

The full description of this chapter is included in an annex of another confidential deliverable due to security reasons.

8. Web-based software tool as a budget simulation module

The Budget simulation module of S4RIS is an integral part of the CAMS tool and not an independent software, however CAMS also includes other functionalities. As indicated in D.7.1 CAMS "uses end-user data, including budget plans that can be de-identified under the scope of the SAFETY4RAILS project. In the S4RIS platform, CAMS is used to inform the station operator of the budget and time estimates to repair, maintain, and restore the infrastructure following cyber-physical incidents. This prediction is based on the normal deterioration of railway assets due to age and the unpredictability of cyber-physical incidents" [63]. CAMS calculates maintenance/repair Time and Budgets Scenario for railway/subway components in case of a cyber-physical attack or ageing considering the aspects of deterioration during any incidents and after incidents discussed in this deliverable. In case of a cyber-physical event, CAMS through the S4RIS enables end-users to identify weak and strong points in their infrastructure and it is able to provide specific reports to help evaluate the predictions produced by the tool by comparison with real-time and historical data. Following the incident, the railroad organisation enables to recognise the asset's vulnerability and fragility, which will help improve resource allocation and reduce financial losses for the future of the station itself. The threat catalogue includes threats for which there may not necessarily be previous records from end-users, or the records of these incidents may not necessarily correspond to the assets currently available. This is why the analysis performed in this deliverable on the potential impact on assets of each type of phenomenon is necessary to be able to make budget estimates but also enables the identification and work on assets that have the most impact on the operation of the station, so that the operation of station can commence as soon as possible after the event.

"The CAMS conceptual data model has been created to show how various entities relate to each other during asset assessment. These relationships have dependent and complicated connections, which are difficult to handle from the end-user's perspective. CAMS has been designed to help decision-makers to establish the hierarchy relationships between the components of the railway infrastructure thereby identifying the importance of individual components with regards to system functioning […] Based on the condition of the element before the event, its intensity, and the intensity of the event, we have some way of estimating the actual condition of the element after an extreme event. […] CAMS tool has the capacity to optimise infrastructure investment across multiple locations. For example, rail lines can be divided into metro lines and suburb lines. For multiple asset groups and a limited budget, the optimisation solution focuses on minimising the total cost while keeping critical assets at a specified level of resilience […] and suggests a budget that is required to maintain the facility according to the scenario that is applied to the assets" [64]. The budgeting tool therefore allows to address threats of different intensity to different types of budgets and to perform a simulation that takes into consideration both elements and gives an optimal response to the event and the end-user's budget, considering criticality of the assets. Thus, taking into account the assets that are affected by each phenomenon and the data provided by the end users on the times and costs of changing and repairing the different assets, it is possible to establish the budget for the effective reactivation of the service, considering the impact that each asset has on the service.

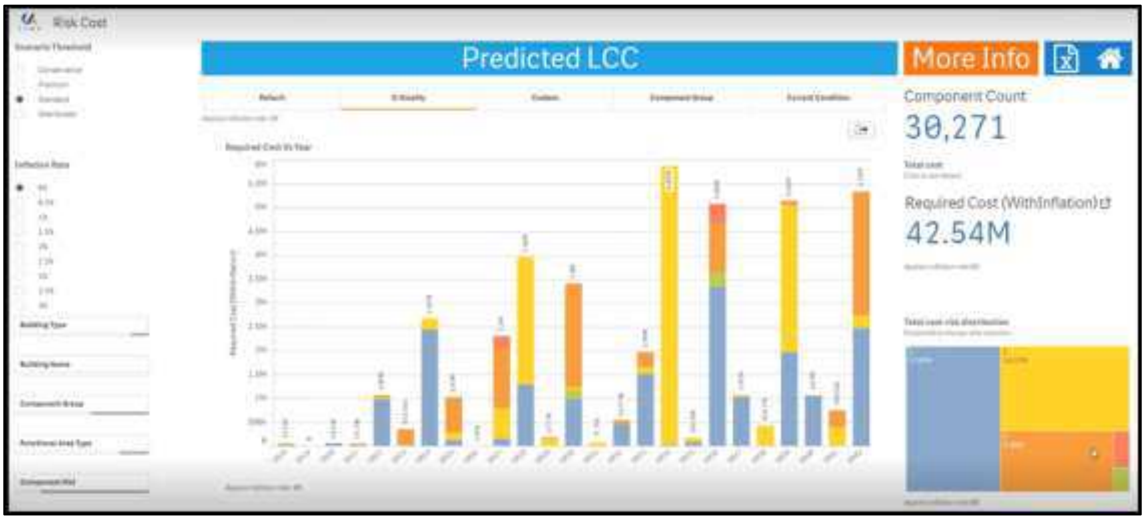

FIGURE 2: CAMS COST DISTRIBUTED BY CRITICALITY. SOURCE D.7.5

9. Conclusion

9.1 Summary

The budget simulation module has developed a catalogue with a total of 228 phenomena related to the threats previously identified in the SAFETY4RAILS project (D3.1) to feed CAMS and allow degradation curves to be made. This module is therefore not a stand-alone tool, but provides a data matrix to be used by CAMS.. A threat can take different forms depending on the particular characteristics of the event and the impact will also be modulated by the characteristics of the target at the time of the event. In order to assess the impact a threat will have on a system, it is necessary to establish both of these characteristics (concerning the threat and the target). In CAMS, end-users can enter detailed information about their asset system, including the number of assets in a location, their replacement cost or repair times, but it is necessary to also consider the characteristics of the event in order to perform a simulation. The budget simulation module, developed in Task 7.3, “Establishing the profile of threats and their budget implications”, provides such data to CAMS allowing budget simulations to be carried out for critical events, taking into consideration their nature and intensity.

Section redacted.

The full description of this section is included in the none redacted report attached to another confidential deliverable due to security reasons.

.

9.2 Future work

Section redacted.

The full description of this section is included in the none redacted report attached to another confidential deliverable due to security reasons.

Bibliography

[1] BENDEA, H., et al. Low cost UAV for post-disaster assessment. *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, 2008, vol. 37, no B8, p. 1373-1379.
[2] BONANNO, George A., et al. Weighing the costs of disaster: Consequences, risks, and resilience in individuals, families, and communities. *Psychological science in the public interest*, 2010, vol. 11, no 1, p. 1-49.
[3] HALLEGATTE, Stéphane. An adaptive regional input-output model and its application to the assessment of the economic cost of Katrina. *Risk Analysis: An International Journal*, 2008, vol. 28, no 3, p. 779-799.
[4] GREENBERG, Michael R.; LAHR, Michael; MANTELL, Nancy. Understanding the economic costs and benefits of catastrophes and their aftermath: A review and suggestions for the US federal government. *Risk Analysis: An International Journal*, 2007, vol. 27, no 1, p. 83-96.
[5] AMENDOLA, Aniello, et al. A systems approach to modelling catastrophic risk and insurability. *Natural Hazards*, 2000, vol. 21, no 2, p. 381-393.
[6] KNEMEYER, A. Michael; ZINN, Walter; EROGLU, Cuneyt. Proactive planning for catastrophic events in supply chains. *Journal of operations management*, 2009, vol. 27, no 2, p. 141-153.
[7] KOKS, Elco E., et al. Regional disaster impact analysis: comparing input–output and computable general equilibrium models. *Natural Hazards and Earth System Sciences*, 2016, vol. 16, no 8, p. 1911-1924.
[8] LI, Jun, et al. Modelling imbalanced economic recovery following a natural disaster using input-output analysis. *Risk analysis*, 2013, vol. 33, no 10, p. 1908-1923.
[9] Chowdhury, S. M., & Gürtler, O. (2015). Sabotage in contests: a survey. Public Choice, 164(1), 135-155,
[10] GNATOVSKAYA, Elena N.; KIM, Alexander A. The Stakhanov movement and the fight against sabotage on the soviet far eastern railway in the 1930s. *The Historian*, 2017, vol. 79, no 2, p. 256-280.
[11] DE LOS COBOS ARTEAGA, Francisco; VARA, Tomás Martínez. Sabotage and management of labour conflicts in the Spanish railway companies (1910-1912). Flux, 2019, no 4, p. 23-33.
[12]https://www.railtech.com/infrastructure/2022/04/15/railway-sabotage-after-50-days-of-war-in-ukraine-here-is-what-we-know/
[13]https://www.theguardian.com/environment/2021/jul/29/activists-sabotaging-railways-indigenou
[14] Oklahoma Energy Today, 2021. Radical environmental activists sabotage railway lines
http://www.okenergytoday.com/2021/07/radical-environmental-activists-sabotage-rai
[15]https://www.telemadrid.es/noticias/madrid/sabotaje-Metro-Madrid-atrapados-pasajeros-0-1418858153--20121213073423.html
[16] Lasslett, K., Green, P., & Stańczak, D. (2015). The barbarism of indifference: Sabotage, resistance and state–corporate crime. Theoretical Criminology, 19(4), 514-533.
[17] Ambrose, M. L., Seabright, M. A., & Schminke, M. (2002). Sabotage in the workplace: The role of organizational injustice. Organizational behaviour and human decision processes, 89(1), 947-965.
[18] GIACALONE, Robert A.; RIORDAN, Catherine A.; ROSENFELD, Paul. Employee sabotage: Toward a practitioner-scholar understanding. En *Work Place Sabotage*. Routledge, 2019. p. 323-343
[19] HARRIS, Lloyd C.; OGBONNA, Emmanuel. Exploring service sabotage: The antecedents, types and consequences of frontline, deviant, antiservice behaviours. *Journal of Service Research*, 2002, vol. 4, no 3, p. 163-183.
[20] Chowdhury, S. M., & Gürtler, O. (2015). Sabotage in contests: a survey. Public Choice, 164(1), 135-155
[21] HOLGERSSON, Annelie; BJÖRNSTIG, Ulf. Mass-casualty attacks on public transportation. *Journal of Transportation Security*, 2014, vol. 7, no 1, p. 1-16.
[22] CHOI, Sungyeol; LIM, Jihwan. A Review on Sabotage Against Transportation of Spent Nuclear Fuel. 2016.
[23] MOSER, Gabriel. What is vandalism? Towards a psycho-social definition and its implications. Vandalism: Research, prevention, and social policy, 1992, p. 20-33.
[24] MIRÓ-LLINARES, Fernando; MONEVA, Asier. What about cyberspace (and cybercrime alongside it)? A reply to Farrell and Birks “Did cybercrime cause the crime drop?”. *Crime Science*, 2019, vol. 8, no 1, p. 1-5.
[25] VAN DIJK, Jan; TSELONI, Andromachi; FARRELL, Graham (ed.). The international crime drop: New directions in research. 2012.
[26] FERNÁNDEZ-MOLINA, Esther; BARTOLOMÉ GUTIÉRREZ, Raquel. Juvenile crime drop: What is happening with youth in Spain and why?. *European Journal of Criminology*, 2020, vol. 17, no 3, p. 306-331.
[27] TURNER, Ralph H. Race riots past and present: A cultural-collective behaviour approach. Symbolic Interaction, 1994, vol. 17, no 3, p. 309-324.
[28] CECCATO, Vania; HAINING, Robert. Assessing the geography of vandalism: Evidence from a Swedish city. Urban Studies, 2005, vol. 42, no 9, p. 1637-1656.
[29] BATES, Eleanor Joanne Wilson. Vandalism: a crime of place?. 2014. Tesis Doctoral. University of Edinburgh.
[30] GOLDSTEIN, Arnold P. The psychology of vandalism. Springer Science & Business Media, 2013.[31] SMITH, Martha Jane. Assessing vandalism cues in an experimental setting: A factorial design involving state of repair, presence of graffiti, target vulnerability, and target suitability. Rutgers The State University of New Jersey-Newark, 1996..

[32] LINCOLN, Alan Jay. Vandalism: causes, consequences and prevention. Library & archival security, 1990, vol. 9, no 3-4, p. 37-61.
[33] SLOAN-HOWITT, Maryalice; KELLING, George L. Subway graffiti in New York City: Gettin'up vs. meanin'it and cleanin'it.". Security Journal, 1990, vol. 1, no 3, p. 131-136.
[34] CLARKE, Ronald Victor Gemuseus; WEBB, Barry. Hot products: Understanding, anticipating and reducing demand for stolen goods. London: Home Office, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, 1999.
[35]https://www.business-standard.com/article/current-affairs/delhi-metro-services-affected-on-blue-line-after-suspected-cable-theft-122071900702_1.html
[36] https://rekord.co.za/424408/metro-introduces-new-cable-theft-hotline/
[37]https://www.networkrail.co.uk/running-the-railway/looking-after-the-railway/delays-explained/vandalism-and-trespass/cable-theft/
[38] https://www.bbc.com/news/uk-england-south-yorkshire-61379785
[39]https://www.verangola.net/va/en/022021/Transports/24172/Police-arrested-two-men-for-allegedly-stealing-railway-sleepers-and-rails.htm
[40] RUBY, Charles L. The definition of terrorism. Analyses of social issues and public policy, 2002, vol. 2, no 1, p. 9-14.
[41] SCHMID, Alex P. The definition of terrorism. En *The Routledge handbook of terrorism research*. Routledge, 2011. p. 39-157.
[42] SCHMID, Alex P. The revised academic consensus definition of terrorism. *Perspectives on Terrorism*, 2012, vol. 6, no 2.
[43] DOUGLAS, John E., et al. *Crime classification manual: A standard system for investigating and classifying violent crime*. John Wiley & Sons, 2013.
[44] CORDESMAN, Anthony H. Terrorism, asymmetric warfare, and weapons of mass destruction: Defending the US homeland. Greenwood Publishing Group, 2002.
[45] NESSER, Petter; STENERSEN, Anne. The modus operandi of jihadi terrorists in Europe. *Perspectives on terrorism*, 2014, vol. 8, no 6, p. 2-24.
[46]CAPELLAN, Joel A.; SILVA, Jason R. An investigation of mass public shooting attacks against government targets in the United States. Studies in Conflict & Terrorism, 2021, vol. 44, no 5, p. 387-409.
[47] LANKFORD, Adam; SILVER, James. Why have public mass shootings become more deadly? Assessing how perpetrators' motives and methods have changed over time. *Criminology & Public Policy*, 2020, vol. 19, no 1, p. 37-60.
[48] THURMAN, James T. *Practical bomb scene investigation*. CRC Press, 2017.
[49] LANGWORTHY, Michael J.; SABRA, John; GOULD, Mark. Terrorism and blast phenomena: lessons learned from the attack on the USS Cole (DDG67). Clinical Orthopaedics and Related Research®, 2004, vol. 422, p. 82-87.
[50] SOLBERG, Kristin. A man I knew became a suicide bomber for IS. 2019.
[51] SHVETSOV, Alex, et al. The "car-bomb" as a terrorist tool at metro stations, railway terminals and airports. Journal of transportation security, 2017, vol. 10, no 1, p. 31-43
[52]Jenkins, B. M., & Butterworth, B. R. (2017). Terrorist vehicle attacks on public surface transportation targets. *Mineta Transportation Institute, San José State University*.
[53] RICHTER, Charles F. An instrumental earthquake magnitude scale. *Bulletin of the seismological society of America*, 1935, vol. 25, no 1, p. 1-32.
[54]LI, Yue; SONG, Ruiqiang; VAN DE LINDT, John W. Collapse fragility of steel structures subjected to earthquake mainshock-aftershock sequences. *Journal of Structural Engineering*, 2014, vol. 140, no 12, p. 04014095.
[55] CHRISTOPOULOS, Constantin; MONTGOMERY, Michael. Viscoelastic coupling dampers (VCDs) for enhanced wind and seismic performance of high-rise buildings. *Earthquake Engineering & Structural Dynamics*, 2013, vol. 42, no 15, p. 2217-2233.
[56]https://www.biome.com.au/blog/what-does-minor-moderate-and-major-flood-levels-mean-in-brisbane/
[57] http://www.bom.gov.au/water/awid/id-333.shtml
[58] https://w1.weather.gov/glossary/index.php?word=flood+categories
[59] SLATER, Louise J.; VILLARINI, Gabriele. Recent trends in US flood risk. *Geophysical Research Letters*, 2016, vol. 43, no 24, p. 12,428-12,436.
[60] HULER, Scott. *Defining the wind: the Beaufort scale and how a 19th-century admiral turned science into poetry*. Crown, 2007.
[61] LEUKFELDT, Rutger; HOLT, Thomas J. (ed.). *The human factor of cybercrime*. Routledge, 2019.
[62] AKDEMIR, Naci; LAWLESS, Christopher James. Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. Internet Research, 2020.
[63] 60. SAFETY4RAILS, Deliverable D7.1 Budget simulation module of S4RIS, august 2022
[64] 60. SAFETY4RAILS, Deliverable D7.5 Budget simulation module of S4RIS, august 2022

ANNEXES

ANNEX I. GLOSSARY AND ACRONYMS

TABLE 9 GLOSSARY AND ACRONYMS

Term	Definition/description
AC	Asset criticallit. Refers to the scale of relevance of the asset in the system.
CBRN	Chemical, Biological, Radiological and Nuclear
CCTV	Closed-circuit television
CRAVED	Concealable, removable, available, valuable, enjoyable, disposable
DDoS	Distributed denial of service
DNS	Domain Name System
EI	Expected Impact. Refers to the scale indicating the level of damage that an asset can sustain.
HTTP	Hypertext Transfer Protocol
I-O models	input-output models
IRV	Individual risk vaules
IT	Information technology
km/h	kilometres per hour
NTP	Network Time Protocol
OIP	Overall Intensity of the Phenomenon. Refers to the total score of the phenomenon under analysis.
OT	Operational technology
PI	Probability of Impact. Refers to the scale indicating the probability of an asset being affected by a phenomenon.
PS	Phenomenom Spectrum. Refers to the number of assets that can be affected in a single incident.
SDoS	XML Denial-Of-Service

SQL	Structured Query Language
XML	extensible markup language

Table 10: List of assets and IDs

table redacted.

The full description of this Table is included in the none redacted report attached to another confidential deliverable due to security reasons.

SAFETY4RAILS

Partners:

Fraunhofer EMI

uic

Metro de Madrid

EGO Genel Müdürlüğü

RFI Rete Ferroviaria Italiana Gruppo Ferrovie dello Stato Italiane

LEONARDO

ceis avisa partners

STAM Mastering Excellence

IC information company

RMIT University

University of Reading

etra I+D

Demokritos National Centre for Scientific Research

RINA

WINGS ICT Solutions

Newcastle University

EOS European Organisation for Security

IN Innova Integra

LAUREA Ammattikorkeakoulu University of Applied Sciences

CyberServices Made in Europe

erarGE

MTRS

INTRACOM TELECOM

Universitas Miguel Hernández

TREE Technology

Elbit Systems C4I and Cyber

ProRail

Comune di Milano

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